А. Д. Прохоров, Д. С. Крымов, С. Д. Мизун, А. А. Пихтулов

НЕСАНКЦИОНИРОВАННОЕ ПОЛУЧЕНИЕ ДАННЫХ О BLUETOOTH-УСТРОЙСТВАХ

Введение

Рассматриваемая атака направлена на получение полной информации об устройстве, в том числе и о наличии уязвимостей. Существует несколько разновидностей данной атаки.

Первая из них предназначена для обхода «скрытого» режима устройства, предусмотренного разработчиками Bluetooth для того, чтобы пользователь мог раскрывать свое присутствие только тем, кого он знает, и оставаться незамеченным для посторонних. Проведя атаку данного вида, злоумышленник может получить адрес Bluetooth устройства, находящегося в скрытом режиме.

Второй вид атаки предназначен для выявления всех данных об устройстве: модели телефона, протоколов его работы и другой важной информации [1].

Несанкционированное получение данных о Bluetooth-устройствах в скрытом режиме

По замыслу разработчиков сети Bluetooth перевод телефона в «скрытый» режим должен обезопасить пользователей от неавторизованного доступа к их устройствам. Тем не менее реализация этого механизма обладает уязвимостью, которая позволяет злоумышленникам определить телефоны, находящиеся в «скрытом» режиме.

Если говорить о простом переборе всех возможных адресов существующих устройств, а также принять во внимание, что обращение вслепую к случайному адресу для обнаружения телефона в зоне покрытия сети Bluetooth занимает около 6 секунд, то на выяснение наличия в комнате, например, аппарата Sony Ericsson уйдет 3 года. В этом случае необходимо перебрать 16 777 216 различных вариантов. Тем не менее существуют возможности для снижения количества попыток.

Если злоумышленник каким-либо образом может определить марку телефона атакуемого или хотя бы его производителя, то количество необходимых ему для перебора комбинаций значительно уменьшается [1].

Дело в том, что большинство фирм, выпускающих мобильные устройства, присваивают вполне определенные значения первым трем байтам адреса телефона. Так, например, первые 7 цифр для аппаратов Sony Ericsson — это всегда 00:0A:D9:E. Таким образом, диапазон необходимых для перебора значений снижается до 5 цифр. Более того, если злоумышленник определит, что перед ним модель Sony Ericsson P900, то с большой долей вероятности сможет сказать, что первые 8 цифр располагаются в диапазоне 00:0A:D9:E7 — 00:0A:D9:EE. Подобные статистические выкладки существуют и для других производителей телефонов и их марок.

Кроме того, повысить скорость обнаружения атакующий может за счет увеличения количества сканирующих устройств, если разделить между ними диапазоны адресов, настроив, например, одно на поиски телефонов марки Sony Ericsson, а другое — на Nokia.

Несанкционированное получение данных о Bluetooth-устройствах, находящихся в открытом для обнаружения режиме

Bluetooth-адрес устройства может быть раскрыт злоумышленником во время установки соединения. Дело в том, что адрес телефона передается в незашифрованном виде. Это значительная уязвимость в реализации протокола сети Bluetooth, хотя по замыслу разработчиков Bluetooth-передача незашифрованных данных все же может считаться защищенной, так как злоумышленник не знает частоты, на которой осуществляется связь двух устройств. Но в настоящее время ее подбор — дело нескольких минут, так как на рынке уже представлены предназначенные для этого устройства [2].

Кроме того, связь всех устройств в piconet-сети происходит на одинаковой частоте. Это означает, что злоумышленник может просто стать на некоторое время частью сети, определить частоту, а затем использовать эти данные для перехвата адресов устройств.

Большинство пользователей держат свои мобильные телефоны в открытом для обнаружения режиме. Это означает, что у злоумышленника гораздо больше шансов определить адрес устройства.

Еще одна уязвимость Bluetooth заключается в том, что для установки соединения между двумя телефонами хотя бы одно из устройств не должно находиться в скрытом режиме.

Таким образом, узнав адрес аппарата, злоумышленник может подсоединиться к нему с помощью запроса на уровне L2CAP. Ни одно из устройств Bluetooth на данный момент не обладает возможностью отказать в подключении неавторизованному пользователю на уровне L2CAP. Более того, пользователь даже не обнаружит факта подключения [2].

Bluetooth-адрес невозможно сменить вручную, так что, один раз узнав адрес телефона, злоумышленник всегда сможет связаться с ним.

Для получения полной информации об устройстве, работающем в сети Bluetooth, злоумышленник вначале вычисляет идентификатор устройства, а затем по специальной базе данных получают всю необходимую информацию об этом устройстве. Рассмотрим алгоритм расчета уникального идентификатора, который имеет следующий вид:

00:60:57@2621543

Первая часть идентификатора — это первые три байта адреса аппарата. Вторая часть после символа @ — это вычисляемая по определенному алгоритму сумма, уникальная для каждого устройства. Порядок ее расчета следующий.

Каждое Bluetooth-устройство предоставляет те или иные сервисы. Какие именно, можно узнать, используя SDP (Service Discovery Protocol). Каждое устройство, предназначенное для работы по Bluetooth, имеет SDP-сервер, который отвечает за предоставление подключаемым по сети Bluetooth телефонам информации о профилях адресуемого устройства.

Запрос на получение таких данных атакующий может выполнить с помощью утилиты sdptool [1].

Так, например, в ответ на запрос о предоставляемых профилях выдается следующее описание профиля OBEX Push.

Service Name: OBEX Object Push
Service RecHandle: 0x1000c
Service Class ID List:
“OBEX Object Push” (0x1105)
Protocol Descriptor List:
“L2CAP” (0x0100)
“RFCOMM” (0x0003)
Channel: 9
“OBEX” (0x0008)
Language Base Attr List:
code ISO639: 0x656e
encoding: 0x6a
base offset: 0x100
Profile Descriptor List:
“OBEX Object Push” (0x1105)
Version: 0x0100

После получения этих данных осуществляется расчет второй части уникального идентификатора. Для этого используются следующие поля:

RecHandle — поле длиной 32 бита, которое инициализируется SDP-сервером при включении устройства (в случае приведенного примера это 0x1000c). Для мобильного телефона эти значения жестко прописаны в памяти и не изменяются.

Channel — номер канала, по которому может быть осуществлено обращение к данному сервису. В рассматриваемом примере это 9.

Для получения необходимого числа следует умножить значение поля RecHandle на значение поля Channel. Аналогичным образом надо поступить для каждого сервиса, предоставляемого устройством. После чего сложить все полученные произведения.

Выглядит эта операция примерно так [2].

RecHandle	Channel	Произведение
0x1000b	2	131094
0x1000c	9	589932
0x1000d	1	65549
0x1000e	15	983250
0x1000f	3	196653
0x10010	13	852176
0x10011	12	786636
		3605290

Таким образом, вычислена вторая часть уникального номера устройства.

Теперь, получив полный идентификатор, злоумышленник может сопоставить его со значениями из специальной таблицы. Пример нескольких строк из нее приведен ниже (таблица 1).

Таблица 1. Выдержка из таблицы идентификаторов устройств

Идентификатор	**Производитель**	**Модель**
00:0A:95@1114112	Apple	Беспроводная клавиатура
00:01:EC@2359452	Ericsson	T39m
00:30:6E@269099048	HP	iPAQ 5500 PocketPC
C6:F7:4A@655407	Motorola	A1000

Результатом атаки является раскрытие детальных данных об устройстве. Необходимо заметить, что подобным образом можно получить и информацию о его уязвимостях.

Атака на практике комбинируется с большинством атак на Bluetooth. Дело в том, что в случае неудачи большого количества атак жертва может заподозрить, что были предприняты попытки взломать телефон. В то же время, если злоумышленник будет располагать подробной информацией до атаки, он может лучше спланировать свои действия и подобрать именно тот способ взлома, который будет наиболее действенен для соответствующей модели телефона.

Защититься от данной атаки можно с помощью дополнительного шифрования передаваемой информации. Таким образом, для раскрытия имени устройства злоумышленнику понадобится значительно больше времени и ресурсов, а так как зона действия Bluetooth-передатчиков ограничена, а значит, и время, в течение которого мобильный телефон подвергается угрозе, также лимитировано, подобная атака становится нецелесообразной.

СПИСОК ЛИТЕРАТУРЫ:

1. *Herfurt M., Mulliner C. R.* Blueprint — proof-of-concept implementation for Bluetooth fingerprinting. December 2004 URL: http://www.trifinite.org.

2. *Laurie B., Laurie A.* Serious flaws in Bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd. January 2004.8. URL: http://bluestumbler.org.