О. И. Шишин, Ю. Ю. Панин, М. И. Дмитриев, А. А. Пихтулов

ВЫВОД BLUETOOTH-УСТРОЙСТВ ИЗ СТРОЯ

Введение

Уязвимости Bluetooth-технологии позволяют злоумышленникам не только прослушивать телефонные переговоры, но и выводить из строя устройства. Подобные недостатки представляют серьезную опасность для обладателей мобильных телефонов. Фактически реализация данной атаки является доказательством неустойчивости Bluetooth-протоколов к DoS-атакам. Стоит отметить, что вывод из строя устройств, поддерживающих Bluetooth, может быть осуществлен сразу на нескольких уровнях.

Вывод из строя Bluetooth-устройства на уровне L2CAP

На уровне L2CAP существует возможность отправки запроса на отклик другого Bluetooth-устройства. Его цель заключается в проверке связи и измерении времени отклика на установленное соединение [1].

Недостатком большинства устройств является отсутствие проверки длины пакета, что делает их уязвимыми к пакетам, длины которых достаточно велики для того, чтобы переполнить выделяемый под них буфер. Как правило, длины пакета в 600 байт оказывается вполне достаточно для переполнения буферов большинства устройств.

Для осуществления атаки злоумышленник на устройстве с операционной системой типа UNIX устанавливает библиотеку BlueZ для работы со стеком Bluetooth. С помощью утилиты l2ping, которая распространяется в дистрибутиве BlueZ, можно задавать длину посылаемых пакетов. Для этого атакующий выполняет команду [2]:

l2ping -s 600 <адрес устройства>

Низкоуровневый протокол работы устройства злоумышленника и атакованного устройства при выполнении данной атаки выглядит следующим образом (таблица 1). Пусть устройство A — это устройство атакующего, а устройство B — устройство жертвы.

Таблица 1. Низкоуровневый протокол работы устройства злоумышленника и атакованного устройства

A -> B	**HCI Command: Create Connection (0x01|0x0005) plen 13**
	0000: b6 1e 33 6d 0e 00 18 cc 02 00 00 00 01
	Запрос от устройства A на создание подключения
A <- B	**HCI Event: Command Status (0x0f) plen 4**
	0000: 00 01 05 04
	Ответ от устройства B о получении запроса
A <- B	**HCI Event: Connect Complete (0x03) plen 11**
	0000: 00 29 00 b6 1d 32 6d 0e 00 01 00
	Ответ от устройства B о создании подключения
A -> B	**ACL data: handle 0x0029 flags 0x02 dlen 28 L2CAP(s): Echo req: dlen 20**
	0000: 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 0010: 55 56 57 58
	Передача пакетов данных в асинхронном режиме

A <- B	**HCI Event: Number of Completed Packets (0x13) plen 5**
	0000: 01 29 00 01 00
	Отправка подтверждения о получении пакетов с данными
A <- B	**ACL data: handle 0x0029 flags 0x02 dlen 28 L2CAP(s): Echo rsp: dlen 20**
	0000: 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 0010: 55 56 57 58
	Отправка обратно полученных данных
A ->B	**HCI Command: Disconnect (0x01|0x0006) plen 3**
	0000: 29 00 13
	Отправка запроса на прекращение соединения
A <- B	**HCI Event: Command Status (0x0f) plen 4**
	0000: 00 01 06 04
	Подтверждение получения запроса
A <- B	**HCI Event: Disconn Complete (0x05) plen 4**
	0000: 00 29 00 16
	Отправка подтверждения о прекращении соединения

В примере приведены пересылаемые датаграммы и порядок их обработки. Именно установка необходимой длины пакетов передаваемых сообщений приводит в большинстве случаев к выходу мобильного телефона из строя.

С различными параметрами уязвимы следующие модели: Nokia N70, SonyEricsson T68i, W800i и K600i.

Защититься от такой атаки существующими средствами невозможно. Единственным средством может быть смена прошивки мобильного устройства, с тем чтобы установить проверку получаемых пакетов.

Вывод устройства из строя при считывании имени устройства-злоумышленника

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

Имя устройства в формате Bluetooth кодируется в формате UTF-8. Все аппараты, представленные на рынке в настоящее время, поддерживают именно эту кодировку. В некоторых интерпретаторах, тем не менее, не реализована проверка вводимой строки. Присутствие в строке имени управляющих символов может привести к отказу программного модуля, отвечающего за ее обработку, и тем самым вызвать зависание аппарата.

Для проведения атаки злоумышленнику необходимо иметь устройство, работающее под управлением операционной системы типа UNIX и оснащенное Bluetooth-передатчиком. Также требуется установить библиотеку Bluez.

Рассмотрим программную реализацию ключевой части данной атаки.

На этапе установки соединения с телефоном атакуемого злоумышленник передает ему неверное имя устройства.

Для этого при получении сокета, который будет использоваться для общения с устройством жертвы, осуществляется запрос с помощью функции hci_send_cmd [2].

Выполняется такое действие следующей командой:

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

Параметр OCF_CHANGE_LOCAL_NAME является идентификатором команды передачи имени устройства. s — это имя открытого сокета. То, что обращение идет к тому уровню стека протоколов, который ответственен за изменение имени, определяется параметром OGF_HOST_CTL.

Кроме того, в качестве параметров в данную функцию передается само новое имя и его длина. Имя передается в структуре cp. Поле данной структуры name должно быть инициализировано специальным значением, содержащим управляющие символы.

Разработчики протокола не учитывали возможность передачи искаженного имени, ведь изначально протокол использовался устройствами, оснащенными достаточно жесткой логикой, где отсутствовала возможность ввода управляющих символов в строке имени.

Таким образом, устройства, поддерживающие Bluetooth-соединения, могут быть выведены из строя злоумышленником как при непосредственном подключении к атакуемому устройству (когда злоумышленник подставляет невалидное имя), так и вообще без ведома атакуемого (когда злоумышленник просто отправляет команду l2ping на устройство жертвы).

СПИСОК ЛИТЕРАТУРЫ:

1. *Herfurt M.* Bluesnarfing @ CeBIT 2004 — Detecting and Attacking bluetoothenabled Cellphones at the Hannover Fairground. Technical report, March 2004. URL: http://trifinite.org.

2. *Laurie B., Laurie A.* Serioius flaws in bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd. January 2004. URL: http://bluestumbler.org.