УДК 004.056.53

Исследование возможности криптоанализа беспроводной non-Bluetooth периферии

С.А. Романов[1], А.И. Шакиров[1]

[1]Московский физико-технический институт (государственный университет)

В последнее время в связи с интенсивным развитием вычислительной техники увеличилось использование беспроводной периферии. Можно выделить два основных класса беспроводной периферии Bluetooth и non-Bluetooth. В данной статье будет проведен пример криптоанализа non-Bluetooth клавиатуры. Защищенность периферийных устройств данного типа является особенно актуальной в связи с типом данных, которые могут быть доступны злоумышленнику при успешном осуществлении атаки [1]. Этими данными могут быть как пароли от различных WEB сервисов, так и возможность получения полного доступа к машине жертвы.

Целью данной работы является проведение криптоанализа non-Bluetooth клавиатуры Microsoft с помощью экономически доступного оборудования, которое свободно продается в большинстве стран мира.

Беспроводные клавиатуры обычно взаимодействуют с компьютером, используя собственные протоколы, работающие в 2,4 ГГц ISM радио диапазона. В отличие от Bluetooth, данная технология не имеет единого стандарта, которому должны были бы следовать производители, что оставляет им достаточно широкое пространство для маневра [2].

Клавиатуры передают пакет данных о нажатой клавиши специальному устройству «USB-dongle», который вставлен в USB-порт компьютера, таким же способом общаются с компьютером беспроводные мыши. В теории все пакеты должны шифроваться, но на практике оказалось, что многие производители пренебрегают шифрованием, а также отсутствует какой-либо процесс аутентификации между периферией и «USB-dongle» [3].

Выбор клавиатуры Microsoft для исследования был обусловлен тем, что они используют хорошо документированный семейство nRF24L приемопередатчиков от Nordic Semiconductor. В сети Интернет можно найти достаточно документации о работе приемопередатчика, а также о структуре пакета. Все это позволяет провести эффективный криптоанализ за короткий промежуток времени [4].

Устройство для проведения криптоанализа было собрано из следующих компонент:

1. Arduino Uno ~ 700 рублей
2. Модуль беспроводной связи nRF24L01+ ~ 240 рублей

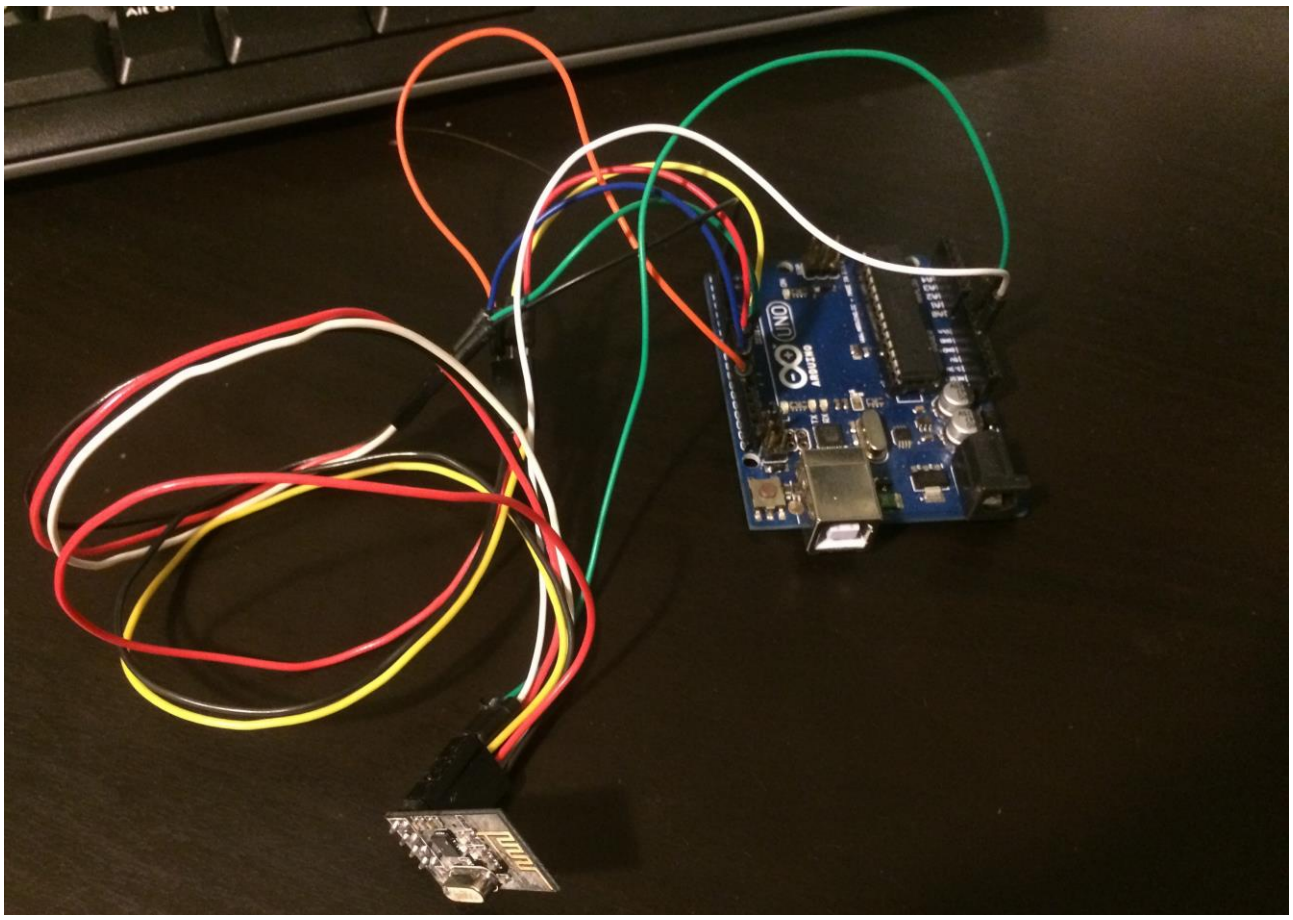
Рис. 1. Фотография полученного устройства

Основная проблема реализации сетевого анализатора заключается в том, что семейство чипов nRF24 не поддерживает promisc mode (неразборчивый режим). Однако уменьшив длину сетевого адреса в nRF24, и применив некоторые другие операции позволили реализовать promisc mode на данном чипе. Что позволило создать простой и доступный сетевой анализатор трафика для устройств, работающих на nRF24.

Однако просто сканируя частоты для нахождения пакетов клавиатуры требовалось достаточно долгое время (~2 часа). Изучив документацию по клавиатурам Microsoft было получено, что используются следующие частоты 2403 - 2480MHz, т.е. возможно использование только 78 каналов из 128, что сократило время на 40%. Далее все клавиатуры используют 2Mbps, что сократило время поиска пакетов еще на половину. Так же было найдено, что у всех клавиатур Microsoft первый бит в MAC равен 0xCD, что позволило сократить время поиска еще в пополам. А также ввести дополнительную фильтрацию пакетов. Все это позволило снизить время поиска адреса клавиатуры до 15 минут при условии ввода нескольких символов в течении 15 секунд, что является совсем небольшой величиной при условии обычной работы за компьютером.

Дальнейший анализ позволил понять структуру пакетов, которые передаются между клавиатурой и «USB-dongle». Что привело к успешному криптоанализу клавиатуры.

Рис. 2. Структура перехваченного пакета

В работе проведен успешный криптоанализ non-Bluetooth клавиатуры Microsoft с помощью экономически доступного оборудования (менее 15 долларов США), которое свободно продается в большинстве стран мира. Исследуемые клавиатуры Microsft подвержены как sniffing, так и инъекции пакетов.

Литература

1. *С. А. Круглик* [*и др.*] Практическая реализация атаки «человек посередине» на сопрягаемые Bluetooth-устройства на примере беспроводной клавиатуры // ТРУДЫ МФТИ. — 2014. — Том 6. – 1934. – Т. 5, № 4. – С. 111–118.
2. *М. Нефёдова* MouseJack — новая атака на беспроводной мыши // Журнал Хакер — февраль 2016
3. *Marc Newlin* — MouseJack: Injecting Keystrokes into Wireless Mice // DEF CON 24 Hacking Conference
4. *А. Гарипов* — Перехват беспроводных гаджетов — от квадрокоптеров до мышек // Международный форум по практической безопасности Positive Hack Days VI