*А. Г. Бельтов, И. Ю. Жуков, А. В. Новицкий, Д. М. Михайлов, А. В. Стариковский*

# НЕАВТОРИЗОВАННОЕ ПОХИЩЕНИЕ ДАННЫХ С BLUETOOTH-УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ УЯЗВИМОСТЕЙ OBEX-ПРОТОКОЛА

## Введение

Атаки, связанные с похищением данных или неавторизованным проникновением в устройства, оснащенные Bluetooth-передатчиком, являются одними из наиболее распространенных. Bluetooth-протоколы уязвимы сразу на нескольких уровнях, что позволяет злоумышленникам выбирать тот или иной тип атаки. Также существенно расширяется номенклатура устройств, подверженных описываемому виду атак. В данной статье речь пойдет об атаках, которые основаны на уязвимости в популярном Bluetooth-профиле OBEX.

## Атака, использующая уязвимости OBEX-профиля

Атака строится на уязвимости ряда устройств, которая связана 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 [1].

Атакующий выполняет OBEX GET запрос к известным файлам, например telecom/pb.vcf (адресная книга) или telecom/cal.vcs (календарь). При отсутствии аутентификации эти файлы передаются злоумышленнику.

Рассмотрим, почему такое стало возможным, более подробно. Клиент OBEX используется для отправки или получения объектов с сервера OBEX. На мобильном устройстве, поддерживающем передачу данных через Bluetooth, как правило, реализован сервер OBEX. Обмен данными между сервером и клиентом происходит с помощью достаточно простого протокола. Базовыми командами протокола, используемыми при атаке, являются PUT и GET. Первая применяется для передачи файлов, вторая — для их получения.

Необходимо заметить, что для того, чтобы получить некоторый файл с удаленного устройства, необходимо знать имя этого файла. В большинстве телефонных аппаратов самых разных производителей такие файлы имеют одинаковые имена.

Реализовать простейшую атаку можно с помощью программных средств Netgraph для операционной системы FreeBSD. Ниже дается пример сеанса OBEX, где с сотового телефона забирается объект с информацией об устройстве, а новый объект (визитная карточка vCard) передается в каталог сотового телефона [2].

```
# obexapp -c -a 00:01:e2:3f:c5:9a -C FTRN
obex> get
get: remote file> telecom/devinfo.txt
Success, response: OK, Success (0x20)
obex> put
put: local file> new.vcf
Success, response: OK, Success (0x20)
obex> di
Success, response: OK, Success (0x20)
```

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

Таким образом, осуществляется одна из простейших, но также одна из самых опасных атак на Bluetooth-устройство.

Ей подвержены следующие телефонные аппараты: Ericsson R520m, T39m, T68, Sony Ericsson T68i, T610, Z1010, Nokia 6310, 6310i, 8910, 8910i.

Для того чтобы защититься от такой 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 возможности получить необходимые патчи ко всем телефонам всех производителей [2].

### Атака, использующая уязвимости OBEX FTP сервера

Атака похожа на предыдущую. В ней используется уязвимость OBEX FTP сервера, который часто устанавливается на мобильный телефон некоторых производителей.

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.

Рассмотрим простейшее приложение на C. Для его реализации злоумышленник обычно использует библиотеку ObexFTP. Алгоритм программы выглядит следующим образом (рис. 1).

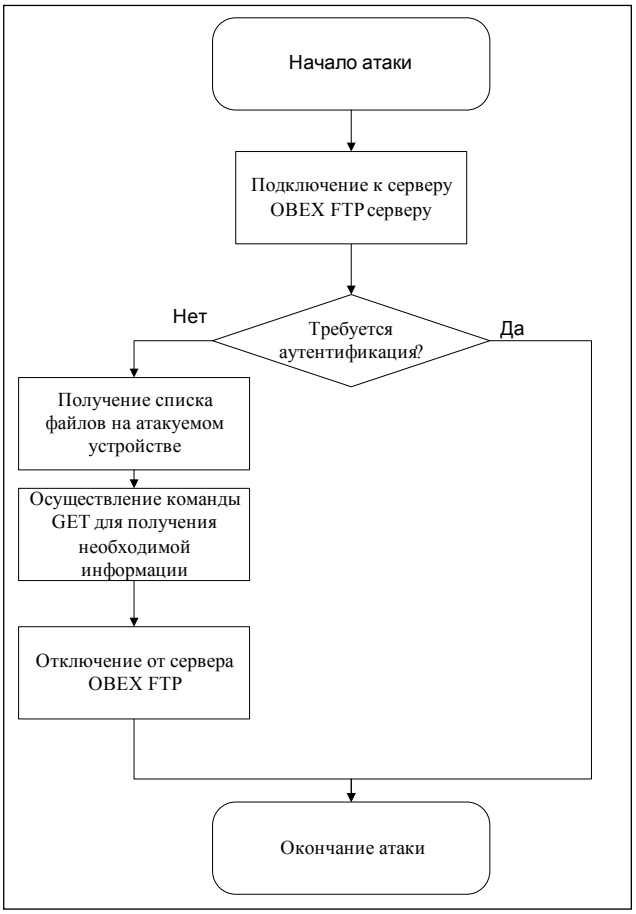


*Рис. 1. Алгоритм атаки, использующей уязвимости OBEX FTP сервера*

Для программной реализации алгоритма используется набор функций библиотеки Bluez для операционной системы типа UNIX [1].

Инициализация клиента на машине атакующего происходит с помощью следующей команды:

**obexftp_client_t *cli = NULL;**

После этого злоумышленник осуществляет открытие устройства с помощью команды obexftp_open, указывая тем самым, что будет осуществляться соединение через Bluetooth.

Полный вариант команды выглядит следующим образом:

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

Наконец, осуществляется подключение к серверу, находящемуся на мобильном телефоне. Для этого необходимо указать адрес атакуемой машины и канала, по которому работает OBEX FTP сервер:

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

Если подключение прошло успешно, выполняется, например, запрос на получение файлов на атакуемой машине с помощью команды obexftp_list:

**ret = obexftp_list(cli, NULL, pathname);**

В результате произведенных действий в буфере структуры cli (cli->buf_data) в виде строки будут располагаться файлы атакуемого устройства.

Чтобы скачать с телефона необходимый файл, можно применить команду:

**ret = obexftp_get(cli, NULL, filename);**

где в качестве параметра filename передается имя файла для похищения.

Закрытие соединения и отключение от сервера выполняются с помощью последовательности команд:

**ret = obexftp_disconnect(cli);**

**obexftp_close(cli);**

Аналогичную атаку можно провести, используя утилиту obexftp. Obexftp позволяет обращаться к профилю OPP для доступа к данным телефона.

Рассмотрим пример такой атаки:

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

Злоумышленник определил, что канал, где находится профиль OPP, имеет номер 10, и указал это в параметрах утилиты с помощью директивы channel. Адрес устройства был передан с использованием параметра -b, а указание на то, что требуется получить файл pb.vcf, выполнено с использованием директивы -g, т. е. команды GET.

Уязвимостью обладают многие телефоны: Nokia 6310, 6310i, 8910, 8910i, Sony Ericsson T68, T68i, R520m, T610, Z600 и Ericsson R520m, T39m, T68.

Для защиты от подобной атаки необходимо установить обязательную аутентификацию для OPP, после чего не следует принимать неизвестные запросы.

Таким образом, разработанный специально для Bluetooth профиль OBEX уязвим сразу для двух атак, которые дают возможность злоумышленнику полностью получить все необходимые ему данные с атакуемого устройства.

## СПИСОК ЛИТЕРАТУРЫ:

1. Networks Associates Technology, Inc. Symbian Cabir. URL: http://vil.nai.com/vil/content/v 126245.htm (дата обращения: июнь 2004 г.).

2. *Laurie B., Laurie A.* Serious flaws in bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd. URL: http://bluestumbler.org/ (дата обращения: январь 2004).