Man in the middle analysis and btproxy

Conor Patrick
2015

What is a mitm

Large scale:

- DNS cache poisoning
- IP/BGP hijacking

Proximity:

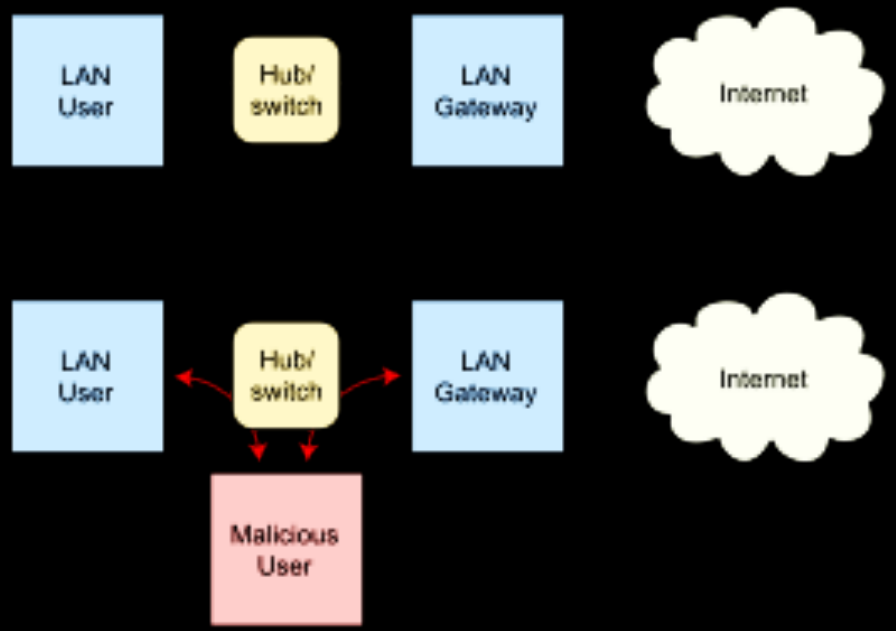
- ARP spoofing
- WiFi Spoofing

ARP Spoofing

1. Tell target that your mac address is the same as the gateway

2. Tell gateway that your mac address is the same as the target

3. Forward packets actively



Bad access points, bad VPNs

https://www.hokieprivacy.org/wifi/

VT Wireless uses TLS, resistant to eavesdropping.

But TLS validation is often improperly validated on devices.

TLS validation authenticates that VT-Wireless is official

Is anyone other than VT mitm'ing your traffic?

Alpha cards, Pineapple card

Why a mitm?

Black hat:

- Steal sensitive information
- Deceive people into logging into fake services

White hat:

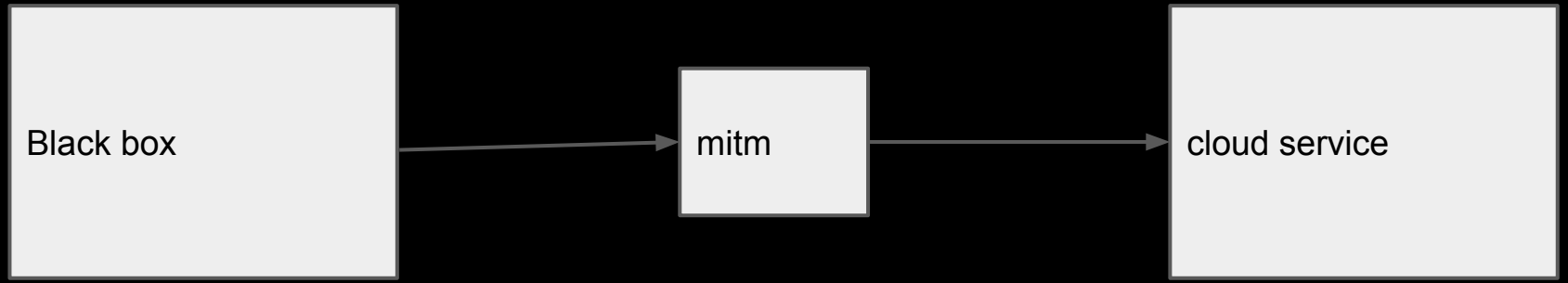
- Incredible useful for security analysis
- Allows black box type of analysis or fuzzing

Example

Hacking Face.com

http://ashkansoltani.org/2012/06/18/facepalm/

Get a Facebook OAuth token for any user ID from Face.com

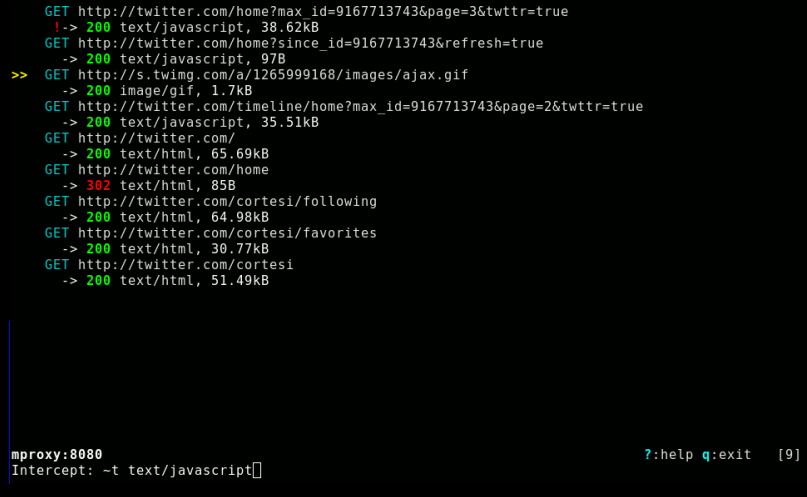


Demo time mitmproxy

Mitm proxy is a interactive headless HTTP proxy

Actively man in the middles traffic and will serve fake CA certs.

Allows manipulation of the packets and scripting



Run through with random app from product hunt

Tripomatic

Can you find the vuln?

btproxy: mitm tool for Bluetooth

https://github.com/conorpp/btproxy

Leverages 1 - 2 Bluetooth adapters

Clones 1- 2 devices to try to spoof them

Open sockets for all advertised services on the slave device

Actively forwards traffic between paired devices

Other solutions

Passive solutions only!

Demo on Pebble

Setbacks

Bluetooth LE doesn’t work (yet)

This is only viable as an analysis tool, not for attacking.

Attacks may be viable with forced disconnects via jamming. Jamming functionality has recently been added to the Ubertooth.

See Hacking an Electric Skateboard

http://www.wired.com/2015/08/hackers-can-seize-control-of-electric-skateboards-and-toss-riders-boosted-revo/