А. А. Пихтулов, Д. В. Шевченко, В. Б. Холявин

АНАЛИЗ И КЛАССИФИКАЦИЯ УГРОЗ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ТЕХНОЛОГИИ BLUETOOTH

Введение

Технология Bluetooth хотя и является относительно новой и, по мнению некоторых экспертов, достаточно безопасной, все чаще становится объектом атак со стороны злоумышленников.

В настоящее время Bluetooth используется как одна из сред распространения вирусных программ для мобильных телефонов (например, Cabir, Lasco, Comwar). Существует несколько механизмов использования новой технологии в целях осуществления вирусных атак.

Несовершенство защиты передаваемых данных — еще один недостаток Bluetooth, ведь возможности хищения и искажения информации являются приманкой для злоумышленников.

Рост числа попыток взлома сетей Bluetooth ограничивают следующие факторы:

— Недостаточная распространенность самой технологии. Однако этот фактор с каждым годом все менее значителен.

— Ограниченность зоны покрытия. В последнее время и данный фактор становится менее значимым. Устройства Bluetooth могут поддерживать покрытие зоны радиусом 100 м.

— Сеть Bluetooth имеет некоторые механизмы защиты от подслушивания и неавторизованного подключения, обход которых требует от злоумышленника определенной квалификации. Однако в этой системе защиты существуют уязвимости.

Таким образом, можно с уверенностью предсказать рост в ближайшем будущем числа попыток атак на мобильные устройства, оснащенные передатчиком Bluetooth.

1. Анализ механизмов проведения атак на устройства Bluetooth

Технология Bluetooth обладает большим количеством уязвимостей [1]. Многие из уровней защиты легко преодолимы. Более того, большинство пользователей не осознают реальность угрозы атаки на их устройства с использованием технологии Bluetooth и поэтому не предпринимают никаких действий для защиты. Рассмотрим наиболее распространенные атаки на мобильные устройства, использующие технологию Bluetooth.

Взлом PIN-кода

Суть атаки заключается в обнаружении PIN-кода, защищающего Bluetooth-соединение. Она проводится злоумышленником для последующего раскрытия всех зашифрованных сообщений, передаваемых по Bluetooth, а также для обхода процедуры аутентификации и получения доступа к устройству [2].

Подобная атака на Bluetooth-устройство может быть проведена несколькими способами, один из них основан на использовании человеческого фактора, второй же использует математические методы.

В результате проведения данной атаки злоумышленник может перехватывать весь трафик, передаваемый между устройствами Bluetooth. Прослушивание при получении PIN-кода будет возможно даже в случае шифрования трафика.

Атака с подменой устройства

При выполнении атаки злоумышленник осуществляет подмену уже авторизованного устройства. Для этого атакующий настраивает новое устройство таким образом, чтобы его адрес, список доступных профилей, а также протокол работы совпадали с аналогичными значениями подменяемого устройства [3].

Выполнить такую подмену возможно, так как в настоящее время существуют Bluetooth-устройства, позволяющие вводить адрес.

В результате выполнения такой атаки злоумышленник может получить полный контроль над телефоном за счет выполнения на нем AT-команд, а также доступ к произвольным файлам.

Атака на piconet-сеть

Атака направлена на разрушение piconet-сети устройством, не входящим в состав сети. В ее основе лежит следующая особенность построения Bluetooth-сетей: устройство типа Master должно поддерживать несколько соединений для образования расширенных сетей (scatternet).

Атакующий может провести описанную выше атаку с подменой устройства на одно из устройств piconet-сети. После того как устройство подменено, оно обращается к устройству типа Master. Такое поведение устройства типа Slave приводит к тому, что устройство типа Master перестает отвечать за контроль piconet-сети и разрушаются установленные в piconet-сети связи [4]. Данная ошибка не связана с производителем устройств, а является уязвимостью, присущей всем устройствам Bluetooth.

Атака со сбросом ключа связи

Атака заставляет устройство Bluetooth сбросить хранимый ключ связи, тем самым давая злоумышленнику возможность прослушать обмен ключами. В последнее время эта атака может быть проведена в режиме реального времени, таким образом, обмен ключами может быть вызван в нужный для атакующего момент [4].

Для проведения атаки злоумышленник должен знать адреса сопряженных устройств. Атакующий подделывает адрес одного из устройств и соединяется с другими. Поскольку злоумышленник не располагает ключом связи, когда целевое устройство посылает запросы проверки подлинности, устройство атакующего будет отвечать «HCI_Link_Key_Request_Negative_Reply», что в некоторых случаях может стать причиной сброса ключа в атакуемом устройстве и перехода в режим соединения.

Атака подделки точки доступа

Некоторые мобильные телефоны обладают уязвимостью, которая может позволить злоумышленнику перехватывать весь исходящий трафик устройства. Дело в том, что некоторые телефоны отображают обнаруженные в результате поиска устройства по именам, присвоенным им их хозяевами. Эти имена, очевидно, могут повторяться, и пользователю достаточно легко будет спутать одно устройство с другим.

Таким образом, злоумышленник может осуществить подмену устройства и прослушивать весь исходящий трафик абонента. Есть несколько возможных применений таких атак.

Так, например, существуют сервисы, предоставляющие возможность обращения к точке доступа в Интернет через Bluetooth. Если злоумышленник получит PIN устройства точки доступа, его адрес и имя, данное пользователем (что можно осуществить с помощью описанных выше видов атак), то сможет перехватить всю исходящую информацию устройства.

Другой сценарий атаки выглядит следующим образом. Пользователь получает сообщение с просьбой об авторизации от знакомого абонента, который на самом деле является злоумышленником. Такая ситуация возможна, например, в случае использования мобильного киоска, в котором пользователь может заказать, оплатить, а потом скачать, например, мелодию для мобильного телефона. Скачивать данные пользователь должен через Bluetooth. Таким образом, злоумышленник может сразу после оплаты атакуемым передаваемых данных отправить запрос авторизации по Bluetooth под именем «mobile-kiosk». Пользователь, позволивший авторизацию, будет атакован, и ему, например, может быть передан вирус.

Атака с раскрытием информации об устройстве

Атака направлена на получение полной информации об устройстве, в том числе и о наличии уязвимостей, и призвана обойти механизмы защиты Bluetooth, целью которых является скрытие всех данных об устройстве [5]. Существует несколько ее разновидностей.

Первый вид атаки предназначен для обхода «скрытого» режима устройства. Данный режим был предусмотрен разработчиками Bluetooth для того, чтобы пользователь мог раскрывать свое присутствие только тем пользователям, которых он знает, и оставаться незамеченным для посторонних (в том числе злоумышленников). В результате проведения атаки злоумышленник может получить адрес Bluetooth-устройства, находящегося в скрытом режиме. Второй вид атаки предназначен для выявления всех данных об устройстве. Эта атака позволяет вычислить модель устройства, протоколы, по которым работает устройство, и другие необходимые данные об устройстве, включая его уязвимости.

Такая атака может использоваться в качестве дополнения к большинству атак на Bluetooth. Дело в том, что в случае многократных неудачных попыток взлома жертва может заподозрить, что ее телефон стал объектом атаки. В то же время, если злоумышленник будет располагать подробной информацией до начала нападения, он сможет лучше спланировать свои действия и подобрать именно тот способ взлома, который будет наиболее эффективен для данного устройства.

Атака с использованием уязвимых каналов

Атака позволяет злоумышленнику совершать с устройствами с включенным Bluetooth неавторизованные действия.

Она основана на уязвимости некоторых устройств, оснащенных передатчиком Bluetooth. Дело в том, что большинство устройств, имеющих возможность удаленного управления, например, средствами гарнитуры, не предусматривают авторизацию таких устройств, т. е. канал (channel) в профиле для гарнитуры не защищен. А ведь именно по этому каналу фактически гарнитура осуществляет управление устройством (а конкретно выполнение AT-команд). Таким образом, злоумышленник может подключиться по такому каналу к устройству и осуществлять удаленное выполнение AT-команд. Это позволяет произвести следующие действия:

- инициировать телефонный звонок;
- посылать SMS-сообщения на любой номер;
- читать SMS с телефона;
- читать и писать записи телефонной книги;
- устанавливать переадресацию звонков [5].

Существует несколько сценариев атаки с использованием данной возможности. Выбор падает на ту или иную версию атаки в зависимости от того, какие цели преследует атакующий.

Атака с переполнением буфера

Атака представляет собой DoS-атаку на устройство Bluetooth. Ей могут быть подвержены устройства, в которых существует возможность переполнения буфера, т. е. не реализована проверка длины пакета. Таким образом, эти устройства являются уязвимыми к пакетам, размеры которых достаточно велики для того, чтобы переполнить выделяемый под них буфер [5]. Атака с переполнением буфера приводит в большинстве случаев к выходу мобильного телефона из строя.

Атака с использованием уязвимости OBEX (OPP)

Одна из самых эффективных Bluetooth-атак. Строится на уязвимости ряда устройств, связанной с реализацией аутентификации при взаимодействии OBEX-клиента и OBEX-сервера.

OBEX Push Profile (OPP) служит для обмена бизнес-картами (vCard) и другими объектами. В большинстве случаев этот сервис не требует аутентификации. Именно этим упущением в безопасности мобильных устройств могут воспользоваться злоумышленники.

Атакующий выполняет OBEX GET запрос к известным файлам, например telecom/pb.vcf (адресная книга) или telecom/cal.vcs (календарь). Ввиду отсутствия аутентификации эти файлы могут быть похищены злоумышленником [5].

Атака с использованием уязвимости OBEX (FTP)

Как и предыдущая, данная атака использует уязвимость OBEX FTP сервера, который часто устанавливают на мобильные телефоны некоторых производителей [5].

Атакующий может просматривать содержимое файловой системы (через команду ls) или, например, удалять файлы (команда rm). Возможны действия с любой памятью, в том числе и с картами расширения memory stick или SD.

Атака с использованием уязвимости передачи vCard устройству Motorola

Атака позволяет злоумышленнику совершать неавторизованные действия с устройствами с включенным Bluetooth. В ее основе лежит уязвимость телефонов Motorola. Если удаленное устройство пересылает устройству Motorola сообщение формата vCard, то телефон Motorola заносит его в список доверенных устройств на время передачи.

Атакующий инициирует соединение через OBEX Push Profile, симулируя посылку vCard. Затем он вызывает прерывание процесса отсылки, после чего устройство атакующего сохраняется в списке доверенных устройств на телефоне жертвы. Если после прерывания устройства злоумышленника не будет в списке доверенных устройств, то процесс отправки-прерывания может быть повторен, пока устройство Motorola не сработает нужным для атакующего образом [5].

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

Атака для определения местоположения объекта

Атака направлена на определение местоположения мобильного телефона объекта [6]. Протокол Bluetooth имеет две уязвимости, используя которые злоумышленник может осуществить следующие виды атаки:

· *Атака с использованием открытого адреса устройства.*

В протоколе Bluetooth адрес устройства передается в незашифрованном виде. Эта уязвимость используется при проведении атак с раскрытием адреса. Адрес большинства устройств Bluetooth изменять нельзя, а это означает, что в случае обнаружения адреса устройства злоумышленник сможет отслеживать местоположение атакуемого. Конечно, радиус слежения ограничивается несколькими сотнями метров, но при использовании специального оборудования этот диапазон можно увеличить.

· *Атака с использованием уязвимостей аутентификации.*

Реализации аутентификации некоторых устройств Bluetooth обладают уязвимостями. Злоумышленник, осуществив проникновение в мобильный телефон жертвы через такую уязвимость, может выполнять на нем произвольные AT-команды, в том числе команды по отправке SMS-сообщений. Кроме того, в упомянутых выше атаках с использованием уязвимости OBEX рассматривались методы возможной передачи файлов на мобильный телефон атакуемого. Таким файлом может оказаться резидентная вирусная программа, способная исполнять AT-команды, отправляя сообщения с местоположением объекта.

Атака с регенерацией ключа

Атака с регенерацией ключа позволяет создать неавторизованное подключение к устройству атакуемого.

Уязвимость, используемая данной атакой, заключается в следующем. Пусть устройство Bluetooth установило авторизованное соединение с удаленной машиной. В том случае, если ключ связи с данного устройства удаляется, сеанс связи не прерывается. Сам атакуемый может во время удаления ключа связи и не знать, что связь не была прервана, а также не подозревать, что такое удаление ключа потенциально опасно [5].

Все, что необходимо сделать после удаления ключа атакующему, — запросить регенерацию ключа. После этого злоумышленник получает новый ключ без аутентификации. Таким образом, он может получить доступ к устройству до тех пор, пока ключ не будет удален.

Атака с использованием уязвимости в интерпретации имени телефона

Атака направлена на вывод из строя атакуемого устройства. Используемая при этом уязвимость заключается в неправильной интерпретации многими телефонными аппаратами имени подключаемого устройства. Имя устройства Bluetooth кодируется в формате UTF-8. Все устройства, представленные на рынке в настоящее время, поддерживают именно эту кодировку. Тем не менее некоторые интерпретаторы не выполняют проверку на наличие в строке имени каких-либо управляющих символов. Присутствие таких символов может привести к тому, что отвечающий за обработку имени программный модуль даст сбой, вызвав тем самым зависание аппарата, поддерживающего Bluetooth-протокол [4].

Атака с подделкой отправителя

Атака не представляет значительной опасности, тем не менее она может стать психологическим оружием.

Дело в том, что существует возможность отправки на устройство жертвы анонимного сообщения. Такое сообщение невозможно отследить, так как на телефоне жертвы оно отображается как сообщение без обратного адреса [7].

Атака с использованием уязвимости RFCOMM

Протокол Bluetooth имеет уязвимости и на уровне RFCOMM, что позволяет злоумышленнику подключиться через сокет RFCOMM к устройству жертвы. Для этого сначала создается канал связи, а затем — подключение к атакуемому устройству. Для передачи команды на мобильный телефон атакуемого необходимо осуществить запись в данное устройство, используя дескриптор файла rfcomm_fp. Для подобных атак существует множество вспомогательных библиотек, например Bluez.

Вирусы Bluetooth

Выше рассмотрен ряд возможных атак на мобильное устройство. Но такие атаки, как правило, совершаются целенаправленно. Тем не менее в мире мобильных устройств существуют также и так называемые мобильные вирусы — программы, действующие автономно от атакующего.

В настоящее время известно несколько вирусов, которые используют Bluetooth как среду распространения [8]. Червь Caribe — первый сетевой червь, распространяющийся через Bluetooth и заражающий мобильные телефоны, работающие под управлением OS Symbian. При каждом включении зараженного телефона червь получает управление и начинает сканировать список активных Bluetooth-соединений, пытаясь передать на них свою копию. Далее применяется техника, аналогичная рассмотренной в атаке с использованием уязвимости OBEX (FTP): вирус создает OBEX FTP-клиент для обращения к мобильному устройству жертвы, используя объект

obexBTProtoInfo, настроенный для связи с сервером OBEX атакуемого мобильного телефона. Таким образом, вирус получает доступ к файловой системе атакуемого мобильного телефона и может осуществить перенос собственного тела на новое устройство.

Еще один известный червь Commwarrior также использует Bluetooth для распространения, однако в зависимости от версии вируса может рассылаться и через MMS. Другое отличие от Caribe заключается в том, что файлы этого вируса принимают произвольные названия при рассылке для маскировки.

2. Классификация Bluetooth-угроз

Из-за относительной новизны большинства перечисленных угроз на сегодняшний день не существовало достаточно полной классификации всех возможных атак на мобильные устройства с поддержкой Bluetooth.

На основе проведенного анализа можно выделить общие черты вредоносных воздействий и сформировать классификацию видов угроз. Полученная классификация приведена на рис. 1. Все угрозы можно разделить на две категории: атаки и вирусы. В свою очередь, атаки и вирусы можно классифицировать далее по различным критериям: по виду вредоносного воздействия, по виду используемой уязвимости и по виду цели атаки. Таким образом, например, взлом PIN-кода можно отнести к атаке с прослушиванием соединения, использующей уязвимость PIN-кода и направленной на сопряженные устройства, а атаку с переполнением буфера — к атаке, выводящей устройство из строя, использующей уязвимость буфера на переполнение и направленной на одно устройство.

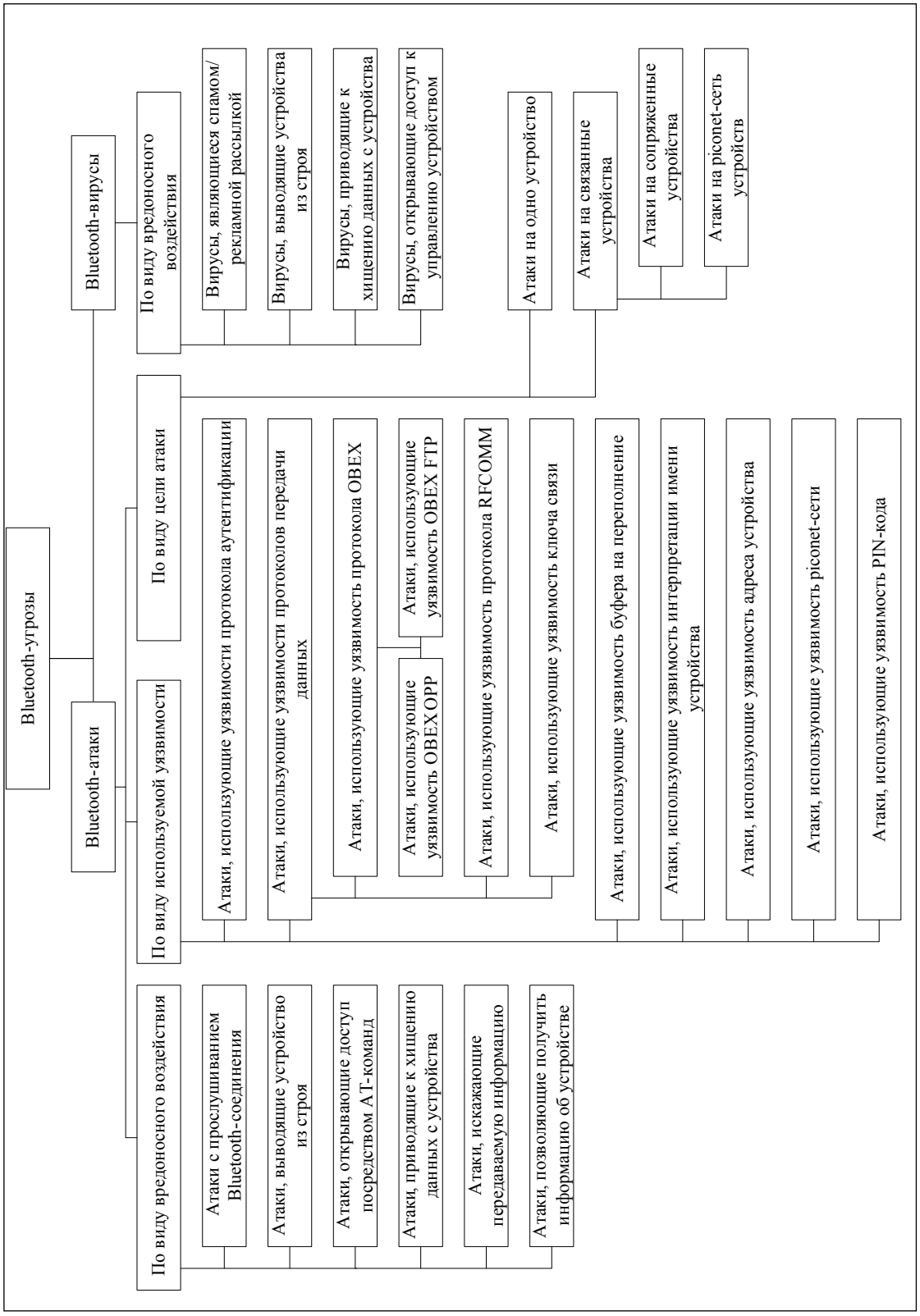

Рис. 1. Классификация Bluetooth-угроз

Заключение

В статье были рассмотрены различные угрозы для Bluetooth-устройств и сформирована их классификация, позволяющая более наглядно представить последствия вредоносного воздействия на мобильные устройства. Кроме того, с ее помощью можно выделить основные направления, в которых нужно двигаться для создания эффективных механизмов для защиты технологии Bluetooth.

СПИСОК ЛИТЕРАТУРЫ:

1. *Михайлов Д. М., Жуков И. Ю.* Исследование уязвимостей Bluetooth-передатчика мобильных телефонов // Научная сессия НИЯУ МИФИ-2010. XIII Международная телекоммуникационная конференция студентов и молодых ученых «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3 частях. Ч. 2. М.: НИЯУ МИФИ, — 276 с., 2010.
2. *Shaked Y., Wool A.* Cracking the Bluetooth PIN. // School of Electrical Engineering Systems. — 22 с., 2005.
3. *Holtmann M.* Bluetooth Security Unleashed. // BlueZ Project. — 30с., 2005.
4. *Laurie A., Holtmann M., Herfurt M.* Bluetooth Hacking: The State of the Art. BlackHat Europe — 51с., 2006.
5. *Laurie A., Holtmann M., Herfurt M.* WhatTheToool // Bluetooth Security Workshop. — 40с., 2004.
6. *Haase M., Handy M.* BlueTrack — Imperceptible Tracking of Bluetooth Devices. University of Rostock, — 2с., 2004.
7. *Laurie A., Holtmann M., Herfurt M.* Hacking Bluetooth enabled mobile phones and beyond — Full Disclosure. // 21C3: The Usual Suspects. — 41с., 2004.
8. *Yan G., Eidenbenz S.* Bluetooth Worms: Models, Dynamics, and Defense Implications. // Los Alamos National Laboratory Publication. № LA-UR-06-1476. — 12 с., 2006.