Man in the middle analysis and btproxy

Conor Patrick
2015

What is a mitm

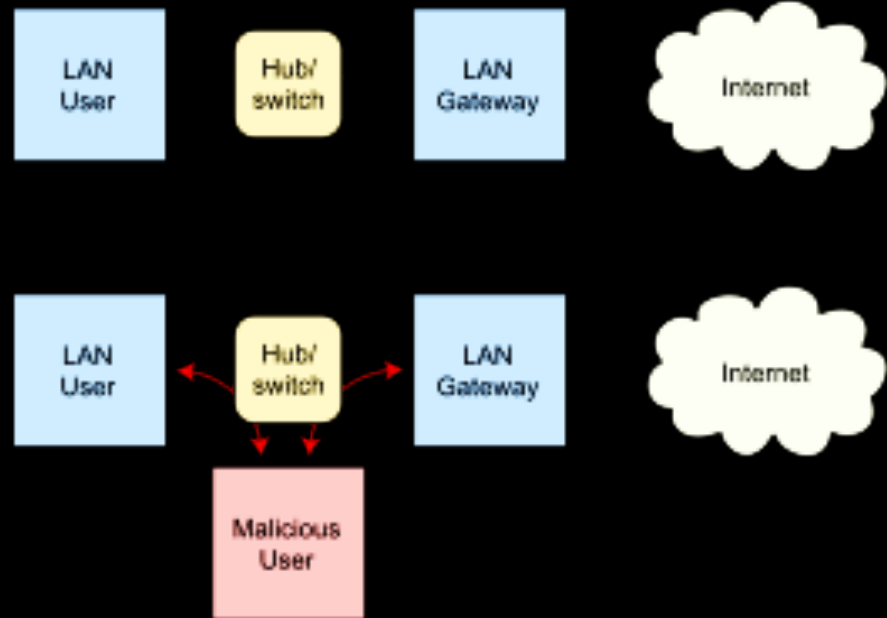Large scale:

 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
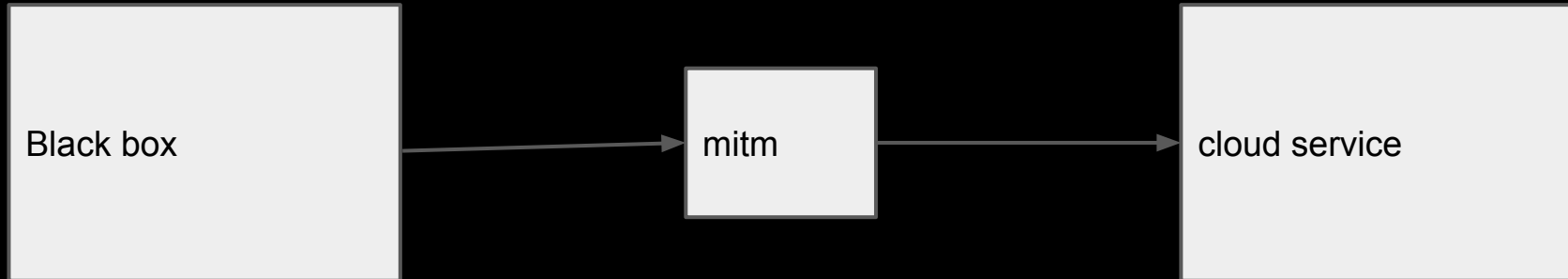
      Allows black box type of analysis or fuzzing

Example

Hacking Face.com

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

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

```
┌─────────────┐         ┌──────────┐         ┌───────────────┐
│             │         │          │         │               │
│             │         │          │         │               │
│ Black box   │────────▶│   mitm   │────────▶│ cloud service │
│             │         │          │         │               │
│             │         │          │         │               │
└─────────────┘         └──────────┘         └───────────────┘
```

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

```
   GET http://twitter.com/home?max_id=9167713743&page=3&twttr=true
   !-> 200 text/javascript, 38.62kB
   GET http://twitter.com/home?since_id=9167713743&refresh=true
    -> 200 text/javascript, 97B
>> GET http://s.twimg.com/a/1265999168/images/ajax.gif
    -> 200 image/gif, 1.7kB
   GET http://twitter.com/timeline/home?max_id=9167713743&page=2&twttr=true
    -> 200 text/javascript, 35.51kB
   GET http://twitter.com/
    -> 200 text/html, 65.69kB
   GET http://twitter.com/home
    -> 302 text/html, 85B
   GET http://twitter.com/cortesi/following
    -> 200 text/html, 64.98kB
   GET http://twitter.com/cortesi/favorites
    -> 200 text/html, 30.77kB
   GET http://twitter.com/cortesi
    -> 200 text/html, 51.49kB
```

```
mproxy:8080                                          ?:help q:exit   [9]
Intercept: ~t text/javascript
```

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

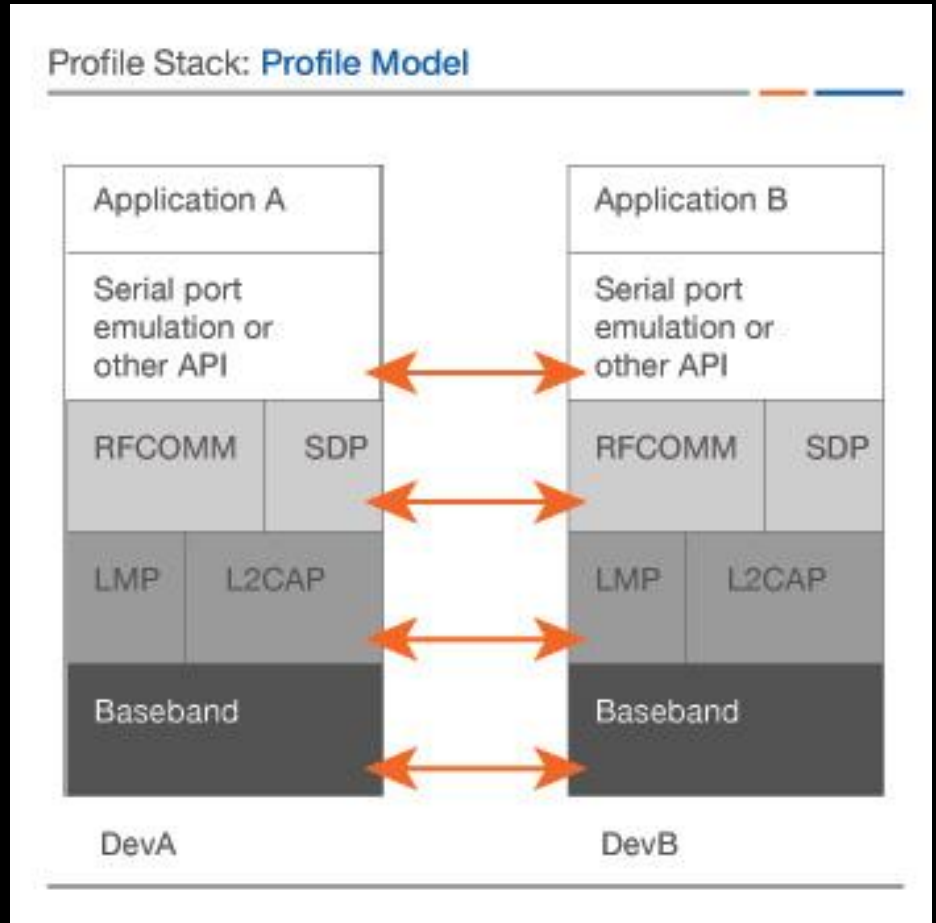Actively forwards traffic between paired devices

Other solutions

Passive solutions only!

L2CAP is like UDP

RFCOMM is like TCP

SDP runs on L2CAP port 1

btproxy opens a new socket for all other services (RFCOMM/L2CAP) on slave.

Profile Stack: **Profile Model**

| Application A | Application B |

Serial port emulation or other API

RFCOMM | SDP

LMP | L2CAP

Baseband

DevA

DevB

Demo btproxy on Pebble
Show connection hijacking vuln

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/