KRU6HFGZ

PEN TESTING: CONTROLLING THE NETWORK

Tom Chothia

KRU6HFGZ

Monday's Exercise

- Most common ways to defend a network
- Thinking about how a network can be attacked.
- Practice in making though choices.
- Not really any wrong of right answers.
- Game code is on the Canvas page.

KRU6HFGZ

Next Exercise

- On Monday we will hand out devices for the next team pen testing exercise.
- Sign up for teams of 5 or 6 on Canvas now,
  - all unassigned people who did Monday's exercise will be randomly added to teams on Monday morning.
- 5 week exercise, you must start as soon as you get the device.
- Monday 5th Feb. will be a 2 hour help sessions, bring your device.

KRU6HFGZ

This Lecture

- The Internet and some tools:
  - nmap
  - WireShark
- The TLS protocol
- Evesdropping and MITMing network traffic

KRU6HFGZ

The Start 1969

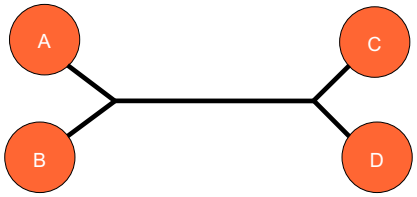
The US Defense Advanced Research Projects Agency (then ARPA now DARPA) gives research grants to universities to buy computers.

They decide to link their computers.

But how?

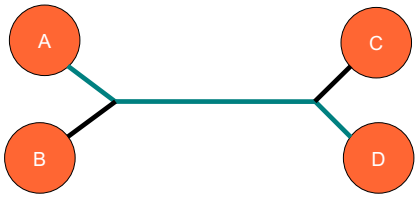
KRU6HFGZ

The Problem With Leased Lines



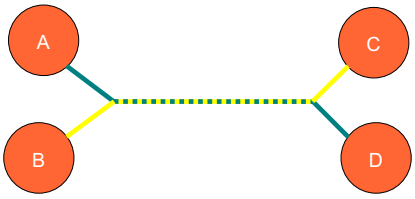
KRU6HFGZ

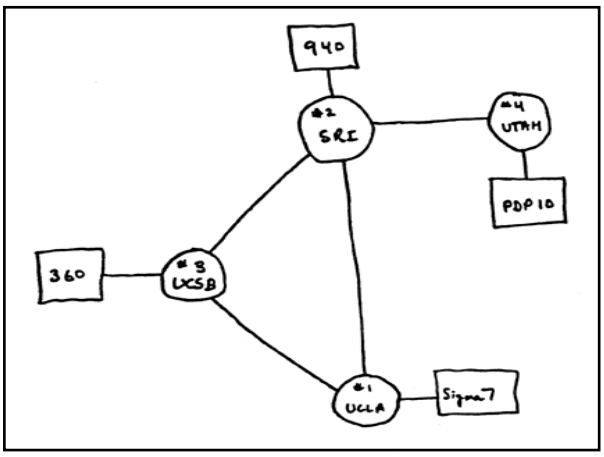
If A and D use the line, then C and B can't

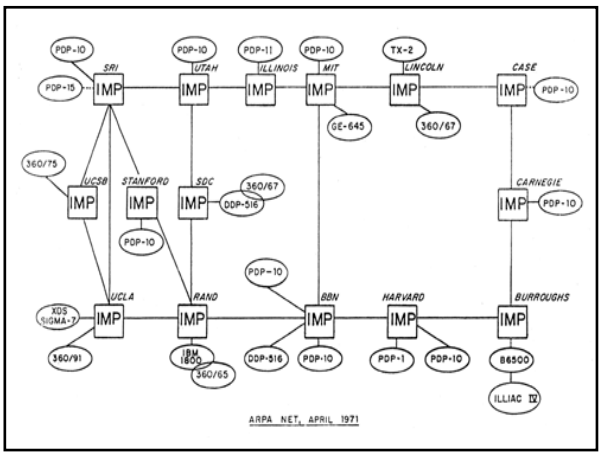


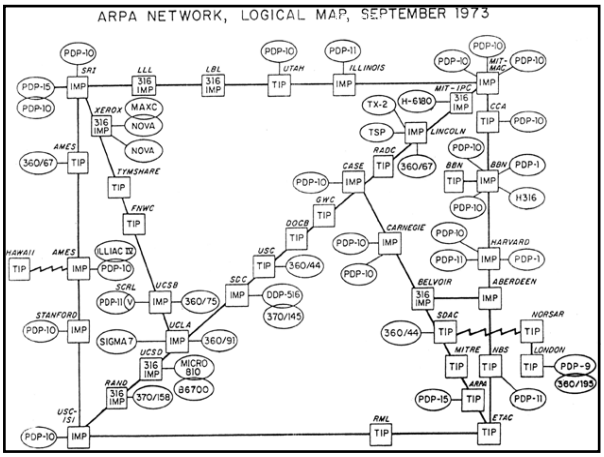
KRU6HFGZ

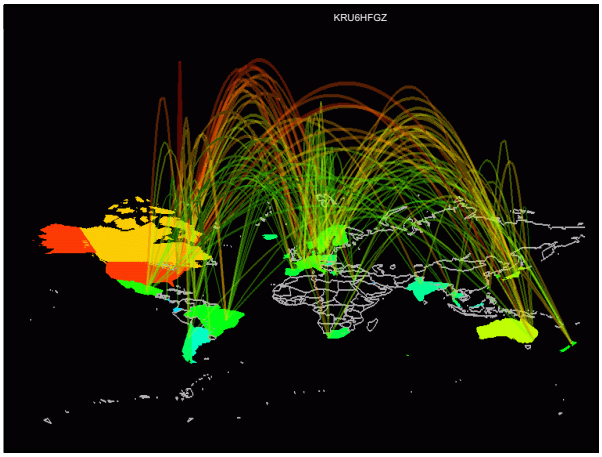
But if everyone just sends a small packet of data, they can both use the line at the same.

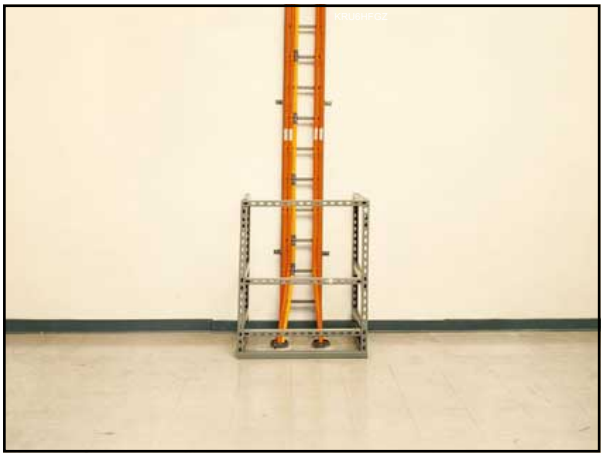












Birmingham to the Washington Post

```
wallace% traceroute washingtonpost.com
traceroute to washingtonpost.com (54.231.80.90), 30 hops max, 60 byte packets
 1  hawke-rw.cs.bham.ac.uk (147.188.193.6)  28.253 ms  28.237 ms  28.229 ms
 2  * * *
 3  hscn-gw.cs.bham.ac.uk (147.188.199.1)  1.129 ms  1.336 ms  1.324 ms
 4  cs-ac00b7e1-2.bham.ac.uk (147.188.121.129)  0.718 ms  1.020 ms  1.046 ms
 5  cs-cc00-ve701.bham.ac.uk (147.188.123.57)  0.991 ms cs-cc000-tb.bham.ac.uk
 6  fw-sr000-trust.bham.ac.uk (147.188.123.9)  0.917 ms  0.525 ms  0.844 ms
 7  gw-sr001-ve10.bham.ac.uk (147.188.123.5)  0.835 ms  0.833 ms  1.391 ms
 8  193.63.208.141 (193.63.208.141)  1.731 ms  1.734 ms  1.722 ms
 9  te2-2.wolv-rbr1.wmrn.ja.net (193.62.80.173)  216.602 ms  216.631 ms  216.6
10  ae1.birmub-rbr1.wmrn.ja.net (193.62.80.153)  2.515 ms  2.494 ms  2.418 ms
11  ae23.erdiss-sbr1.ja.net (146.97.37.153)  24.962 ms  24.630 ms  24.610 ms
12  ae29.manckh-sbr1.ja.net (146.97.33.42)  4.677 ms  4.754 ms  4.784 ms
13  port-channel205.car1.Manchester1.Level3.net (195.50.119.97)  67.868 ms  64.
14  ae-1-60.edge3.Washington1.Level3.net (4.69.149.17)  84.511 ms ae-4-90.edge
15  AMAZON.COM.edge3.Washington1.Level3.net (4.59.144.174)  84.429 ms  84.272
16  72.21.220.131 (72.21.220.131)  85.204 ms 72.21.220.123 (72.21.220.123)  85.
17  205.251.245.168 (205.251.245.168)  85.329 ms  85.802 ms  86.399 ms
```

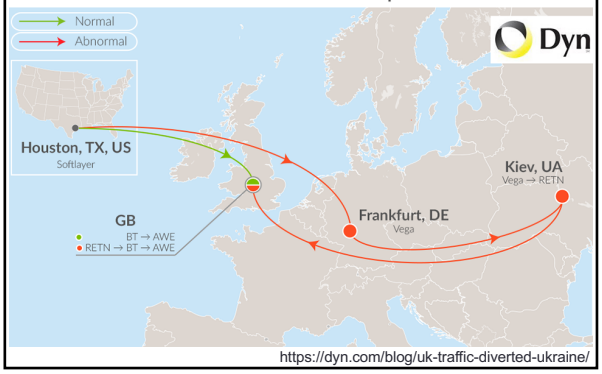

BT and Vodafone among telecoms companies passing details to GCHQ

Fears of customer backlash over breach of privacy as firms give GCHQ unlimited access to their undersea cables

The document identified for the first time which telecoms companies are working with GCHQ's "special source" team. It gives top secret codenames for each firm, with BT ("Remedy"), Verizon Business ("Dacron"), and Vodafone Cable ("Gerontic"). The other firms include Global Crossing ("Pinnage"), Level 3 ("Little"), Viatel ("Vitreous") and Interoute ("Streetcar"). The companies refused to [illegible] on any specifics relating to Tempora, but several noted they were obliged to comply with UK and EU law.

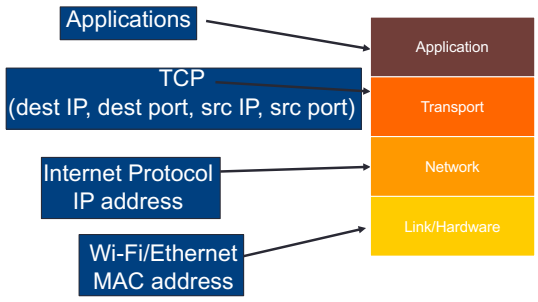
- http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

Redirected traffic to UK Atomic Weapons Establishment



https://dyn.com/blog/uk-traffic-diverted-ukraine/

The Stack, Most of the Time:



Nmap: http://nmap.org/

Check if 1000 most common ports are open:

```
nmap 127.0.0.01
```

Additionally send messages to ports to find out what the service is:

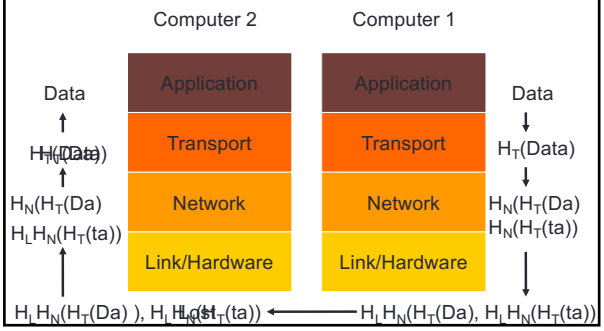
```
nmap -A 127.0.0.01
```

Scan all ports

```
nmap -p- 127.0.0.01
```

KRU6HFGZ

Using the Stack to Send Data



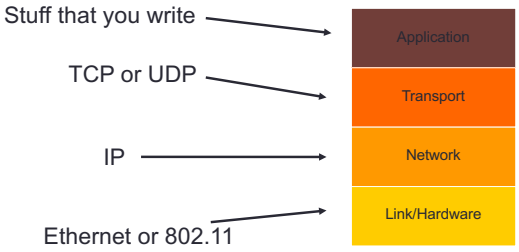
KRU6HFGZ

WireShark www.wireshark.org

- A network protocol analyzer: It records all Internet traffic, so it can then be viewed and analysed.
- Excellent for debugging protocols and network problems
- See also tcpdump, which writes packets directly to disk.

KRU6HFGZ

The Internet Protocol Stack, (Most of the Time):



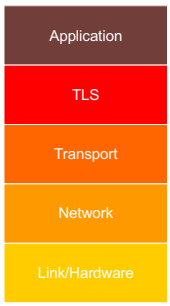
KRU6HFGZ

The Internet Protocol Stack with TLS

The TLS layer runs between the Application and Transport layer.

The encryption is transparent to the Application layer.

Normal TCP and IP protocols etc. can be used at the low layers



KRU6HFGZ

Self signed certificates

- Maintaining a set of certificates is hard (especially on apps and IoT devices).
- It's much easier just to accept any certificate, (or certificates that sign themselves).
- If the client accepts the self signed certificates then it's easy to man-in-the-middle.
- This has been shown to happen a lot in devices and code that uses TLS!

KRU6HFGZ

Using your own certificate

- If you can add your own certificate to the trust store of the device you can MITM TLS traffic.
- Easy to do on a laptop or routed phone.
- Some apps may be programmed to only accept a particular TLS cert.
  - This is called certificate pinning.
- In this case the app needs to be patched to remove this or use an certificate you control.
- More about this next week.

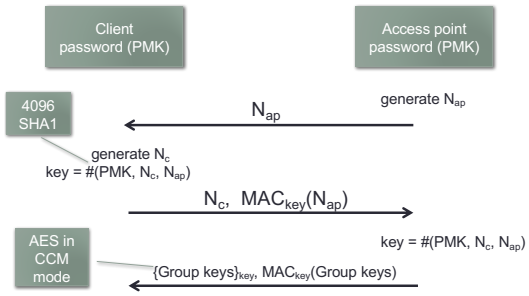
KRU6HFGZ

WPA2 wi-fi security

- First wi-fi protocol: WEP completely broken.
- Second wi-fi protocol: WPA used own cipher, broken
- Third protocol WPA2 uses AES in CCM mode. Secure.
- Security is based on a password known to the wi-fi base station and the client.
- Runs on top of wireless protocol 802.11

KRU6HFGZ

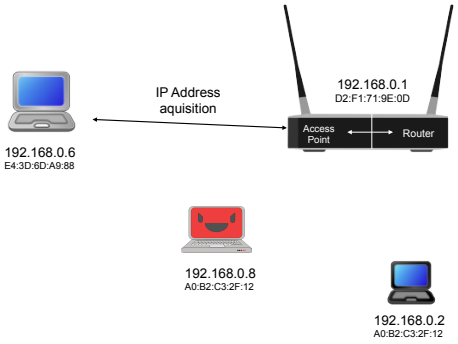
Simplified WPA

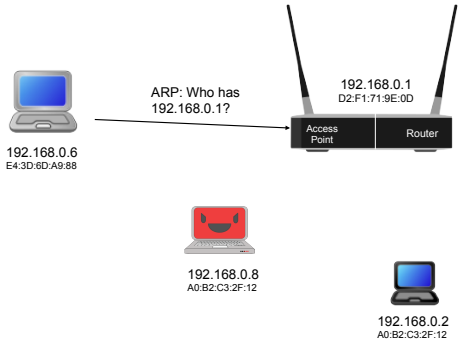


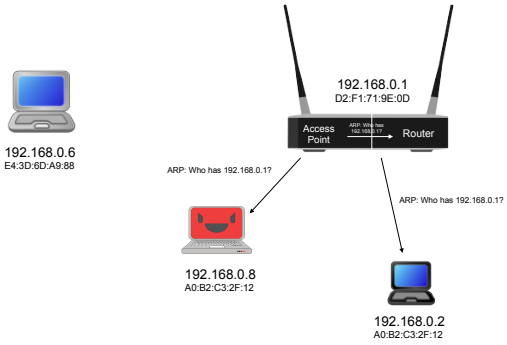
KRU6HFGZ

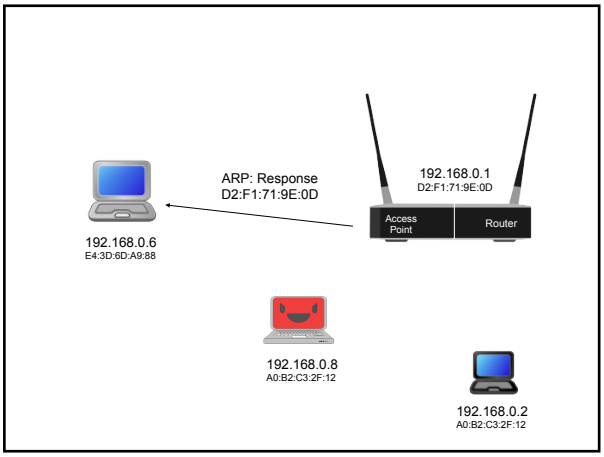
Decrypting WPA with Wireshark

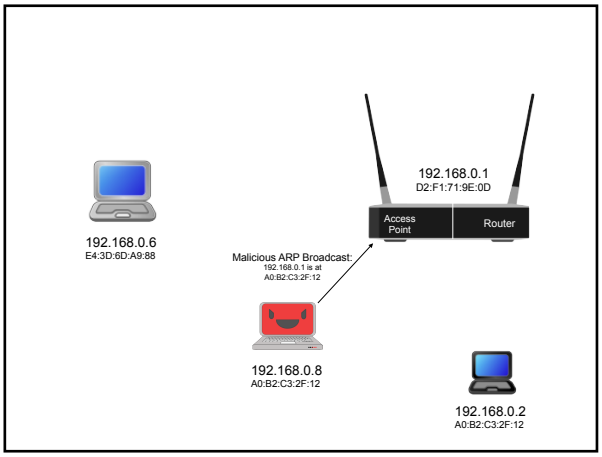
- nonce (in 4-way handshake), + password + SSID gives you the key
- If you tell wireshark the password and SSID it will decrypt WPA traffic.
- Remember the each client has a different key.
- More details here: https://wiki.wireshark.org/HowToDecrypt802.11

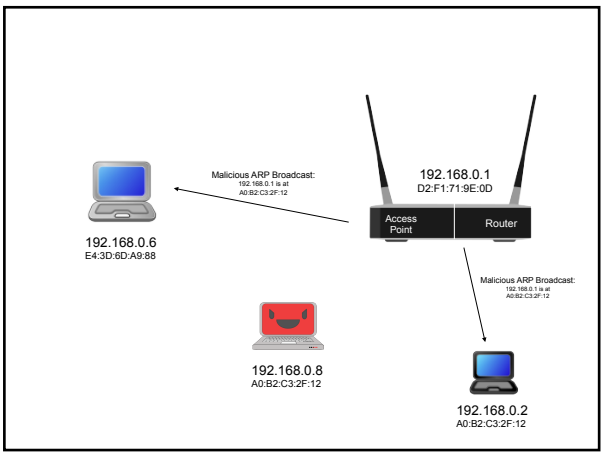


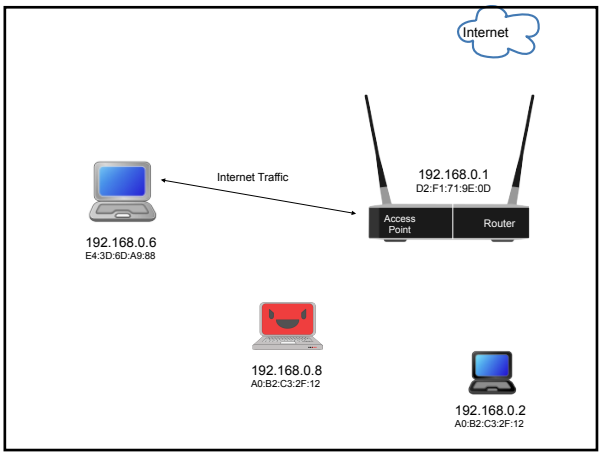


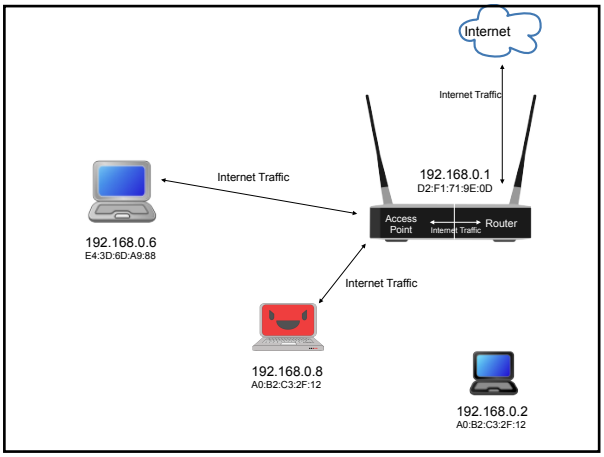












KRU6HFGZ

Bettercap

- Bettercap lets you ARP poison a network
- You can monitor all traffic in e.g. Wireshark
- You can to redirect traffic to any port, e.g. to Burp Proxy or program you have written yourself.
- Details:
  - https://miloserdov.org/?p=1112#44
  - https://github.com/bettercap/bettercap/wiki
  - https://www.evilsocket.net/2018/02/27/All-hail-bettercap-2-0-one-tool-to-rule-them-all/
- N.B. Bettercap v2 (Feb 2018) very different from version 1.

KRU6HFGZ

Different methods

- You have seen 3 method that look similar but are very different.
- Set HTTP Proxy to Burp
  - Target device must support a proxy
  - App must accept proxy setting and use HTTP
- Decrypt WPA in Wireshark
  - Don't need anything from device, any type of traffic.
  - Can only read traffic.
- ARP poison with Bettercap
  - Don't need anything from device, any type of traffic.
  - Can read and alter traffic