Introduction to (home) network security.

Paul Lockyer (a.k.a: Egor)
egor-ccc@outlook.com

How many of you identified the item in the image?
Hard shell, squidgy interior.

How many figured out where the After Eight mint fits into a talk about network security?

Will return the our friendly mint later.

- What
- Why
- How

What – the fundamentals of network security
    High level (concepts not in-depth how to)

Why talk about the fundamentals of network security at a hacker camp?
    Diverse audience – not everyone expert
    IT large topic, expert in one area not in another
    Encourage other experts to start conversations
    Topic I frequently find people don't know about

How – Using vulnerability management theory as a framework to structure the talk around.

Vulnerability Management

- Assets: Things we own that we protect (this could be physical (eg: mobile phone), or virtual (eg: digital images, or reputation).
- Threats: What we must protect against (cyber threat actor, malicious script, DDOS attack, etc).
- Vulnerabilities: Where people or systems have a weakness that could be exploited.
- Risk: The exposure of assets if a threat successfully exploits a vulnerability.

Four basic aspects to vulnerability management.

Threats seek to obtain assets, generally they do so by exploiting vulnerabilities due to a lack of mitigation, remediation, or poor design. Typically, this is due to failure to identify the risks associated with the vulnerability, or failing to remediate in an appropriate timescale.

Internet circuit – asset, vulnerable, low risk

Lets consider each of these four areas as they relate to network security.

Assets

- What is an asset in a network?
  - Physical infrastructure.
  - Connected endpoints.
  - Data (on endpoints and flowing across the network).

Assets: Things we own that we protect

Lots to protect!

Threats

Types of threat:

- DoS
- Ransomware
- Phishing
- Data theft
- Tracking
- Identity theft
- Botnet

Sources of threats:

- Threat actors:
  - Individuals with malicious intent.
  - Nation state sponsored groups.
- Commercial organisations.

Threats: What we must protect against (cyber threat actor, malicious script, DDOS attack, etc).

DoS: Consumer vs. business.
Phishing: Indirect, enables other threats.

Individuals with malicious intent:
Vary in capability and threat

Vulnerabilities: Sources

- Design problems
- Implementation flaws
- Configuration issues
- Changes over time
- Failure to apply security updates
- Assumption of trust

Vulnerabilities: Where people or systems have a weakness that could be exploited.

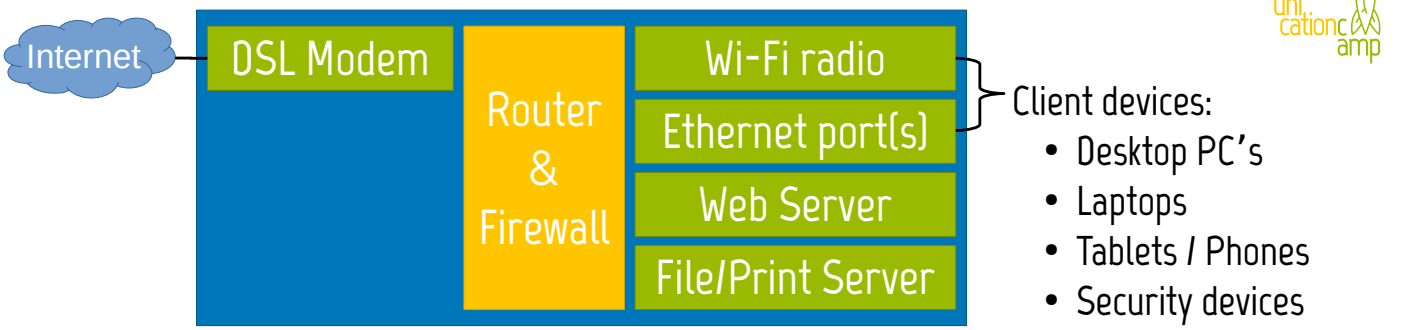
Implementation flaws:
- Lost in translation
- eg: VLAN segregation

Changes over time:
- Cumulative effect
- Change in usage

Failure to apply security updates
- Zero-day vs. patch not applied

Assumption of trust:
- In the people you allow to connect devices
- In the devices you add to your network
- In data (eg: email attachments)
- In people (eg: help desk call)

Vulnerabilities: Typical small network

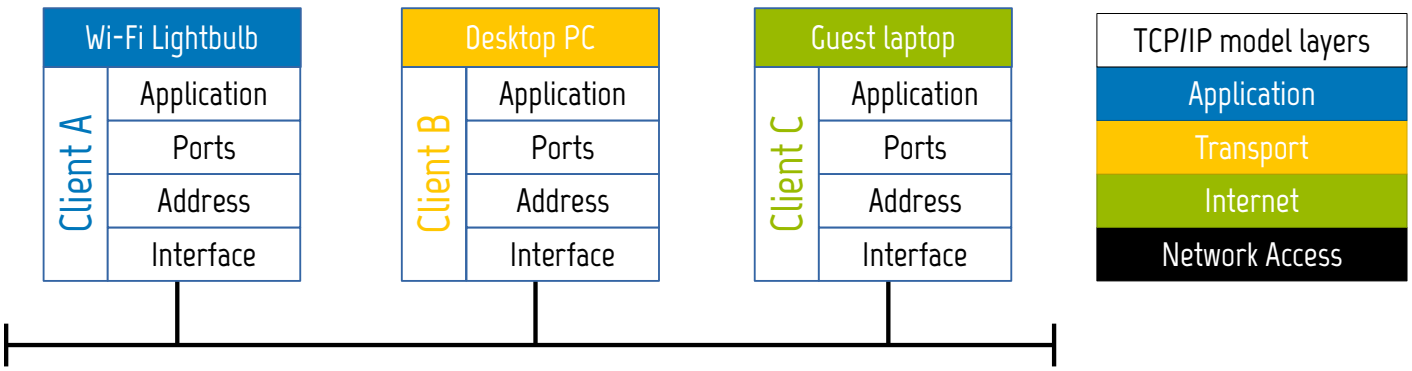


- Typically closed source firmware
- Built to cost
- Remotely accessible / updatable by ISP
- Web server
- File/Print server
- Flat network

External (wide area network)
Internal (local area network)

Vulns:
Closed source – can't easily review, and those with skills unlikely to do so.
Built to cost – lack of incentive to maintain.
Built to cost – lack of features
Logging
Ability to segregate traffic
Web server – may be accessible externally.
Web server – default credentials.
Flat network – the After Eight mint model for network security

Vulnerabilities: Network Fundamentals



Network access:
- Physical connection to the network
- Various protocols – Ethernet for small networks
- Local transmission in addressed frames

Internet:
- Logical addressing
- Packet delivery – may or may not arrive, and order not guaranteed
- Routing
- IP / ICMP / ARP

Transport:
- End to end communication
- Error free delivery, and in sequence (TCP)
- Best effort (UDP)

Application:
- HTTP / FTP / SSH

Vulns:
- Access beyond least privilege (IoT camera example)
- Guest equipment – AV, been on other networks
- Guest equipment – typically Wi-Fi

Vulnerabilities: Wi-Fi

- Do you control the hardware?
- Do you control the software / firmware?
- Are the protocols broken?
- Who have you given access to? Are their systems secure?
- Who's network have you connected to?
- Non-physical connection increases attack surface.

Risk

- What do we do about risk?

  Two choices:

  1) Ignore / Accept it

  2) Mitigate

The exposure of assets if a threat successfully exploits a vulnerability.

Ignore vs Accept, difference is risk analysis:
Analysis: Probability, Impact, Cost

Mitigation – Many forms, quickly look at some

Risk Mitigation: Groundwork

- There is no magic bullet
- What is your acceptable level of risk?
- Don't try and do everything at once
- Presume you will be compromised
- Apply security in layers
- Security is an iterative process, the threat landscape is constantly changing
- A healthy dose of scepticism combined with good critical thinking are your best defensive weapons

Magic bullet – 'what software should I buy?'

Presume compromise:

What if?

Recovery

Layers - "I've got anti-virus so I'm done right?"

Risk Mitigation: Knowledge

- Know your gear
- Port scanning (eg: Nmap)
- Firewall logging
- Monitoring/Detection systems
  - Intrusion Detection and Intrusion Prevention
  - Security Information and Event Management (SIEM)
  - Eg: Suricata, Snort, OSSEC
- Packet capture and analysis (eg: Wireshark)

Know your gear: Knowledge is power
Port scanning: Baseline, know what is ‘normal’
Firewall logging: Key tool for understanding

Ascending order of complexity

Packet capture will reveal traffic flow issues on flat networks

Risk Mitigation: Traffic segregation

- Principle of least privilege
- Physical vs. virtual network segregation

Least privilege – not all traffic should be equal

Unlikely that ISP supplied ‘all-in-one’ will support this

Risk Mitigation: Wi-Fi

- SSID hiding doesn't work
- WEP is broken
- Don't use SSID's that make you a target
- Consider shutting down SSID's when not in use
- WPA3
- Locate access points and set power to minimise external signal propagation
- Your WiFi is only as secure as the weakest device connected
- Segregate traffic
- Disable access to configuration interfaces from Wi-Fi
- Disable Wi-Fi Protected Setup (WPS)
- Subscribe to alerts for vulnerabilities and patches, and apply
- Configure logging and alerts.
- Use strong passwords and consider multi-factor authentication
- Consider WPA2 Enterprise over WPA2 Personal
- Consider using 802.1Ix
- Your WiFi is only as secure as the firewall.
- Consider disabling UPnP
- Don't enable auto-connect on other people's networks

Alerts/patches: Document if business

Risk Mitigation: General

- Data retention
- DNS
- VPN
- Anti-virus
- Remove unneeded devices and services
- Is your hardware physically secure?
- Be extra vigilant with devices that you use to roam on other networks (eg: coffee shop wifi etc)
- Consider 'what if' before making decisions to use services, create/store data, etc.
- Consider disabling JavaScript in web browsers
- Be afraid of links in emails
- Use unique, strong passwords for each site / service / device
- Be careful what you install, not all free software is free
- Consider restricting devices to internal service proxies for DNS, SMTP, etc.
- Consider containerisation for email and/or web browsing
- Visiting interesting places
- Encrypt data written to any media (flash, disk, cloud, etc).
- Patching is pointless if your configuration management is poor
- Backups

Summary

- Network security starts with knowledge
- Knowledge is the basis for risk management
- Aim for incremental gains

Final thoughts

- Feedback
- Thanks
- Happy hacking

To all the angels working behind the scenes to support this talk

For listening