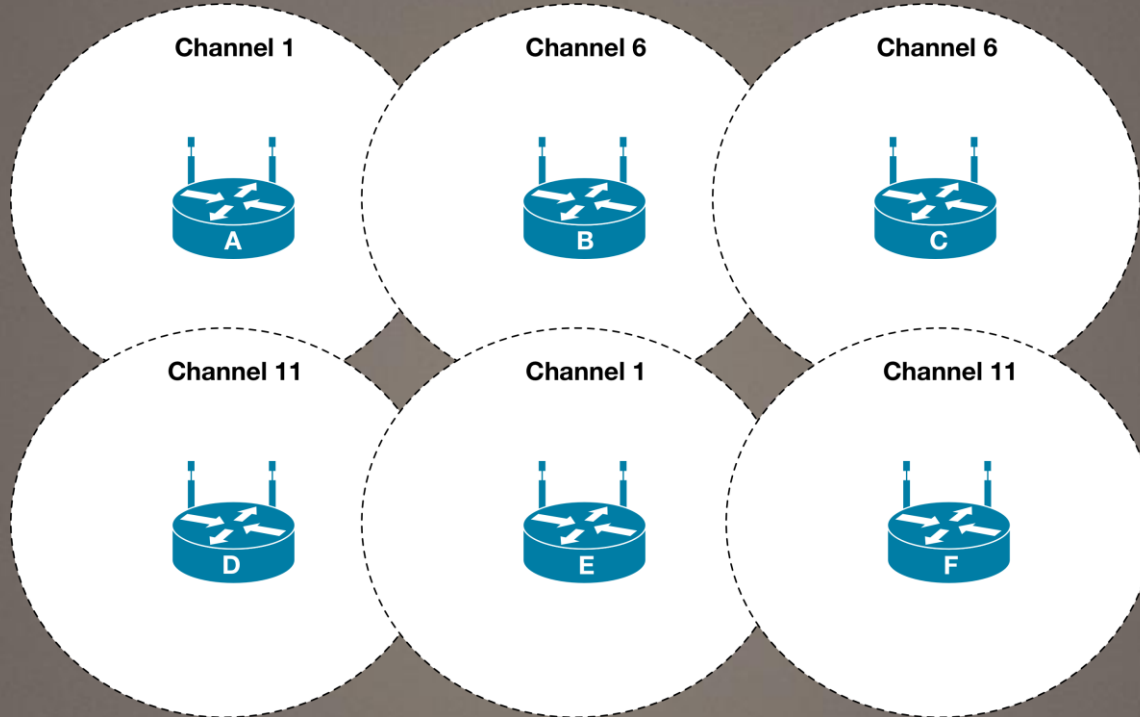


Review Question

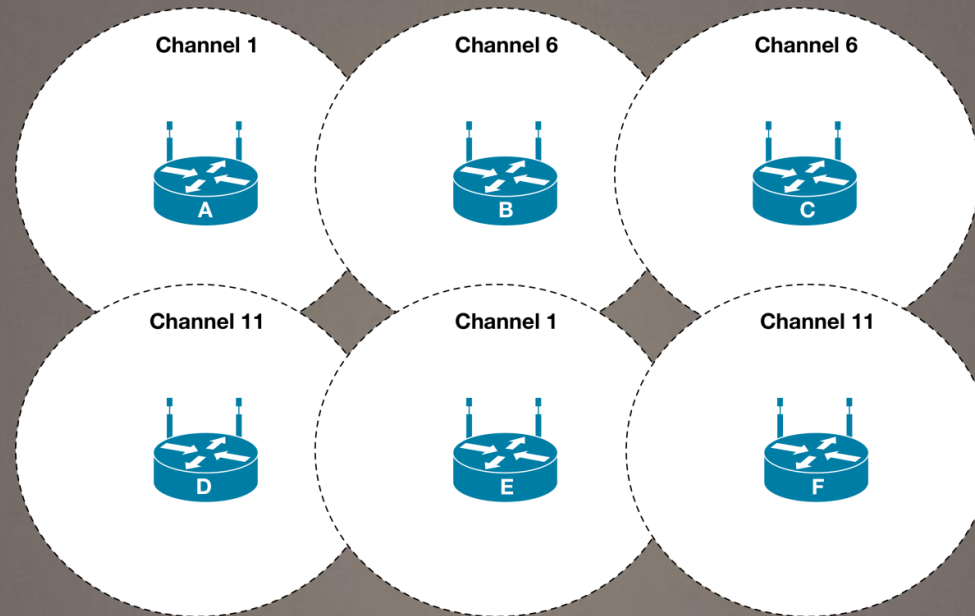
Consider the topology below



- How would the current deployment impact client performance?
- What could be done to improve this 2.4GHz wireless deployment?

Review Question

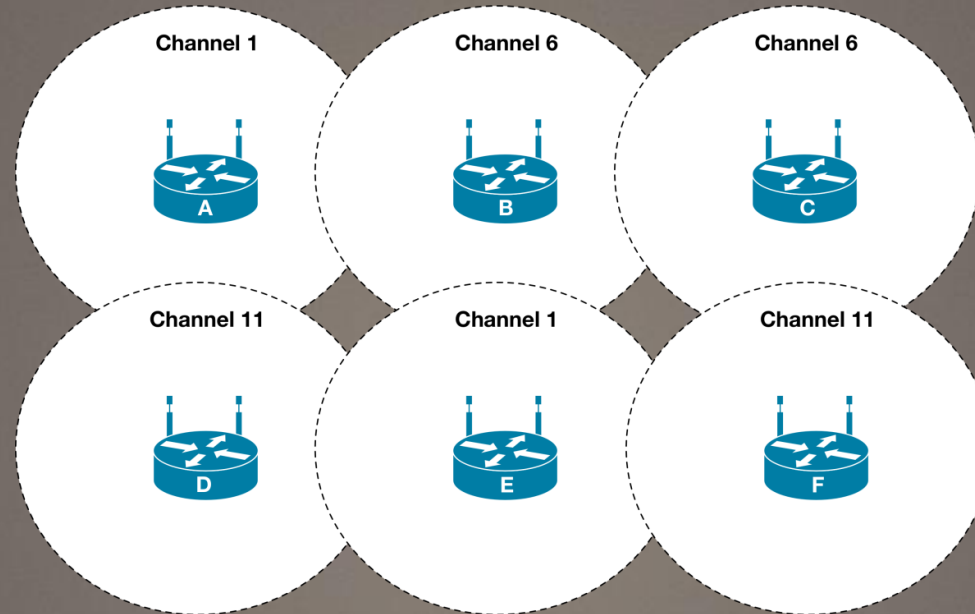
Consider the topology below



- How would the current deployment impact client performance?
Given that access points B and C are adjacent and transmitting on Channel 6, performance for devices in the coverage area for both access points could be degraded as the medium is shared by all clients in the shared coverage area

Review Question

Consider the topology below



- What could be done to improve this 2.4GHz wireless deployment?

Access points B and C are adjacent and transmitting on Channel 6, moving C to Channel 11 and F to Channel 6 would improve performance



Murdoch
UNIVERSITY

Internet Security

ICT169

Foundations of Data
Communications



Admin

- Lecture recording for Topic 9 missing audio
 - Second half of the lecture missing audio due to LCS failure
 - Lecture recording from 2017 available
- Unit and Teaching surveys now open
 - Your chance to tell us how we're going and reward staff you think are working hard and / or doing a good job
 - Make sure you leave written comments so we know what we're doing well or could do better
 - Open until 6 December (but please don't forget!)

Practical Exam

- Runs during Session 12 (Week 14) during lab times, you **must** attend the lab you are enrolled in
- Online (LMS-based) test, 100 minutes
- Use Packet Tracer for your implementation
- You will need to be able to:
 - Design an IP addressing scheme (subnet)
 - Build a network topology in Packet Tracer
 - Configure router interfaces and routing via CLI
 - Troubleshoot
- Contributes 25% of your final grade

Last Week

- Wireless technologies and applications
- Properties of wireless as a communications medium
- Wireless standards, configuration and security

7. Application

6. Presentation

5. Session

4. Transport

3. Network

2. Data Link

1. Physical

Lecture Overview

- An introduction to computer / network security
 - Motivations for cyberattacks
 - Different classes of cyberattacks and enabling techniques
 - Methods for securing devices
 - Notable cyberattacks in recent history



<https://hackaday.com/2017/04/01/ask-hackaday-which-balaclava-is-best-for-hacking/>

Cyberattacks are on the Rise

- Security is an increasing and ongoing concern for organisations and individuals
- New data breaches are reported with increasing regularity
 - [US State Department, September 2018](#) – email inboxes compromised
 - [Perth Mint, September 2018](#) – details of 3200 customers compromised
 - [Facebook, September 2018](#) – approx. 30 million accounts compromised
 - [Various, October 2018](#) – SuperMicro servers used in companies like Apple, Amazon, and the CIA alleged to include additional chip that could allow remote access

Cyberattacks are on the Rise (cont.)

- Many security breaches are accidental
 - [GovPayNet, September 2018](#) – 14 million records leaked
 - [Google+, October 2018](#) – data of 500,000 users leaked
- The prevalence of these breaches is exhausting, but will only continue
 - Tools for hacking and penetration testing are getting better (and easier to use)
 - Computer systems and networks are becoming bigger and more complex
 - Nation-states are getting in on the action
- An attacker only needs to identify a single vulnerability, while defenders must find (and fix) them all

Motivations for Hacking

- Hacking is not inherently malicious and may be done out of curiosity, educational interest, or to seek a personal / professional challenge
- **White hat hackers** seek to identify security flaws and inform vendors so that they can be fixed
 - Security researchers and professionals often engage in this form of hacking
- **Black hat hackers** exploit vulnerabilities for personal gain



Motivations for Hacking (cont.)

- Hacking may also be done to promote a social or political agenda
- Anonymous and L0lsec are well known for engaging in this form of hacking
- Government actors may engage in hacking to further political agendas or for intelligence purposes
 - US National Security Agency (NSA) / Central Intelligence Agency (CIA)
 - Russian Intelligence Directorate (GRU)
 - Chinese People's Liberation Army (PLA)

The CIA Triangle

- Three primary principles and goals used in security:
 - Confidentiality – keep the data secure from unauthorized people
 - Integrity – prevent tampering with the data
 - Availability – make sure the data and services are always available
- Referred to as the **CIA triangle** (or sometimes triad)

Reconnaissance and Information Gathering

- Find information regarding a potential victim
 - What kinds of network defenses are present?
 - Who is in charge of the network?
 - How aware are employees of security practices?
- Information is usually used to help plan another attack (like an intrusion)
- Can be active (directly communicate with the target) or passive (use already published information)

Passive Reconnaissance

- Use existing information about the target to gain information
- Internet whois queries
 - Who is in charge of the network?
 - How can they be contacted
- Public websites
 - Who is in charge of the company?
 - Where are they located?
- Social media presence
 - Where did someone go to school / university?
 - Where have they lived?

WHOIS information for cisco.com :

```
[Querying whois.verisign-grs.com]
[Redirected to whois.melbourneit.com]
[Querying whois.melbourneit.com]
[whois.melbourneit.com]

Domain Name..... cisco.com
Creation Date..... 1987-05-14
Registration Date... 2011-04-06
Expiry Date..... 2012-05-16
Organisation Name... Cisco Technology, Inc.
Organisation Address. 170 W. Tasman Drive
Organisation Address.
Organisation Address. San Jose
Organisation Address. 95134
Organisation Address. CA
Organisation Address. UNITED STATES

Admin Name..... Info Sec
Admin Address..... 170 West Tasman Drive
Admin Address.....
Admin Address..... San Jose
Admin Address..... 95134
Admin Address..... CA
Admin Address..... UNITED STATES
Admin Email..... infosec@cisco.com
Admin Phone..... +1.4085273842
Admin Fax..... +1.4085264575

Tech Name..... Network Services
Tech Address..... 170 W. Tasman Drive
Tech Address.....
Tech Address..... San Jose
Tech Address..... 95134
Tech Address..... CA
Tech Address..... UNITED STATES
Tech Email..... dns-info@cisco.com
Tech Phone..... +1.4085279223
Tech Fax..... +1.4085267373
Name Server..... NS1.CISCO.COM
Name Server..... NS2.CISCO.COM
```

Active Reconnaissance

- Use more direct methods of information gathering
- Network and port scanning
 - What hosts are present on the network?
 - What applications are running?
 - What operating system is being run by the target?
- Use this information to investigate potential vulnerabilities
- Can also be based on direct interaction



Social Engineering

- The act of manipulating a victim into performing specific actions or providing confidential information
- Can exploit a number of psychological principles to convince the target to comply



Phishing

- Attempt to trick a victim into providing sensitive information (eg. usernames, passwords, credit card numbers)
- Usually uses a fake email and / or website to entice the user by offering something they might want
- Different forms of phishing attacks exist, with **spear phishing** targeting a more specific group of users



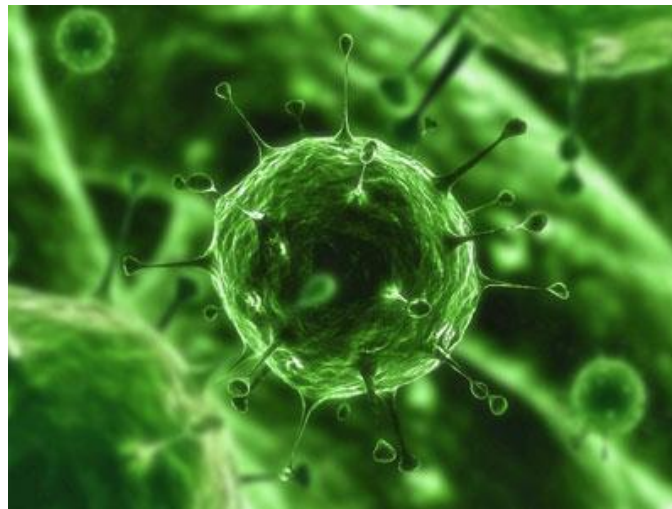
Access and Intrusion

- Aim to gain unauthorised access to a system or network
- Use the information gathered during reconnaissance to figure out where to gain access
- Can be as simple as guessing (or obtaining a password or much more complex
- May involve gaining access to less secure hosts or services then leveraging access to compromise more sensitive targets



Viruses

- Frequently used as an umbrella term for most forms of malicious software (worms, malware, spyware, rootkits)
- Actually describes a piece of code that attaches itself to a file or application and replicates
- Historically spread through sharing floppy disks, but now via email and websites



<http://health.howstuffworks.com/medicine/modern-technology/light-virus.htm>

Worms

- Similar to viruses but are able to exist without attaching to other files
- Exploit network-based vulnerabilities to spread
- Deliver a payload (malicious code)



Trojan Horse

- More frequently referred to as a 'trojan'
- Software that masquerades as a harmless (or even desirable) application that includes malware
- For example, a "free" version of Adobe Photoshop that transmits your keystrokes to an attacker



Software Exploits

- Software or sequence of inputs that takes advantage of a vulnerability in existing software
- Usually mitigated by applying software patches
 - Not always released or applied in a timely fashion
- Exploits that are used before the vulnerability is publicly known are referred to as **zero day exploits**



Rootkit

- Software designed to access privileged areas of the system
- Originates from the *nix name for the admin user: root
- Usually installed through an exploit, but can be deliberately or unintentionally installed by the user
 - Sony copyright protection rootkit
 - Superuser access to phones
- Difficult to detect and remove due to the high level of access gained



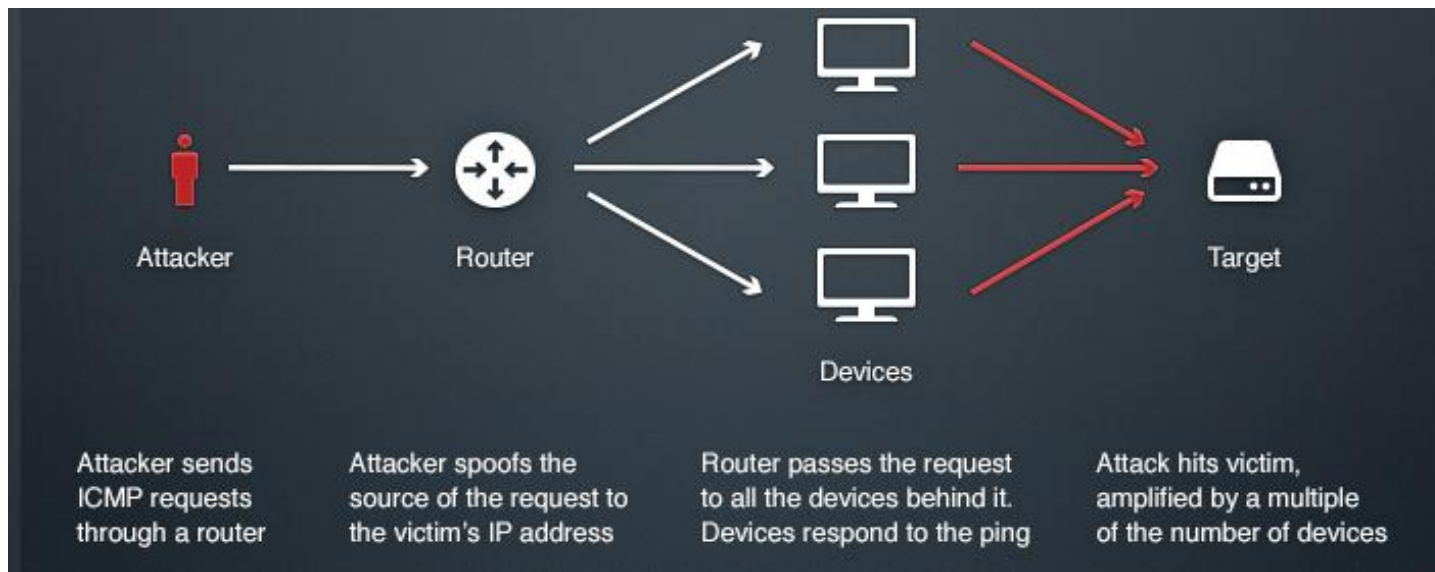
Denial of Service (DoS) Attacks

- Aim to impact the availability of a system or network, preventing legitimate access
- In the context of networks, usually try to overwhelm the target with more traffic than it can handle / process
- Early denial of service attacks could be carried out by a single host (or a small number of them)



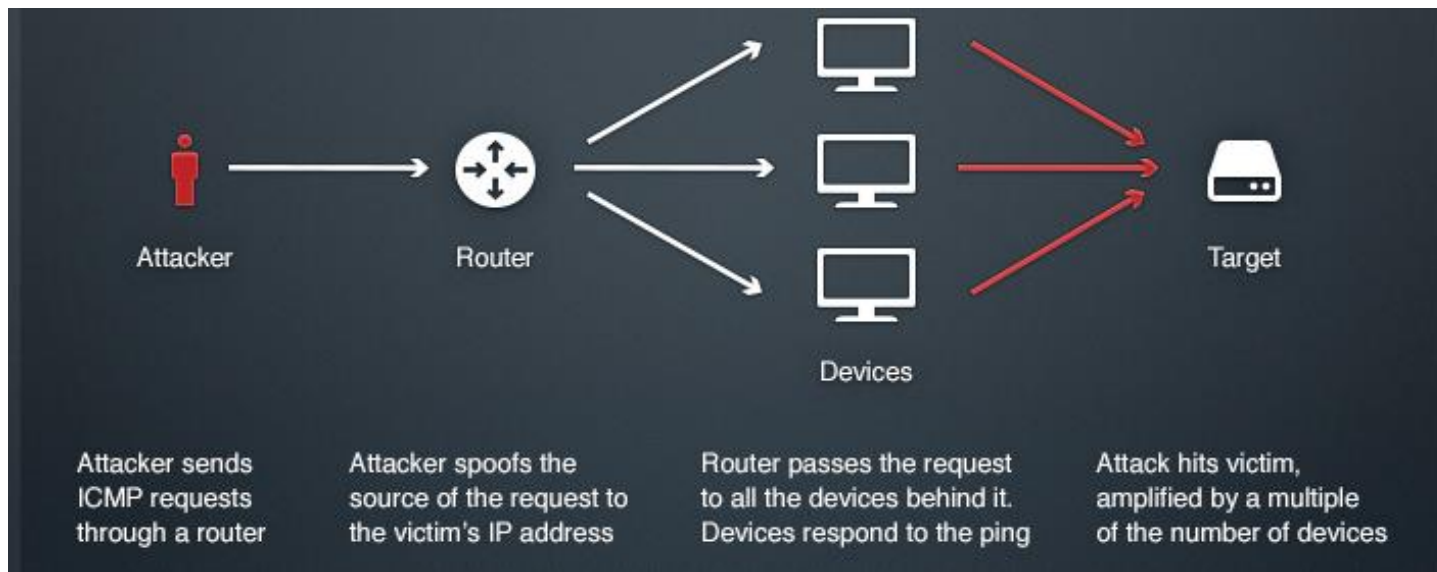
Types of Denial of Service Attacks

- Different variations of DoS attacks have developed over time, exploiting different implementation or design flaws
- **Ping of death:** send a large ICMP message to cause a operating system crash
- **Smurf attack:** send ICMP as broadcasts with a spoofed source address to have all hosts respond



Types of Denial of Service Attacks (cont.)

- **TCP SYN Flood:** continually send TCP synchronisation requests to a target to create large numbers of TCP connections
- **DNS / NTP Amplification:** send requests to DNS or NTP servers with a spoofed source address causing servers to send traffic to the target



Distributed Denial of Service (DDoS) Attacks

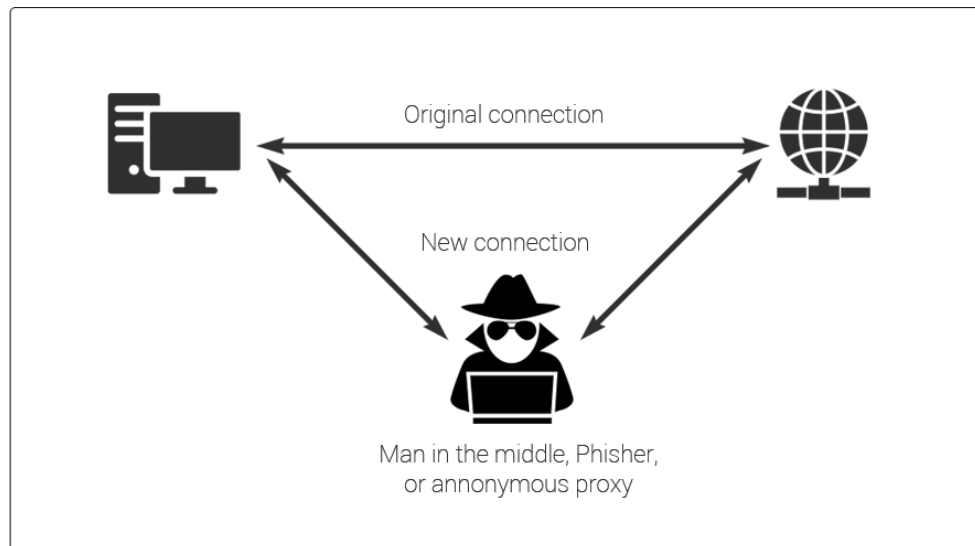
- Bandwidth now more readily available requiring more resources (hosts) to impact availability
- May involve numerous attackers cooperating, but more likely to use a **botnet**
- Botnets are groups of compromised hosts that can be instructed to perform actions by the handler
 - Recent attacks have used smart appliances as bots
- More difficult to defend against as traffic may appear to be legitimate



<http://en.wikipedia.org/wiki/Botnet>

Man-in-the-Middle Attack

- An attacker intercepts communications between the victim and their destination
- Communications can be read and / or modified
- One scenario might be where an attacker acts as a rogue wireless access point to capture packets from nearby users



Break

When we return: Securing devices and notable cyberattacks

Defending Against Cyberattacks

- Defending against threats is arguably more difficult than attacking
- Defenders must secure **all** potential vulnerabilities, while attackers only need to find and exploit a single one
- The safest approach would be to turn off your computer and never use it again, but this isn't very practical
- You need to consider your **threat model** when designing countermeasures (who or what are you trying to defend against?)



Security through Obscurity

- Before we discuss countermeasures, let's clear up what isn't security
- Any measures that rely on hiding or obscuring technical details from others are not considered secure
- An analogy from Bruce Schneier:

“If I take a letter, lock it in a safe, hide the safe somewhere in NY, then tell you to read that letter, its not security. Its obscurity

On the other hand if I take a letter, lock it in a safe and then give you the safe along with the design specifications of the safe and a hundred identical safes so that you and the worlds best safe crackers can study the locking mechanisms and yet you still can't open the safe, that's security”

Security through Obscurity (cont.)

- To discuss security through obscurity more specifically, we should look at some examples:
- If a wireless access point is prevented from advertising the presence of a network, is this secure?
- If a new encryption protocol was designed, would you trust it more if it were open or closed source?

Defence in Depth

- Refers to the practice of implementing **several layers** of countermeasures to protect your device or network
- Based on the strategic principle that it will be more difficult to defeat a multilayered system than a single mitigation
- For example, an organisation may have a network level firewall, as well as firewalls on endpoint devices (like PCs)



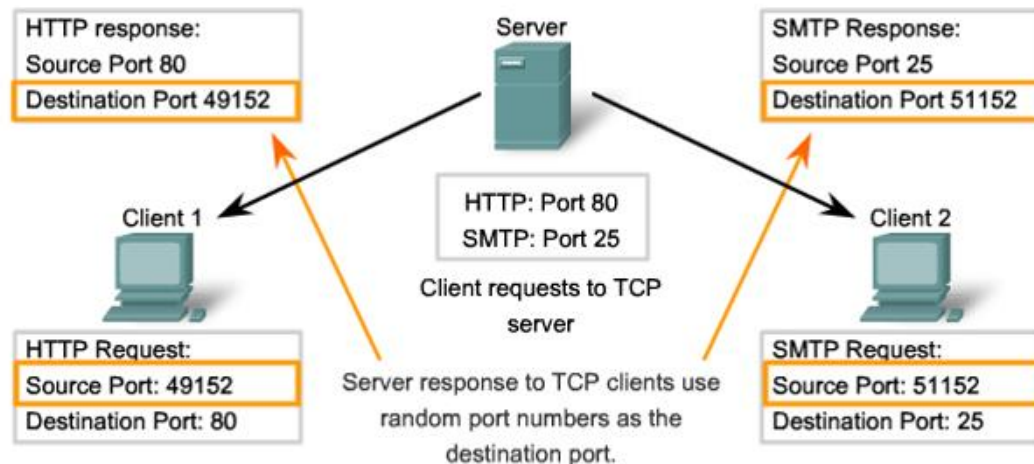
<https://www.forcepoint.com/cyber-edu/defense-depth>

Securing Networked Devices

- Potential mitigations and countermeasures can be deployed at two major points in the network
 - **Network edge:** point of ingress / egress from your network, usually a router with an Internet connection
 - **Endpoints:** end-user hardware like PCs and mobile devices
- There will be some overlap in the types of defences that can be deployed at each point, but the goals may differ

Reducing the Attack Surface

- Recall that networked applications will use a TCP or UDP port to listen for incoming traffic
- Most open ports are legitimate, but it's worthwhile checking that no unnecessary ports have been left open
- The obvious approach to dealing with open ports is to terminate the application using the port, but it can also be secured with a firewall



Network Firewalls

- A firewall is barrier with set of rules defining which network traffic can or cannot pass
- Two approaches to configuring firewalls
 - Blacklist: permit everything except traffic specified
 - Whitelist: deny everything apart from traffic specified
- Whitelisting is more secure, but requires more maintenance (new applications must be explicitly added to the list)
- Filtering is based on source and destination IP addresses and port numbers
- NAT is sometimes erroneously thought of as a firewall

Intrusion Detection and Prevention Systems

- More advanced firewalls that consider the contents of the packet (or series of packets)
- Allows for more advanced detection of threats to the network
 - Signatures of known attacks
 - Abnormal traffic (eg. sudden spike in bandwidth use)
- Intrusion Detection Systems merely log these events, while Intrusion Prevention Systems can mitigate them
- Can be dedicated hardware appliances or software-based

Securing Wireless Connections

- Recall that WiFi broadcasts packets through the air, allowing for traffic to be intercepted
- Wireless traffic should be encrypted using WPA2 (or WPA3, when it becomes available)
- A Virtual Private Network may also suffice if the wireless network is outside your control



Endpoint Security

- Possible security measures depend on the exact device
- Numerous sets of recommendations
 - [Australian Cyber Security Centre \(ACSC\) Essential Eight](#)
 - [UK National Cyber Security Centre 10 Steps: Secure Configuration](#)
 - [US Computer Emergency Readiness Team Security Recommendations to Prevent Cyber Intrusions](#)
 - [Canadian Centre for Cyber Security Top 10 IT Security Actions to Protect Internet Connected Networks](#)
- Recommendations focus on different areas, but many recommendations will be overlapping

Ensure Patches are Installed

- Many major security breaches could have been avoided had updates been installed sooner
 - ACSC recommends within 48 hours for high risk issues
 - Consider enabling automatic updates
- Both applications and operating system must be updated
- Some applications are more vulnerable than others, consider whether they're needed at all
 - Adobe Flash and Java are frequently requiring updates

Windows Update

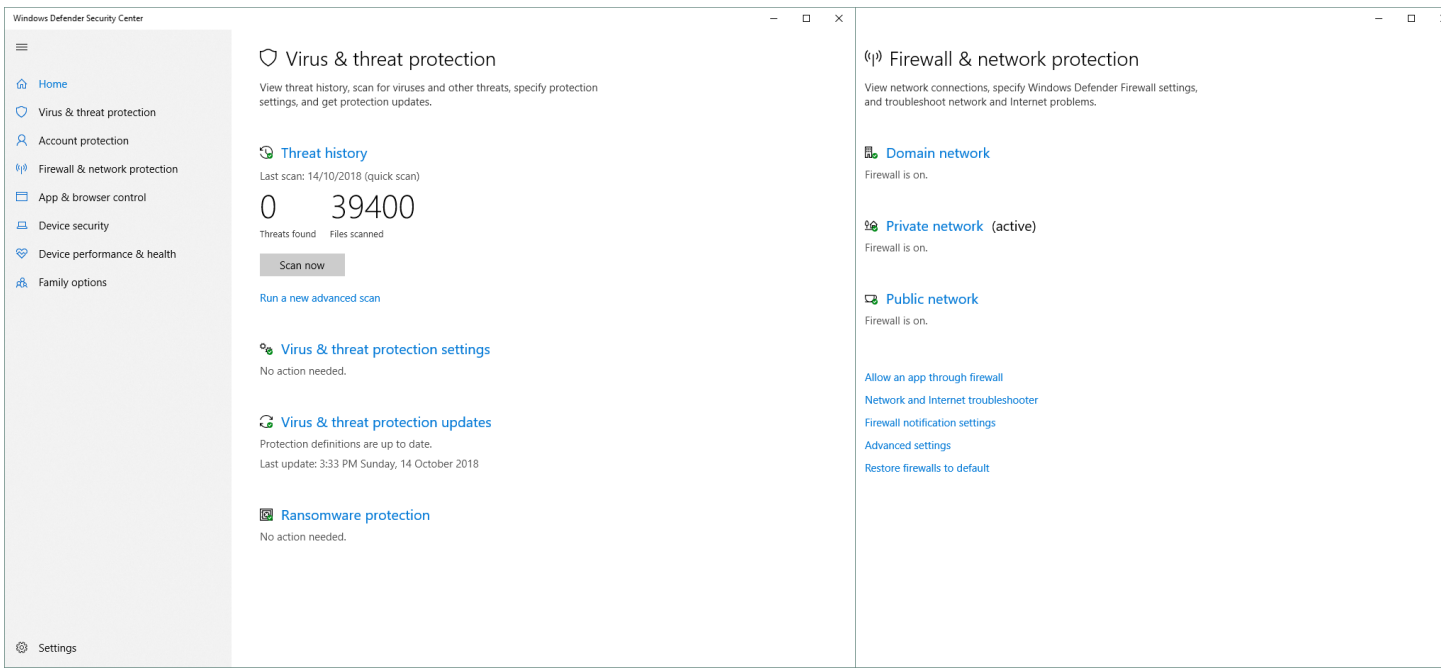


You're up to date
Last checked: Yesterday, 11:52 PM

Check for updates

Endpoint Firewalls and Anti-malware

- Most operating systems have some form of firewall integrated (eg. Windows Firewall)
- Antivirus and anti-malware is also often included too
- Make sure that it is enabled and kept updated (these are applications too!)



The screenshot displays the Windows Defender Security Center interface. On the left is a navigation pane with options: Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main area is split into two panels. The left panel, titled 'Virus & threat protection', shows a 'Threat history' section with a last scan on 14/10/2018 and 39,400 files scanned. Below this are links for 'Virus & threat protection settings', 'Virus & threat protection updates', and 'Ransomware protection'. The right panel, titled 'Firewall & network protection', shows settings for three network types: Domain network, Private network (active), and Public network, all with 'Firewall is on'. At the bottom of this panel are links for 'Allow an app through firewall', 'Network and Internet troubleshooter', 'Firewall notification settings', 'Advanced settings', and 'Restore firewalls to default'.

Endpoint Firewalls and Anti-malware (cont.)

- Third party antivirus software is available, but requires significant access to the operating system
- Interface used may [introduce additional vulnerabilities, so choose wisely](#)

Tuesday, June 28, 2016

How to Compromise the Enterprise Endpoint

Posted by Tavis Ormandy

Symantec is a popular vendor in the enterprise security market, their flagship product is [Symantec Endpoint Protection](#). They sell various products using the same core engine in several markets, including a consumer version under the [Norton](#) brand.

Today we're publishing details of multiple critical vulnerabilities that we discovered, including many wormable remote code execution flaws.

These vulnerabilities are as bad as it gets. They don't require any user interaction, they affect the default configuration, and the software runs at the highest privilege levels possible. In certain cases on Windows, vulnerable code is even loaded into the kernel, resulting in remote kernel memory corruption.

As Symantec use the same core engine across their entire product line, all Symantec and Norton branded antivirus products are affected by these vulnerabilities, including:

- Norton Security, Norton 360, and other legacy Norton products (All Platforms)
- Symantec Endpoint Protection (All Versions, All Platforms)
- Symantec Email Security (All Platforms)
- Symantec Protection Engine (All Platforms)
- Symantec Protection for SharePoint Servers
- And so on.

Some of these products cannot be automatically updated, and administrators must take immediate action to protect their networks. Symantec has published advisories for customers, available [here](#).

Let's take a look at a sample of the vulnerabilities we found.

New vulnerability uses antivirus software to infect systems with malware

Abusing the Restore from Quarantine feature

By Rob Thubron on November 12, 2017, 2:07 PM | 7 comments



Antivirus programs are supposed to keep us safe from all that malware floating around online, but devious hackers have been known to utilize the software for malicious purposes. The latest example of this practice involves using the "restore from quarantine" feature and has been discovered in multiple AV solutions.

Austria-based security auditor Florian Bogner discovered the vulnerability and dubbed it AVGater. It essentially works by relocating malware from an AV quarantine folder to a sensitive location on a victim's system.

Bogner, who works for [Kapsch](#), says he has notified the vendors of all the antivirus programs that contained the flaw. Some of the companies have released updates that address the issue, including Emsisoft, Ikarus, Kaspersky, Malwarebytes, Trend Micro, and ZoneAlarm

POPULAR



Wikileaks dumps Amazon data center locations for all to see



EA says it plans to remaster classic Command and Conquer games

Passwords

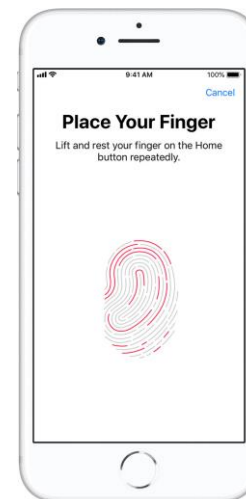
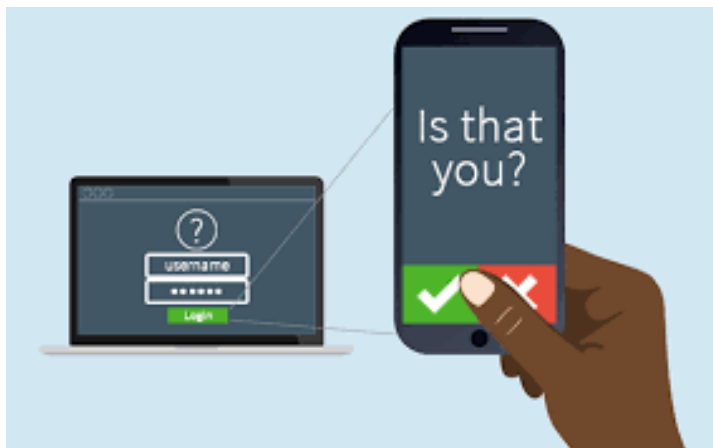
- Using endpoint security measures will be of limited effectiveness if an attacker gains physical access
- Passwords are stored on every device and in every service you use, but (usually) not in plaintext
 - Should be hashed to avoid being human-readable
- Choosing strong passwords is crucial as these are usually your first line of defence
- Some guidelines from the [National Institute of Standards and Technology](#):
 - Should not be guessable
 - Minimum of 8 characters
 - Not in the dictionary (these can be compromised by dictionary attacks)

Don't Use These Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. Football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123123
18. dragon
19. passw0rd
20. master

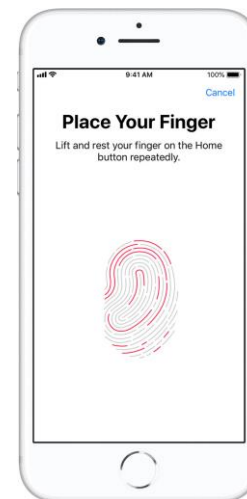
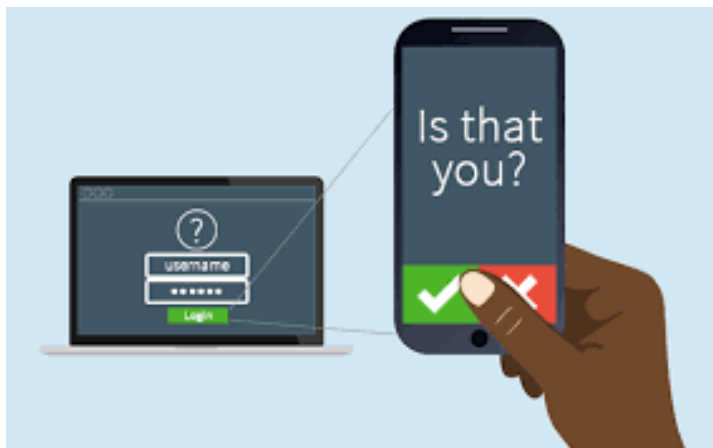
Two-Factor Authentication (2FA)

- Most services use a password – something you know – as an authentication method
- Two additional paradigms exist
 - Something you have (usually a token)
 - Something you are (biometrics)
- These additional factors can, and should, be used to authenticate a user (especially for sensitive accounts)



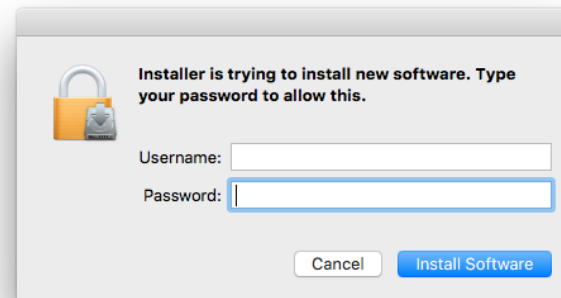
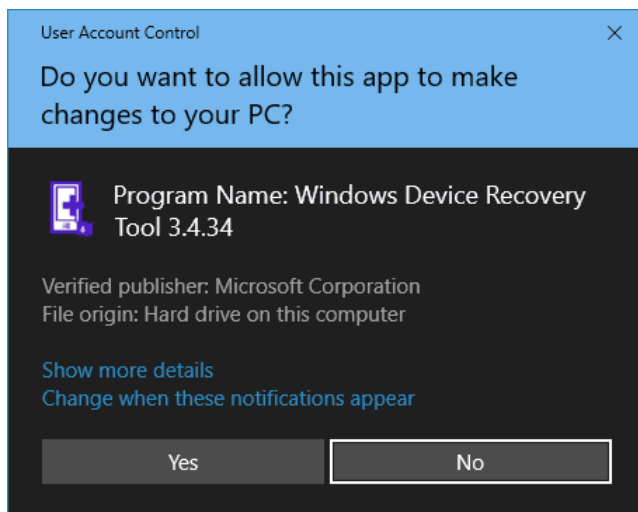
Two-Factor Authentication (cont.)

- Most services use a password – something you know – as an authentication method
- Two additional paradigms exist
 - Something you have (usually a token)
 - Something you are (biometrics)
- These additional factors can, and should, be used to authenticate a user (especially for sensitive accounts)



The Principle of Least Privilege

- Most users will have administrative accounts for the operating system by default
- Administrative users can have the ability to install software and access files without restriction
- Consider whether administrative privileges are needed for all users (and remove them if they aren't)



Backup Your Data (Off-site)

- Important data should be backed up regularly
 - Protects against hardware failure
 - Also allows you to recover after an attack (particularly from ransomware)
- Use the 3-2-1 rule for important data
 - Ensure you have **three copies** of any important data
 - Keep these copies in at least **two formats** (eg. on your hard drive and on a USB drive)
 - One copy should be stored **off-site** (at another location)

Encrypting Data at Rest

- Encrypting data on your device renders it unreadable to an attacker that gains physical access
 - Particularly useful if your device is stolen
 - Has also been used in cases where devices are seized
- Most operating systems (desktop and mobile) have inbuilt full disk encryption
 - Windows BitLocker
 - Apple FileVault
- Used to slow down devices, now limited performance impact due to hardware acceleration



Security vs. Convenience

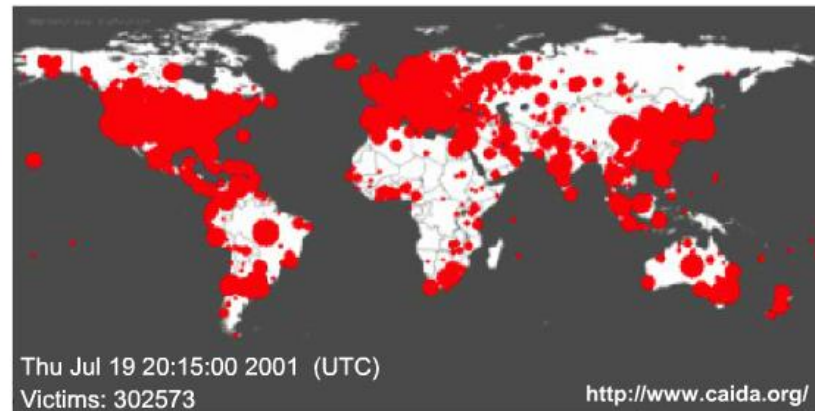
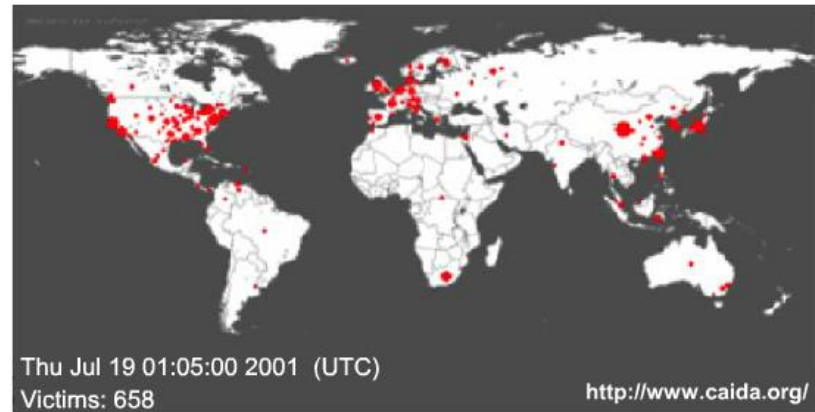
- We've discussed a quite a number of mitigations, and the list is not exhaustive
- Implementing all of these measures would make you more secure, but some reduce usability
 - Secure passwords are difficult to remember
 - Having to type in your password to install software is a nuisance
 - Finding your phone (or security token) to login to your PC is even worse
- Security and convenience are often seen as in opposition

Security vs. Convenience (cont.)

- Need to determine what level of security is required based on the threat model
 - Are you defending against a nation-state intelligence service or just your nosey housemate?
- Identifying the threats you are trying to defend against will help determine which countermeasures are necessary

Code Red Worm (2001)

- Targeted Microsoft Internet Information Services (IIS) web server
 - Could be triggered by a HTTP GET request
- Buffer overflow allowed arbitrary execution of code
- Payload of worm defaced web site and executed a DoS against specific targets
- Peaked July 19, 2001 with 359,000 infected hosts
- 1-19 July: spreading phase
- 20-27 July: DoS attacks on certain targets



Buffer Overflow

- Write more information into buffer than it can hold
- Missing or non-functional bounds checking when writing to memory
- Can either be used to crash a system or to execute arbitrary code
- Requires in-depth knowledge of low level programming, such as assembler

```
void function(char *str) {
    char buffer[16];

    strcpy(buffer, str);
}

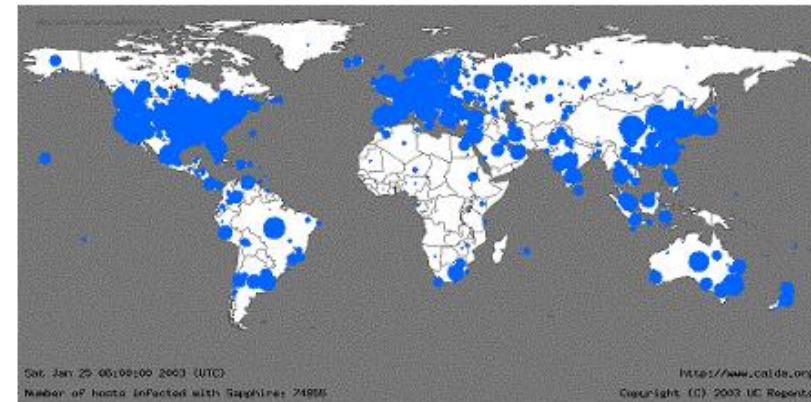
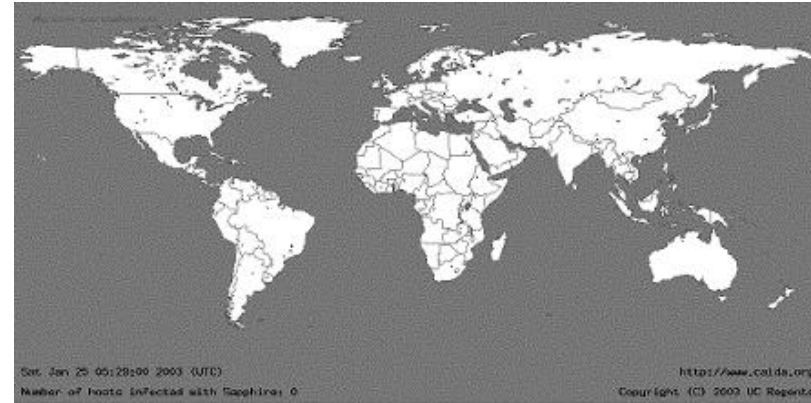
void main() {
    char large_string[256];
    int i;

    for( i = 0; i < 255; i++)
        large_string[i] = 'A';

    function(large_string);
}
```

Slammer Worm (2003)

- Buffer overflow in Microsoft SQL Server 2000
- Patches released 6 months earlier but not applied by many
- Worm fit into one UDP packet
- Most victims were infected within 10 minutes of release
- No payload, but networks became overloaded with Slammer traffic and became inoperable (DoS)
- Seen again in 28 November—4 December 2016



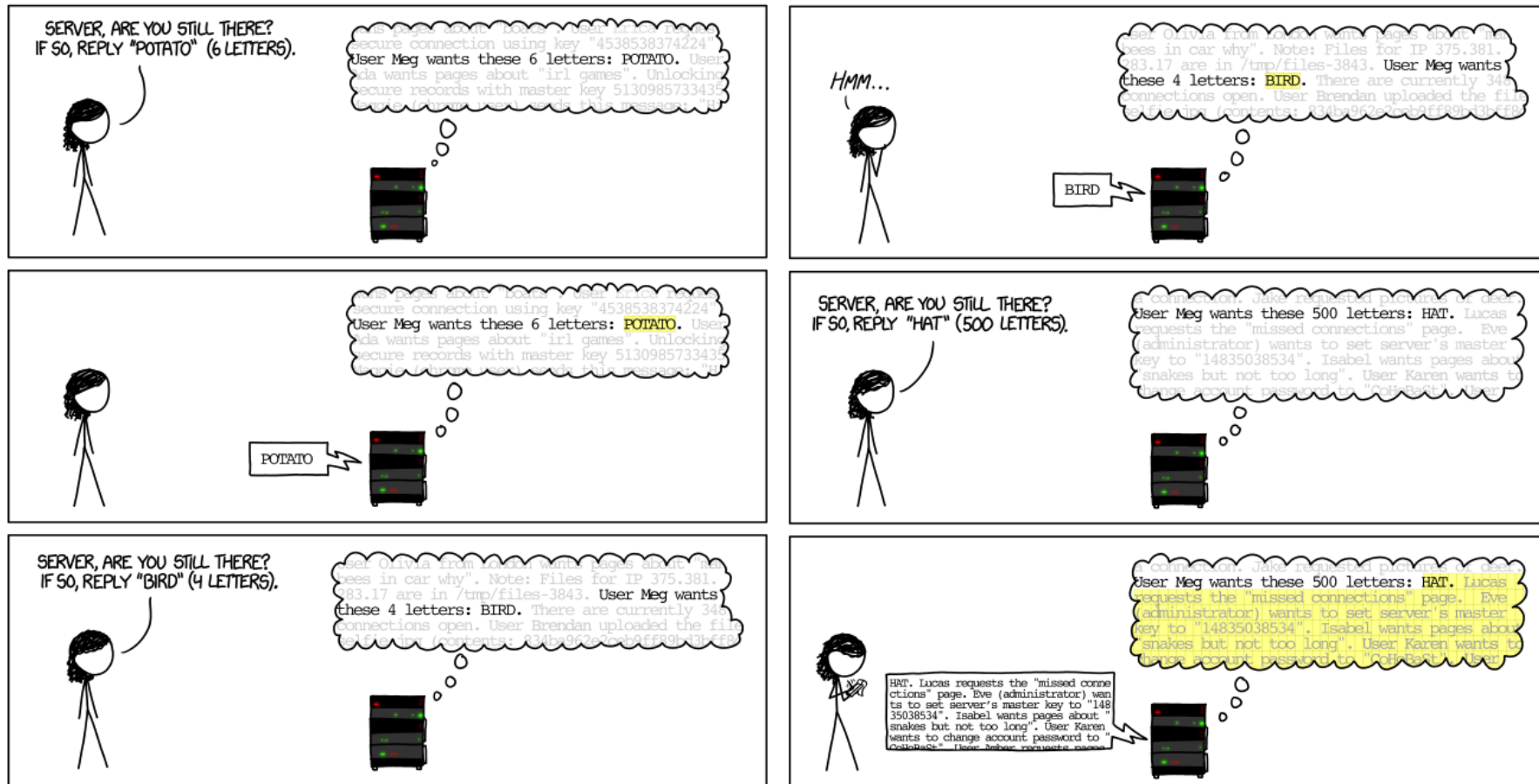
Heartbleed (2014)

- Vulnerability in OpenSSL – SSL implementation for Linux – disclosed in April 2014
- Buffer over-read exploit that allows anyone on Internet to read memory of affected systems, compromising usernames, passwords and keys
- Uses specifically crafted SSL/TLS heartbeat messages



<http://heartbleed.com/>

Heartbleed (2014) – An Example



XKCD comic describing Heartbleed

BlackEnergy (2015)

- Trojan horse that targeted the Ukrainian power infrastructure in December 2015
- Gained access via spear-phishing attacks against staff at power companies
- Included KillDisk payload to delete data and render systems inoperable
- Targeted the Industrial Control Systems used to operate the power grid
- Power supply was interrupted for 1—6 hours (likely staged recovery)
- Attack attributed to Russian Federation

Yahoo (2016)

- Actual breach took place in 2014 but data was only dumped in dark web in mid-2016 including data of over 500 million accounts
- Second breach discovered to have taken place in August 2013 including 1 billion accounts
- Names, emails, phone number, security question answers and responses (some as cleartext), hashed passwords (at least they were salted)
- Yahoo claims “state-sponsored” hackers to be responsible, but there is no evidence for that

Mirai Botnet DDoS (2016)

- DDoS that used Internet of Things (IoT) devices – such as CCTV cameras and DVRs – to generate traffic
- Devices were compromised using default login credentials (that couldn't be changed in most cases)
- First targeted (unconfirmed) websites hosted by French-based provider OVH on 19 September, 2016
- Second attack against Dyn (DNS provider) on 12 October, 2016
- Different botnets (using same exploit code) used for each attack
- Peak throughput for the OVH attack was close to 1Tbps (Dyn didn't disclose throughput)

WannaCry Ransomware (2017)

- Ransomware that targeted Windows hosts running SMB (file sharing protocol)
- Encrypted data and demand ransom payment in Bitcoin
- Patch was released 2 months prior but (as usual), many users had not installed the update
- UK National Health Service hospitals were among those impacted



Equifax (2017)



- Data breach in July 2017 resulted in personal information being compromised
 - 145–148 million US citizens
 - 15.2 million UK citizens
- Included social security numbers and drivers license numbers
- Targeted a flaw with Apache Struts used in Equifax's dispute system
 - Flaw in parsing of certain HTTP headers
 - Patch was made available in March 2017
- Website allowing users to check if they were effected was equally insecure

Netlink Computer Inc (2018)

- Large electronics retailer based in Canada declared bankruptcy
- IT assets including servers, PCs, and hard drives sold without being deleted
- Contained records for 385,000 customers including names, email addresses, passwords (in plaintext) and some credit card details

NCIX  **.com**

GREAT TECHNOLOGY, SELECTION & SERVICE

<https://en.wikipedia.org/wiki/NCIX>



Supermicro Servers (2018)

- Developing story, first reported by Bloomberg Businessweek on 4 October 2018:

[The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies](#)

- Alleged that small chips were installed on Supermicro servers installed in numerous companies that phoned home to China
- Companies alleged to be involved (including Apple and Amazon) [strongly deny the claims](#)



Supermicro Servers (2018)

- UK National Cyber Security Centre (NCSC) and US Department of Homeland Security (DHS) [support Apple and Amazon denials](#)
- Joe Fitzpatrick (named source in original article) [has expressed some doubts since](#)
- Bloomberg [stands by the story](#)
- Details likely still to come..



Lecture Objectives

You should now be able to:

- Describe motivations for hacking
- Differentiate between white hat and black hat hackers
- Describe confidentiality, integrity, and availability in relation to computer security
- Differentiate between types of cyberattacks
- Differentiate between active and passive reconnaissance in relation to computer security
- Identify tools and techniques that can be used in cyberattacks
- Describe a denial of service attack
- Differentiate between denial of service and distributed denial of service attacks
- Describe defence in depth in relation to computer security
- Describe the concept of 'security through obscurity'
- Describe methods for securing the network
- Describe methods for securing endpoint devices
- Describe the tradeoff between security and convenience

Lecture Summary and the Week Ahead

- Today's lecture has been a brief introduction to cybersecurity, looking at:
 - Motivations for cyberattacks
 - Different classes of cyberattacks and enabling techniques
 - Notable cyberattacks in recent history
- We've also discussed recommendations for securing devices and networks
- If you're interested in cybersecurity, then this topic is continued in **ICT287 – Computer Security**
- Readings for this week are Routing and Switching Essentials, Chapter 9, as well as links on LMS
- In the labs: port scanning and threat analysis

Next Week

- A look at emerging trends and technologies in data communications
 - Software-defined networking
 - Whiteboxing and orchestration
 - Internet of Things

