**Network Isolation: IoT, Arp and Switches**

**Network isolation** is physically or logically putting devices on different networks to control which devices can communicate with each other

Are there untrusted devices on your network?

* Guests
* Family members who aren’t as secure as you
* Are any of the devices not up to date (patched)
* IoT devices: set-top box, lightbulbs, smart-TV

**IoT devices are a growing target for attacking local networks**

US Director of National Intelligence:

“In the future, intelligent services may use the IoT for identification, surveillance, monitoring, location tracking and targeting for recruitment, or to gain access to networks or user credentials”

What can an attacker do when on the network

* Local traffic sniffing/spoofing
* MITM attacks, inject and manipulate traffic e.g., SSL Stripping, inject code into HTTPS
* Attacking devices directly through open services and ports

**Arp Spoofing & Switches**

**Switches**

* Where the network cables are plugged in in the router
* Keep a table of ethernet MAC address (MAC tables)
* Uses the addr to send traffic from unique devices to its destination
* Works at data link layer (layer 2)

Once data is travelling in the local network, IP addr aren’t used, MAC aaddr are used for traffic to find its way to the local network

Ips get used for the internet through a router device

**Isolated collision domain**

When data is passed through a network, the switch knows what MACaddr the data is supposed to go

This means that the data is physically sent over one wire specific to the destination device using the MAC addr

* No other device on the local network will receive this data

An ethernet switch is easy to infiltrate as a MITM can pretend to be the router gateway

**Arp**

Address resolution protocol

* IP to MAC resolution
* Resolves network layer IP into data link layer MAC addresses
  + Arp -a, shows the arp cache or arp table for this device

TuxCut

NetCut

* Perform DoS attacks using arp protocol
* Can also protect you against such attacks