Introduction To MitM

PRESENTED BY:
Tim Wilkes

Who am I?

- Tim Wilkes
- Ex- Unix Sys Admin for various Web companys / ISPs / Telecos
- @Timmehwimmy on Twitter
- I tinker with things

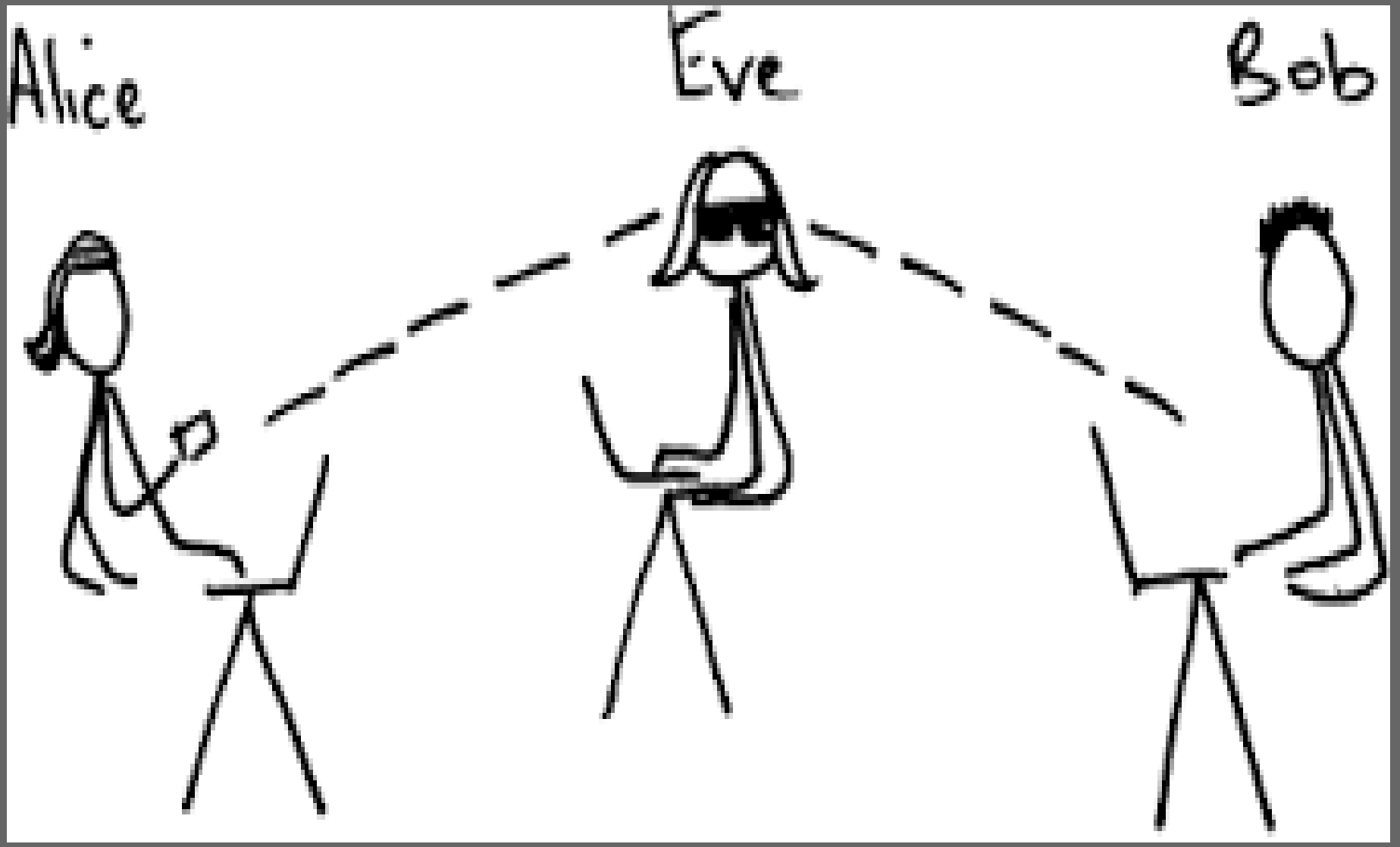
Disclaimer: Please don’t be a dick. I accept not responsibility.
Ever.
For Anything.

What is MitM?

- From Wikipedia:

  In computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

The world’s oldest love triangle



Quick Question

- So, What do the following have in common?
  - Languages / Dialects
  - Caesar Cipher
  - Wax

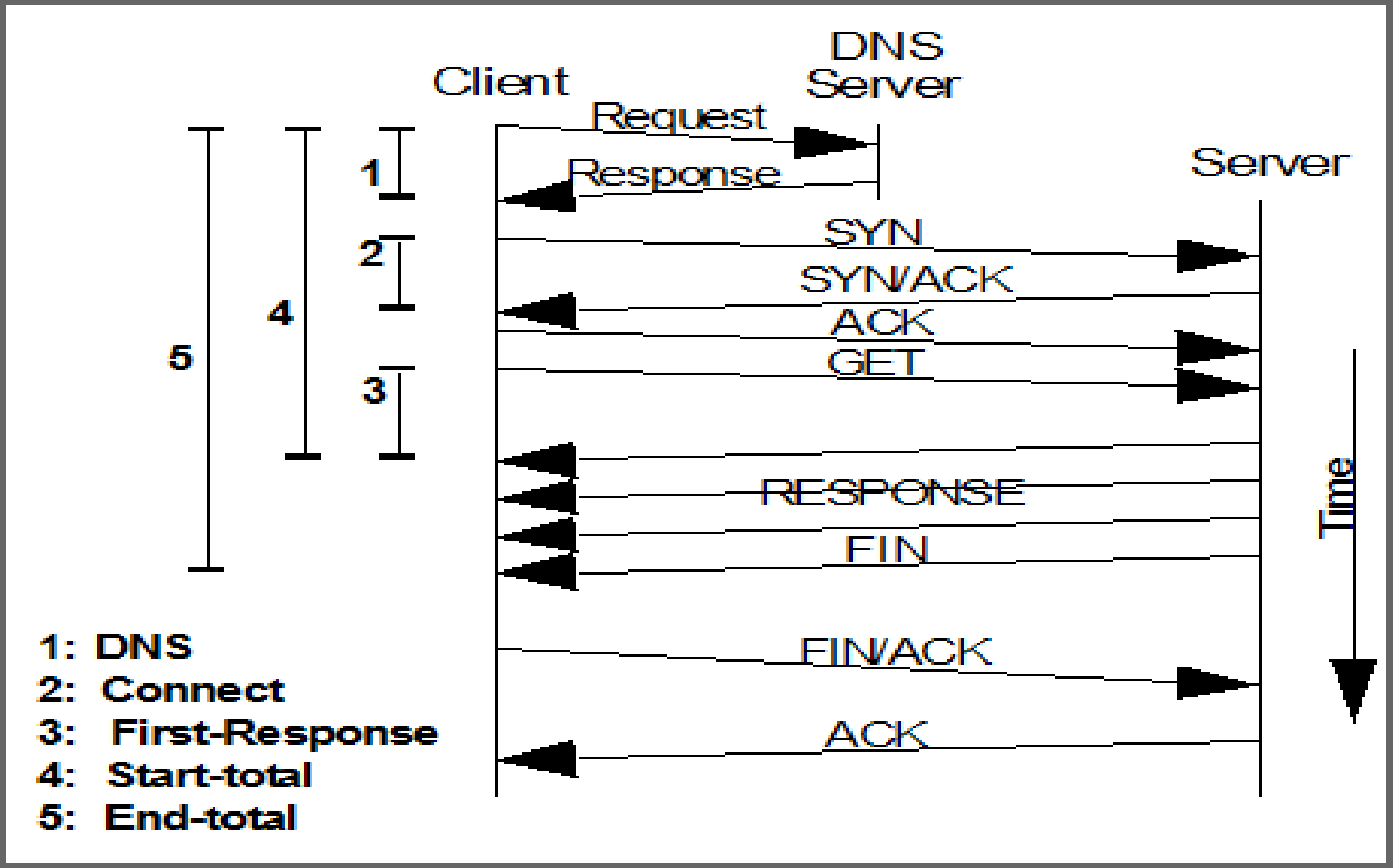
Quick Answer

- All aim to defeat MitM attacks.
  - Language / Dialects – Stop people eavesdropping, Eg. Cockney Rhyming Slang
  - Caesar Cipher – Moving characters on 4 places, Encryption
  - Wax – Used in seals form impressions to verify the sender, and is unread – IE, Signature

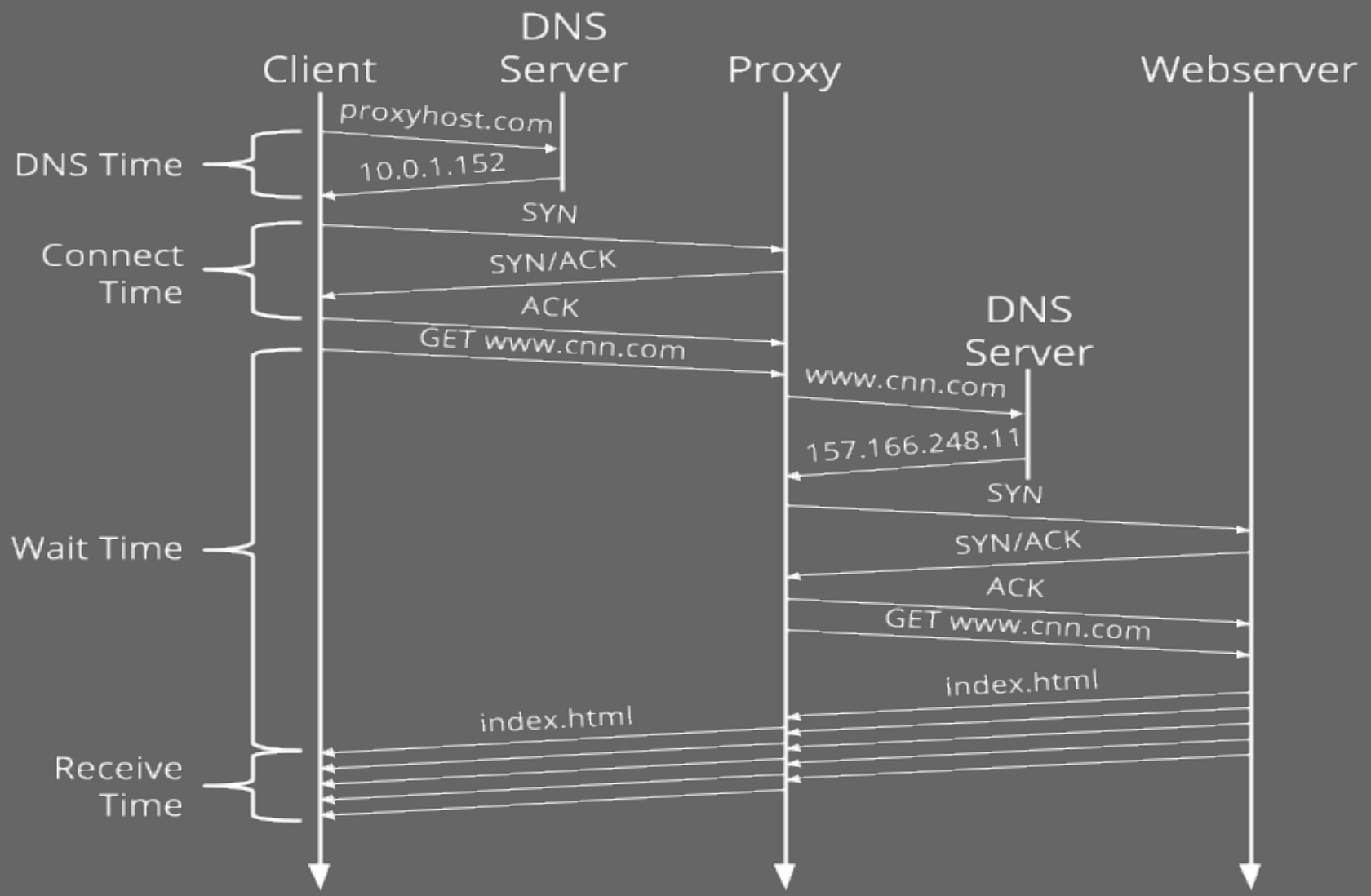
Why MitM?

- Web Caching
- Software testing
- Anti-Virus
- IDS / IPS
- Bad things...
  - Back door injection
  - Manipulating web pages
  - Turning the Internet upside down.

Quick guide to how the Internet works...



Internet With a Proxy



Where do you MitM?

- In the middle of what?
  - The Host? Local Proxy
  - The Switch network? Aren’t switches meant to prevent this?
  - The Router? Could be a wifi router
  - Anywhere as long as it is between the two parties.

How do I Mitm?

- Insert yourself (or a computer) in the network.
- Act as a gateway / DNS server.
- Decide what traffic you want to intercept
  - Start off with Wireshark / tcpdump ?
  - Application specific proxy / Alternative service

Demos (aka squeaky bum time)

- Burpsuite (Web Proxy)
  - CTF
- Mitmf (Man In the Middle Framework)
  - Upsidedownternet

Ok, so how do I get in the middle?

- To recap, we can manipulate the data once we see it.
  - Using STARTTLS won’t help – IE, Opportunistic Encryption.
  - We can simple block the starting commands.

What about Switches ?

- Surely they prevent traffic being seen by other devices?
- Be on a different switch / vlan?
- Yersinia
  - DTP – Dynamic Trunking Protocol
  - BPDU (Bridge Protocol Data Unit) spoofing
- DSniff
  - Floods the mac address table
  - Forces switch to act like a hub

Prevention

- Don’t let nasty people plug in to your network...
- Physical security
- Rate limit MAC addresses
- Encryption
- BPDU Guard

DHCP Server

- If you are on the layer 2 network, run your own!
- Easy to set up
- Just set yourself as the router.

DHCP Server prevention

- DHCP Snooping
- Certain switches can prevent this by not allowing certain ports to send DHCP Offers.

ARP Spoofing

- Changes the layer 2 mapping between MAC addresses and IP address.
- Easy to achieve
- Assumes you are on the same VLAN

ARP Spoofing Prevention

- DHCP Snooping and DAI (Dynamic ARP Inspection) enabled on Cisco kit
- ARP Rate limiting.
- Don’t let the people on the vlan?

Layer 2 Tools

- DHCP Servers
  - ISC DHCPd
- ARP spoofing
  - Yersinia (STP Packets)
  - Ettercap (with plugins)

Hardware Show and tell...

- Lan Turtle
- Wifi Pineapple Mk4
- Wifi Pineapple MK5

Layer 3 Tools

- Any OS capable of routing traffic
- Way to divert traffic (Eg, IPTables)
- DNS Responder (Eg, DNS Masq)
- A way to host your proxy

Other Tools

- Squid (yes the web cache)
- SSLStrip / SSLSplit
- NetSed – Like sed, but for streams
- Scapy (ie, write your own)
- ...

Prevention

- Encryption
- Security headers on websites
  - HSTS
  - HPKP
- Don’t connect to shoddy wifi (ever!)

Nation States and Organized Criminals

- Mess with BGP Routing
  - Google (in South America) diverted for several minutes
- Mess with DNS Registrars
  - Criminals did this to a Brazilian bank
  - Used Lets encrypt to provide SSL Certs for proxies.

BGP

- Routes the internet
- Requires Peers to co-operate
- Not authenticated
- You can just inject routes
- Fixes are coming

So, How do I rob a bank with this?

- https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/
-

ANDY GREENBERG SECURITY 04.04.17 10:52 AM

HOW HACKERS HIJACKED A BANK'S ENTIRE ONLINE OPERATION

GETTY IMAGES

THE TRADITIONAL MODEL of hacking a bank isn't so different

How do I stop the bank robbers?

- HPKP
  - But it’s not for the faint of heart.

Questions?

CONTACT:
mitm@php-systems.com