Wireless, Mobile, Cloud & IoT

Dr Rob Hegarty

Aims & Objectives

- Upon completion of this lecture you will be able to:
  - Describe the threats posed to users of wireless networks
  - Compare the benefits and drawbacks of cloud computing (in a security context)
  - Explain the security challenges posed by B.Y.O.D
  - Summarise the type of data at risk of attack on mobile devices
  - Evaluate the security issues in emerging computing areas (Cloud, Mobile, etc)

Overview

- Wireless
- Mobile
- B.Y.O.D (Bring Your Own Device)
- Cloud
- Summary

Wireless

- Wireless networks are pervasive
- Advantages
  - Rapid deployment
  - Flexibility / Mobility
  - Cost reduction
- Disadvantages
  - Chaotic topologies
  - Interference
  - Limited range
  - Open transfer medium (Air)

Wireless Technologies

Technology	Typical Range	Bandwidth	Applications
RFID	20cm	424Kbps	EPOS, Passports, Credit Cards
Bluetooth	10m	2Mbps / 25Mbps	Headsets
Wi-Fi (802.11 Family)	100m	11Mbps / 1.3Gbps	PCs, Laptops, Smartphones, Tablets
GSM / GPRS / UTMS / LTE	Kilometres	9.6Kbps/171Kbps/3Mbps/50Mbps	Mobile devices

Others; Bluetooth Low Energy, Zigbee, ANT, CDMA, IrDA

RFID – Threats & Countermeasures

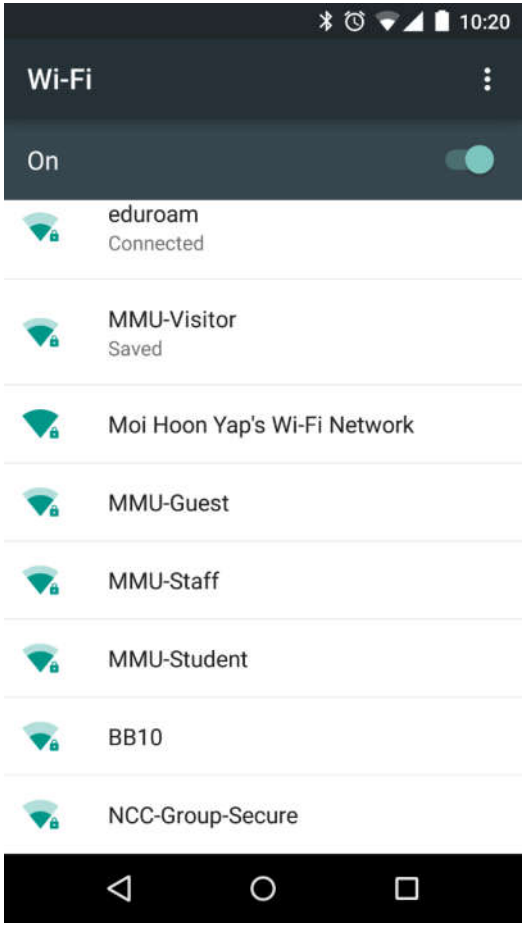
- Threats
  - Eavesdropping / skimming
  - Traffic analysis / profiling
  - Spoofing
  - Denial of Service (Tag kill command)
  - Jamming
- Countermeasures
  - Password protection of tag memory
  - Tag locking (make tag read only)
  - Faraday cage
- Further reading - http://www.infosec.gov.hk/english/technical/files/rfid.pdf

Bluetooth

- Named after the Viking king, Harald Bluetooth Gormsson and his abilities to make 10th-century European factions communicate.
- Bluesnarfing – Information stolen from device (Address book, IMEI, SMS, etc)
- Bluebugging – Authorised access to the microphone, speaker, etc
- Bluejacking – Spamming through Bluetooth business cards
- DoS – Rapid number of pairing requests to deplete battery
- Countermeasures
  - Bluetooth Employs frequency hopping,
  - Discovery mode,
  - Pairing codes
  - Switch off when not in use
- Further Reading
  - http://www.swedetrack.com/images/bluet11.htm
  - https://www.schneier.com/blog/archives/2005/04/bluetooth_snipe.html

Wi-Fi – Threats & Countermeasures

- Ubiquitous WLAN technology
- Threats
  - Eavesdropping
  - Unauthorised access
  - Jamming
- Countermeasures
  - Encryption
  - Access control



Wi-Fi - Eavesdropping

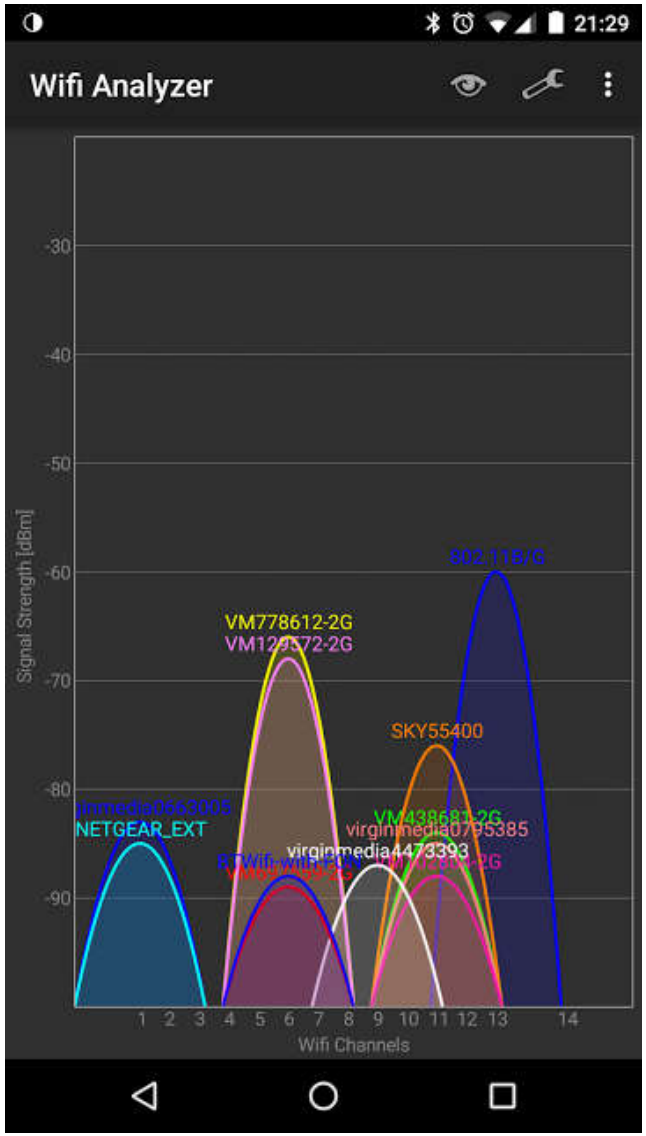
- Wi-Fi uses an open communication media (air) this makes it susceptible to eavesdropping
- Confidentiality is breached through unauthorised interception of radio signals
- Eavesdropping is a passive attack, data is unaltered and the user is unaware of the intrusion
- Due to the range of Wi-Fi the attacker can be some distance away (possibly miles with the correct antenna)

Wi-Fi – Unauthorised Access

- Unprotected shared file stores become vulnerable on wireless networks
- Attackers masquerade as authorised user (e.g. MAC Spoofing)
- Confidentiality and integrity of the network is breached
- Stolen device used to access the network
- Malware may propagate across wireless networks infecting connected machines
- Man-in-the-middle attack - gains access to user's communications
  - Two network cards to form a bridge, connecting users to the legitimate access point via the man in the middle
- Evil Twin attack – rogue access point poses as a legitimate one
  - Facilitate man-in-the-middle attack on HTTPS connections (provide bogus SSL certificate)
  - Facilitate phishing attack with bogus DNS server

Wi-Fi Jamming

- Radio interference can degrade or prevent transmission
- Interference can occur accidentally (Wi-Fi base stations, devices on the same frequency (2.5GHz / 5GHz)
- Deliberate jamming
  - High power covering a large frequency range
  - Low power targeting specific channels within a frequency
- DoS attacks, sending nodes into sleep mode



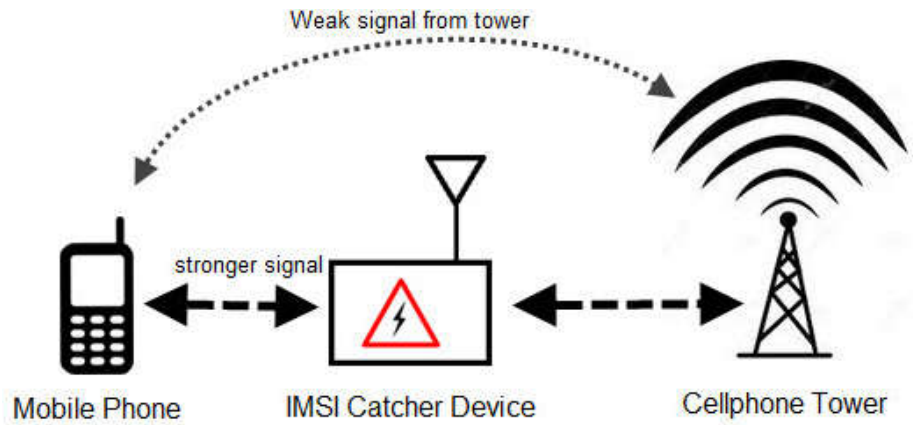
Wi-Fi Countermeasures

- Encryption
  - WEP – Layer 2 (Data Link Layer)
  - WPA - Layer 2 (Data Link Layer)
  - WP2 - Layer 2 (Data Link Layer)
    - Use AES rather than TKIP
  - VPN – Layer 3 (Network Layer)
- Access Control
  - MAC Filtering
  - Disable SSID (Service Set Identifier) broadcast
  - Radius server
    - More complex, allows policies, de-auth, LDAP / AD

GSM / UTMS / LTE

- Pervasive technology
- Provides
  - Voice
  - Data
  - SMS
- Uses unique USIMS / IMEI numbers
- GSM employs A5 stream cipher (broken)
- UTMS employs KASUMI block cipher (known weaknesses)
- LTE employs SNOW 3G stream cipher
- Further reading
  - http://spectrum.ieee.org/telecom/security/the-athens-affair

IMSI Catcher



- IMSI Catcher – Fake Cell tower performs MITM attack
- Catcher device masquerades as cell tower
- Forces mobile to communicate in plaintext
- Used by law enforcement and intelligence services & ???
- UTMS catchers force the mobile to fall back to GSM
- Controversial as any devices in the vicinity are compromised, not the just the target device.

Mobile Devices

- Mobile device use has increased dramatically over the last decade
- Mobile devices;
  - Small, and therefore
    - Easily lost / Stolen
  - Connected to high value gateway accounts
    - Personal email, corporate email
  - Always on, and always connected
    - Wi-Fi / LTE connects
  - Contain large amounts (GBs) of personally sensitive information

In Class Task

- Evaluate the security of your own personal mobile devices:
  - What threats do they face?
  - What threats to they pose to a business environment?
- Research some recent attacks on mobile devices and document the key lessons learned.

Mobile Device - Data

- Contact data
- Credentials
- Social Network Accounts
- Personal Diaries
- Access to cloud systems (iCloud, Google)
- Access to emails, and therefore access to payment methods
  - Identity theft / Account lockout

Mobile Device - Threats

- Malware attacks
- Wireless Network Attacks (ARP poisoning, Snooping)
- Theft
- Premium rate number scams
- Data leakage via apps

Mobile Devices - Mitigation

- Use of VPN on untrusted networks
- Secure device with a strong password
- Encrypt device storage
- Only install apps from trusted sources
- Be mindful of app permissions

Cloud Computing - Definition

- The National Institute of Standards and Technology (NIST) describe the following essential characteristics:
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service

  Source:
  http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Cloud Computing – Service Models

- The three broad service models are:
  - SaaS – Software as a Service e.g. Google Documents
  - PaaS – Platform as a Service e.g. Google App Engine
  - IaaS – Infrastructure as a Service e.g. AWS (Amazon Web Services)

Cloud Computing – Technical Overview

- Clouds are made up of a number of components:
  - Cloud Controller
  - Custer Controller / Storage Controller
  - Clusters
  - Nodes
  - Hypervisors
  - Virtual Machines

Cloud Computing Security Drawbacks

- Data dispersal and international privacy laws
- Loss of direct control of data / infrastructure
- Data ownership issues (who now owns the data?)
- Potential for increased attacks from hackers (clouds are viewed as high value targets)
- Exposure of data to foreign government agencies
- Multi-tenancy issues, other users may attack the system
- Insider threat from Cloud provider

Cloud Computing Security Benefits

- The cloud provide may provide a dedicated security team
- Cloud environments offer greater resiliency
- Offsite backup of data
- Hypervisor protection against attacks
- Widespread use of encryption for data in transit and at rest

B.Y.O.D – Bring Your Own Device

- As mobile devices have increased in popularity a trend of people using their personal devices for work has emerged.
- Overt usage
  - Employees are encouraged to use their own device, if they comply with policy
- Covert usage
  - Employees engage in business activities e.g. check email, on personal devices without regard for policy

B.Y.O.D. Threats

- Introduction of a new attack vector
- Loss of corporate control, inability to enforce policy on personal devices
- Malware Introduction via personal devices that may not be adequately protected
- Data Breaches, mobile devices with large storage capacities are easily lost or stolen
- Personal Threat- Corporate Control of Personal Device (Remote Wipe, Tracking)
- Breach of DPA – Employees my accidentally breach the DPA by mishandling customer data on their personal devices

B.Y.O.D Mitigation

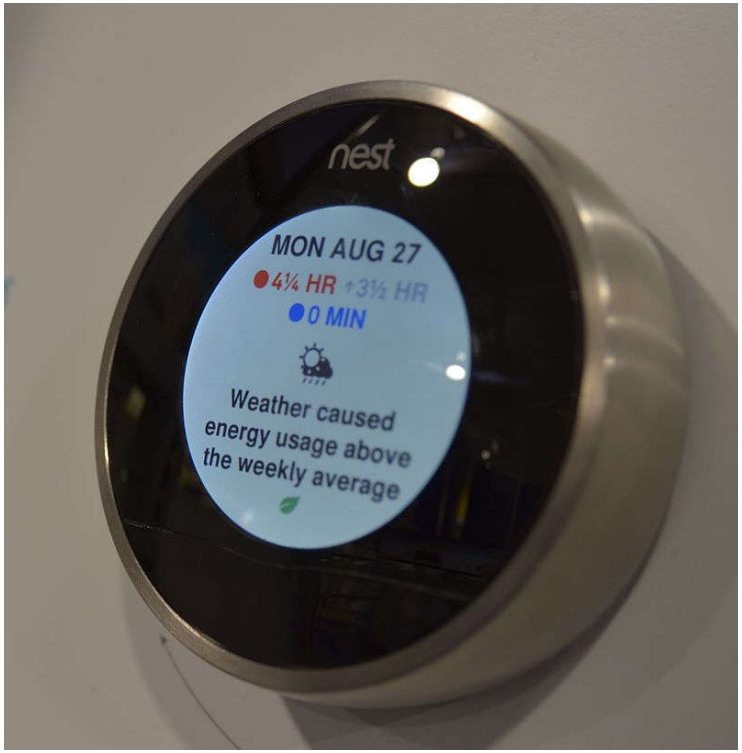
- Have a policy on what is and isn’t allowed with regard to B.Y.O.D.
- Secure containers e.g. KNOX
  - Hardware and software integrated security
  - Allow separation of personal and business apps and data
- Proportional remote wipe facilities
- Mandatory use of passwords / encryption
- Validate DPA compliance

IoT – Internet of Things

- What are IoT Devices?
  - “Non-PC”
  - Proprietary OS
  - Low Resource
  - Low Cost
  - Cloud Backed
  - Sensors / Control of Physical World Devices
  - Environmental Data aggregators?

IoT Devices

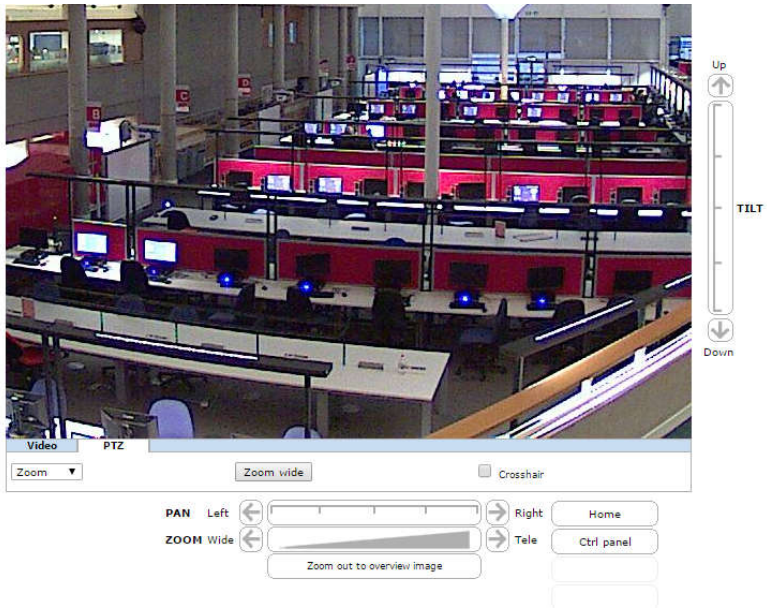
- Example Devices
  - Smart Appliances
    - Fridges, Cookers, TV's
  - Thermostats
  - Light Bulbs
  - Fitness Tackers
  - Vehicles
  - Locks



IoT Security Challenges

- Devices are opaque
  - Lack of control over data
  - Undocumented functionality
- Surveillance capitalism & Mass surveillance
- UPnP – Automated Reconfiguration of Networks
- Race to market = insecure devices
  - Default configuration
  - Vulnerable firmware
  - Lack of update mechanisms

IoT Threats & Risks



- Direct Threat - Ownership risk
  - Direct invasion of privacy via device
  - Backdoors / Foot holding points into network
- Indirect Threat - Internet Community risk
  - Threat from compromise devices forming botnets
  - Internet Infrastructure threatened
  - ISP’s and large targets may be taken offline

Mirai Botnet

- Mirai is a botnet of IoT devices
  - Used to launch record breaking DDoS attacks (1Tbps+)
  - Well documented attacks against Krebs & Dyn
- Used the DNS infrastructure to amplify attacks
  - http://tinyurl.com/hyff4w3
- Mapping Mirai
- http://tinyurl.com/jag69al

Vulnerable Devices (Mirai Botnet)

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Shodan

SHODAN | videoiq | Explore | Enterprise Access | Contact Us | New to Shod

Exploits | Maps

TOP COUNTRIES

United States	3

TOP SERVICES

HTTPS	2
HTTP	1

TOP ORGANIZATIONS

Microsoft Azure	3

Total results: 3

168.62.37.153
Microsoft Azure
Added on 2017-01-19 03:09:46 GMT
United States, Boydton
Details

SSL Certificate
Issued By:
|- Common Name: Starfield Secure Certificate Authority - G2
|- Organization: Starfield Technologies, Inc.
Issued To:
|- Common Name: view.myvideoiq.com

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-AspNetMvc-Version: 5.2
X-Powered-By: VideoIQ
X-Build-Id: 2.2.10.2804
X-Machine-Name: RD00155D47355E
X-Instance-Id: WebUI_IN_0
X-Powered-By: ASP.NET
Date: Thu, 19 Jan 2017 03:09:35 GMT
Content-Length: 18365
```

104.45.133.205
Microsoft Azure
Added on 2017-01-14 17:06:38 GMT
United States, Boydton
Details

SSL Certificate
Issued By:
|- Common Name: Starfield Secure Certificate Authority - G2
|- Organization: Starfield Technologies, Inc.
Issued To:
|- Common Name: view2.myvideoiq.com

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-AspNetMvc-Version: 5.2
X-Powered-By: VideoIQ
X-Build-Id: 2.2.10.2804
X-Machine-Name: RD000D3A125EB4
X-Instance-Id: WebUI_IN_1
X-Powered-By: ASP.NET
Date: Sat, 14 Jan 2017 17:06:27 GMT
Content-Length: 7885
```

IoT Mitigation

- Turn off UPnP
- Update device firmware if possible
- Research the vendor (Devices often rebadged)
- Create a separate network (Guest Network or Second Router)
- Change default passwords
- Read privacy policy associated with the device and cloud provider
- Device vetting, check if it is calling home?
- Don’t use the device in a sensitive network

Summary

- Wireless, Mobile, Cloud and IoT technologies all present potential threats to security.
- In order to preserve the security of a computer network using these technologies specific countermeasures, and mitigation strategies can be employed.
  - Encryption (Data in transit and at rest)
  - Policy
  - Access control
  - Network separation
  - Device configuration and vetting

Next Week

- Revision