А. Г. Бельтов, И. Ю. Жуков, А. В. Новицкий

НЕАВТОРИЗОВАННОЕ ПОХИЩЕНИЕ ДАННЫХ С BLUETOOTH-УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ УЯЗВИМОСТЕЙ НА УРОВНЕ RFCOMM

Введение

Уязвимости Bluetooth-устройств дают возможность неавторизованному пользователю получить доступ к любым данным, хранящимся на мобильном телефоне. Кроме того, описываемая атака позволяет злоумышленнику выполнять с устройствами с включенным Bluetooth-передатчиком неавторизованные действия.

Атака становится возможной из-за уязвимости некоторых устройств, оснащенных функцией удаленного управления, например, с помощью беспроводной Bluetooth-гарнитуры. К сожалению, некоторые аппараты не предусматривают авторизацию этих устройств, т. е. канал (channel) в профиле для гарнитуры не защищен. А ведь именно по этому каналу гарнитура фактически осуществляет управление устройством (выполнение AT-команд). Таким образом, злоумышленник может подключиться по незащищенному каналу к устройству и осуществлять удаленное выполнение управляющих команд [1].

Техническая реализация атаки

Рассмотрим программную реализацию атаки на мобильные устройства с открытым каналом Bluetooth. Сначала программа злоумышленника получает дескриптор сокета hci_sock вызываемого устройства. Сделать это можно, используя стандартные функции библиотек для работы с Bluetooth-передатчиком в операционной системе UNIX.

После того как дескриптор получен, должна быть выполнена следующая команда:

bt_configure(dev_id, hci_sock, name);

Функция bt_configure конфигурирует сокет для установки будущего соединения таким образом, чтобы использовать уязвимость некоторых моделей телефона. Ниже приводится полный код функции:

```
int bt_configure(int dev_id, int s, char *name)
{
 struct hci_dev_req dr;
 change_local_name_cp cp;
 dr.dev_id = dev_id;
 dr.dev_opt = AUTH_DISABLED;
 if (ioctl(s, HCISETAUTH, &dr) != 0) {
  fprintf(stderr, "HCISETAUTH failed: %s\n", strerror(errno));
  return 1;
 }
 dr.dev_opt = ENCRYPT_DISABLED;
 if (ioctl(s, HCISETENCRYPT, &dr) != 0) {
  fprintf(stderr, "HCISETAUTH failed: %s\n", strerror(errno));
  return 1;
 }
 return 0;
}
```

Рассмотрим основные действия функции bt_configure. Во-первых, осуществляется установка режима работы сокета таким образом, чтобы обмен данными осуществлялся без авторизации (с помощью директивы AUTH_DISABLED). Во-вторых, отключается режим шифрования для работы с данным сокетом (директива ENCRYPT_DISABLED) [2].

После выполнения функции создается сокет для канала RFCOMM:

```
sock = socket(AF_BLUETOOTH, SOCK_RAW, BTPROTO_RFCOMM);
```

Наконец, выполняется стандартная установка связи с устройством.

Необходимо отметить важную деталь. Как уже было сказано выше, выбор канала для каждого устройства — это ключевой момент атаки. Например, для модели телефона Nokia 6310i это значение должно быть равно 13, так как именно этот канал является незащищенным для устройства и используется для управления телефоном с помощью гарнитуры.

На следующем шаге злоумышленник открывает свое устройство на запись и получает дескриптор для записи. Для простоты возьмем устройство, используемое по умолчанию для этих целей: "/dev/rfcomm" [2]:

```
rfcomm_fp = fopen("/dev/rfcomm", "r+");
```

Далее программа атакующего выполняет вызов функции bt_rfcomm_config, которая используется для создания скрытого неавторизованного канала и имеет следующий синтаксис:

```
bt_rfcomm_config(fileno(rfcomm_fp);
```

И наконец, выполняется часть программы, реализующая запрограммированные злоумышленником действия на аппарате атакуемого:

```
at_dial (rfcomm_fp, "XXXX");
```

Рассмотрим пример реализации этой функции. В данном случае она выполняет простейшее действие — вызывает набор телефонного номера, переданного злоумышленником, с машины атакуемого [1].

```
int at_dial(FILE *fp, const char *call_id)
{
 fprintf(fp, "AT");
 fprintf(fp, "D");
 sprintf(fp, "%s;", call_id);
 fprintf(fp, "\r\n");
}
```

В переданный дескриптор атакуемого устройства записывается AT-команда набора телефонного номера. После ее получения телефон жертвы инициирует вызов на указанный номер без ведома самого атакуемого.

Время атаки составляет не более 7-8 секунд.

Уязвимыми для этой атаки являются большинство аппаратов с поддержкой Bluetooth и возможностью управления при помощи гарнитуры. Тем не менее в последних моделях телефонов производители реализуют необходимую аутентификацию и для канала управления через гарнитуру. Но все же если пользователь на запрос злоумышленника о подключении к телефону по Bluetooth даст положительный ответ, то его телефон также будет поражен. В настоящее время существуют следующие телефоны, где нет никакой защиты от данного типа атак: Sony Ericsson T610, Nokia 6310 и 8910 [1].

Получив возможность удаленного исполнения AT-команд, злоумышленник может выполнить на аппарате атакуемого следующие действия:

- инициировать телефонный звонок;
- посылать SMS-сообщения на любой номер;

- читать SMS с телефона;
- читать и добавлять записи в телефонной книге;
- устанавливать переадресацию звонков.

Защититься от приведенной атаки с помощью настроек телефона или установки программного обеспечения невозможно. Решение проблемы может заключаться в усовершенствовании существующего протокола обмена данными между Bluetooth-гарнитурой и устройством, например, в разработке средства, подразумевающего введение дополнительного шифрования передаваемой информации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hermelin M. and Nyberg K.* Correlation properties of the Bluetooth combiner generator // Information Security and Cryptology, LNCS 1787. Springer-Verlag, 1999. P. 17–29.
2. *Krause M.* BDD-based cryptanalysis of keystream generators // Advances in Cryptology - EUROCRYPT'02, LNCS 1462 / L. Knudsen (ed.). Springer-Verlag, 2002. P. 222–237.