Secure Systems & Network Engineering

Advanced Security

Lab 1 Bluetooth

Bimaganbetov Bagdat, Grebennikov Sergey,
Sharafitdinova Iuliia

January 23, 2018

Bluetooth mitm proxy

Question 1

What kind of mitm proxies are out there?

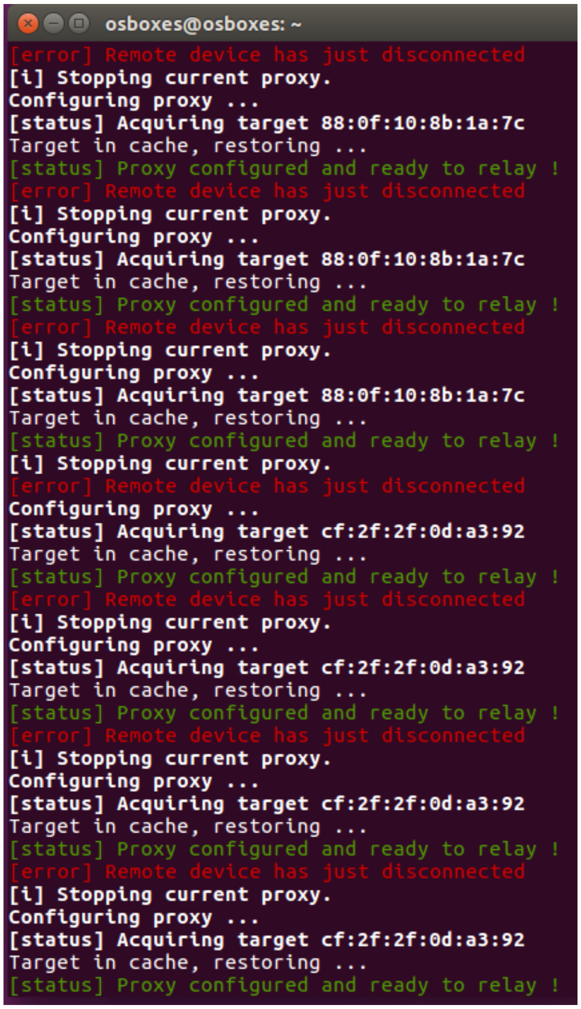
Answer

There are the following Bluetooth mitm proxies:

- **Btproxy**. The program allows performing Man-in-the-Middle attack on Bluetooth devices, but this program doesn't yet have support for Bluetooth Low Energy.
- **BtleJuice**. The program is a complete framework to perform Man-in-the-Middle attacks on Bluetooth Smart devices (also known as Bluetooth Low Energy).
- **Gattacker**. A Node.js package for BLE (Bluetooth Low Energy) Man-in-the-Middle.

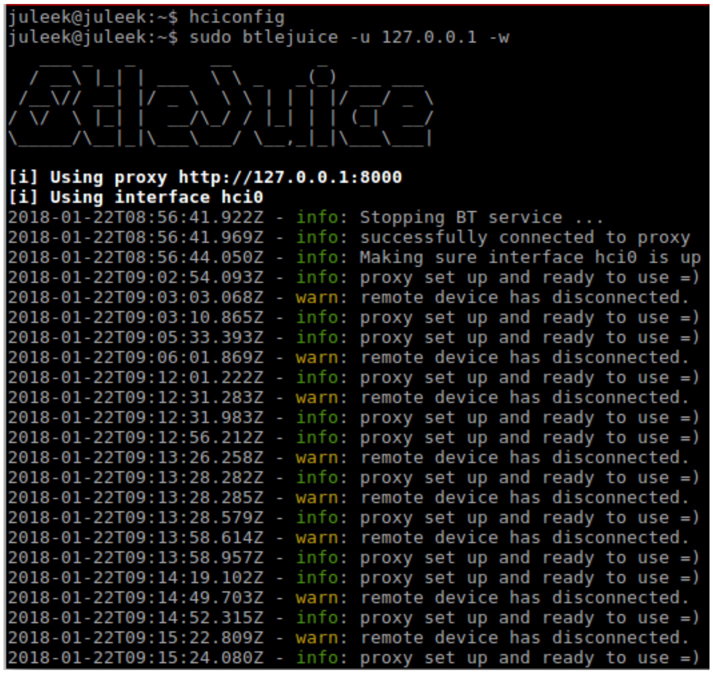
We have tried to make MITM attack on Bluetooth Smart devices but devices that we have are safer. For this attack we used **BtleJuice** framework (Figure 1, 2) and **Gattacker** package (Figure 3).

Figure 1: BtleJuice



```
[error] Remote device has just disconnected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target 88:0f:10:8b:1a:7c
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
[error] Remote device has just disconnected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target 88:0f:10:8b:1a:7c
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
[error] Remote device has just disconnected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target 88:0f:10:8b:1a:7c
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
[i] Stopping current proxy.
[error] Remote device has just disconnected
Configuring proxy ...
[status] Acquiring target cf:2f:2f:0d:a3:92
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
[error] Remote device has just disconnected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target cf:2f:2f:0d:a3:92
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
[error] Remote device has just disconnected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target cf:2f:2f:0d:a3:92
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
[error] Remote device has just disconnected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target cf:2f:2f:0d:a3:92
Target in cache, restoring ...
[status] Proxy configured and ready to relay !
```

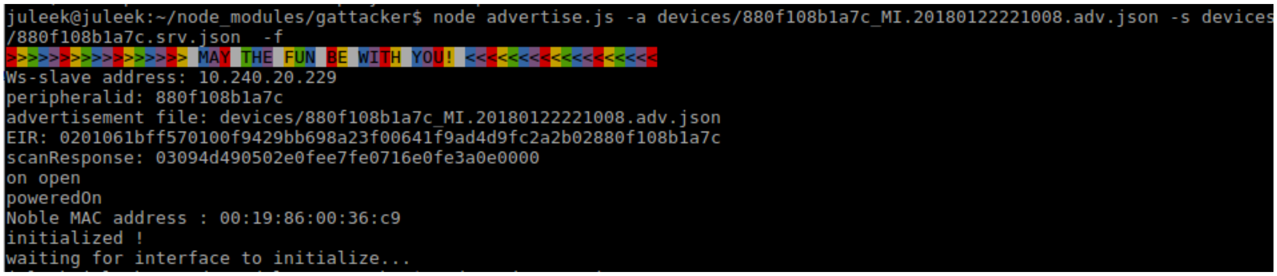
Figure 2: BtleJuice



```
juleek@juleek:~$ hciconfig
juleek@juleek:~$ sudo btlejuice -u 127.0.0.1 -w
   ___ _   _         __       _
  / __\ |_| | ___    \ \_   _(_) ___ ___
 /__\// __| |/ _ \    \ \ | | | |/ __/ _ \
/ \/  \ |_| |  __/ /\_/ / |_| | | (_|  __/
\_____/\__|_|\___| \___/ \__,_|_|\___\___|

[i] Using proxy http://127.0.0.1:8000
[i] Using interface hci0
2018-01-22T08:56:41.922Z - info: Stopping BT service ...
2018-01-22T08:56:41.969Z - info: successfully connected to proxy
2018-01-22T08:56:44.050Z - info: Making sure interface hci0 is up
2018-01-22T09:02:54.093Z - info: proxy set up and ready to use =)
2018-01-22T09:03:03.068Z - warn: remote device has disconnected.
2018-01-22T09:03:10.865Z - info: proxy set up and ready to use =)
2018-01-22T09:05:33.393Z - info: proxy set up and ready to use =)
2018-01-22T09:06:01.869Z - warn: remote device has disconnected.
2018-01-22T09:12:01.222Z - info: proxy set up and ready to use =)
2018-01-22T09:12:31.283Z - warn: remote device has disconnected.
2018-01-22T09:12:31.983Z - info: proxy set up and ready to use =)
2018-01-22T09:12:56.212Z - info: proxy set up and ready to use =)
2018-01-22T09:13:26.258Z - warn: remote device has disconnected.
2018-01-22T09:13:28.282Z - info: proxy set up and ready to use =)
2018-01-22T09:13:28.285Z - warn: remote device has disconnected.
2018-01-22T09:13:28.579Z - info: proxy set up and ready to use =)
2018-01-22T09:13:58.614Z - warn: remote device has disconnected.
2018-01-22T09:13:58.957Z - info: proxy set up and ready to use =)
2018-01-22T09:14:19.102Z - info: proxy set up and ready to use =)
2018-01-22T09:14:49.703Z - warn: remote device has disconnected.
2018-01-22T09:14:52.315Z - info: proxy set up and ready to use =)
2018-01-22T09:15:22.809Z - warn: remote device has disconnected.
2018-01-22T09:15:24.080Z - info: proxy set up and ready to use =)
```

Figure 3: Gattacker



```
juleek@juleek:~/node_modules/gattacker$ node advertise.js -a devices/880f108b1a7c_MI.20180122221008.adv.json -s devices
/880f108b1a7c.srv.json  -f
>>>>>>>>>>>>>>>> MAY THE FUN BE WITH YOU! <<<<<<<<<<<<<<<<
Ws-slave address: 10.240.20.229
peripheralid: 880f108b1a7c
advertisement file: devices/880f108b1a7c_MI.20180122221008.adv.json
EIR: 0201061bff570100f9429bb698a23f00641f9ad4d9fc2a2b02880f108b1a7c
scanResponse: 03094d490502e0fee7fe0716e0fe3a0e0000
on open
poweredOn
Noble MAC address : 00:19:86:00:36:c9
initialized !
waiting for interface to initialize...
```

Question 2

How can you use a man in the middle tool to provide insight in the communication?

Answer

Most mobile applications initiate a connection to the device by searching for advertisements transmitted by the device. Typically, LE devices optimize advertising intervals to minimize energy consumption. However, an attacker can broadcast relevant advertisements at minimal intervals (much faster than the original device). The mobile application will interpret the first advertisement received, and in this case it will most likely be fake.

The tool used creates an exact copy of the attacked device in the Bluetooth layer, and then deceptions the mobile application to interpret its broadcast messages and connect to it instead of the original device. Also it continues to actively connect to the device and sends it data exchanged with the mobile application. Thus, acting as MITM, you can intercept and/or change sent requests and responses.

Question 3

Would it be possible to modify the content of the transmission?

Answer

In short - yes. The MITM attacker node is behaving like the original node and it can modify the data between source and destination nodes. The sender node does not know that the receiver is attacker and it trying to access or modify the message. Also receiver node does not check neither the sender, nor the received data. Thus, the attacker controls the entire communication.