Week 1 – Authentication, Authorisation and Access Control

Challenges of Cybersecurity

- No single simple solution exists for protecting computers and securing information
  - Try to protect the whole network
- Different types of attacks that computers face
- Difficulties in defending against these attacks

Difficulties in defending against attacks

- Universally connected devices - Everything is connected - IoT
- Increased speed of attacks - Computers are getting more powerful
- Greater sophistication of attacks
- Availability and simplicity of attack tools
- Faster detection of vulnerabilities - Companies must continuously release updates to perform security checks
  - Delays in security updating - Older version of products are much more vulnerable because updates may not work.
  - Weak security updates distribution
- Distributed attacks
- User Confusion

What is Cyber Security?

- Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access.
  - Task of securing information in a digital format
  - Ensures protective measures are properly implemented
  - Protected information with value to people and organisations

- CIA - Protections cyber security must provide
  - Confidentiality
    - Term for cyber security - No one else aside from senders and recipients should receive the message
  - Integrity
    - Keeping true to your moral principles, there should never be a change once claimed (Originality of the message)
  - Availability
    - If you belong to an organisation, you should have access to it at any time

(NOTE) Real Life Scenario - Is my company cyber secure?

Defining Cyber Security

- Addition to CIA triad
  - Authentication - Giving the details that belong to you - Only you know - Proof - checking identity
  - Authorisation - Access/privileges - what user can access
  - Accounting - Connecting every single piece of information (Form of logs) - Proof

Understanding Security

- When security is high = Lower convenience
- Reduce convenience before creating a security device as it improves it

Information Security Layers

- Information in the middle must be 100% accurate and always protected
- Organisations have rules e.g. visitors and badges

Cyber Security Terminology

- Asset
  - Something of value
- Threat
  - Type of action with potential to cause harm
- Threat Agent
  - Person or element with power to carry out a threat
  - Element -
- Vulnerability
  - Flaw or weakness that allows a threat agent to bypass security
- Exploit
  - The vulnerability though a threat vector
    - Threat vector - means by which attack can occur
- Risk
  - The likeli
  - Options of dealing with risk - Creating a plan - Some steps to consider to remove the risk
    - Risk Avoidance
    - Risk Acceptance
    - Risk Mitigation
    - Risk Deterrence

Understanding the important of cyber security

- Identity Theft
  - Stealing a person's information
  - Using information to impersonate the victim
  - Usually motivated by financial gain
  - Thieves can:
    - Create new bank or credit card accounts under the victim's name
    - File fictitious income tax returns in order to receive the victim's tax refund

Who are the attackers?

- Divided into several categories
- People who launch attacks to other users
- Targets individuals and business'
  - Cybercriminals
  - Script kiddies
    - Attackers who lack knowledge to perform attack on their own
    - Use automated attack software
    - Purchase exploit kit for a fee from hackers
    - Over 40% of attacks require low or no skills
  - Brokers
    - Sell their knowledge of vulnerability to other attackers or governments
    - Goals;
      - Break into computer or system
      - Take information without drawing attention to their actions
      - Possess excellent computer skills
  - Insiders
    - An organisation own employee
  - Cyberterrorists
    - Attacks may be ideologically motivated
      - For principals and beliefs
    - Almost impossible to predict when or where an attack may occur
    - Can be inactive for years and then suddenly strike
  - Hacktivists
    - Motivated by ideologies
    - Direct attacks at specific web sites

        - May promote political agenda
        - Don't threat public
    - State-sponsored
        - Governments instigate attacks against own citizens or foreign
- Surface web
    - Anything that can be found and indexed by a search engine
        - Textbook publisher website
- Deep web
    - Content that cannot be found by a search engine but only through a search dialog box on the site
        - e.g. - State medical license database
- Dark Web
    - Information that has been intentionally hidden and cannot be accessed through a standard web browser
        - e.g. - Black Market

Building comprehensive security strategy

- Practical security strategies
    - Block attacks
    - Update defences
    - Minimise losses
    - Stay alert

Terms

- DVL - Damn Vulnerable Linux
- Win12R2 - Windows operator
- DMZ - Demilitarised zone
- Without router we cannot connect with other networks - That's why we use pfSense
- ~ - home
- pwd - Personal working directory - tells where we are
- ls - list all files in the current directories
- mkdir … … …- makes a folder/directory, make sure not to put spaces when naming a folder because it will assume you want to create another folder
- cd - change directory
- man - gives information on how to use things

Week 1 Practical Notes:

- The first field is a dash (-) for a file or a (d) for a directory
- The 2nd through 4th fields are for the user's permissions
- The 5th through 7th fields are for the group's permissions
- The 8th through 10th fields are for others (accounts other than those in the group)

chmod command	Results
chmod u+rwx	Adds read, write and execute permissions for the user
chmod u+rw	Adds read and write permission for the user
chmod o+r	Adds read permission for others
chmod g-rwx	Removes read, write and execute permissions for the group

The other way of assigning permissions besides using symbolic permissions is the use of absolute permissions. Absolute permissions use a three-digit octal number to represent the permissions for owner, group and other. The table below outlines each absolute value and its corresponding permissions:

Number	Permissions
7	Read, Write and Execute
6	Read and Write
5	Read and Execute
4	Read
3	Write and Execute
2	Write
1	Execute
0	None

By typing the command, *chmod 764 <examplefile>*, the *examplefile* will be assigned the follow permissions:

- The user will get Read, Write and Execute permissions
- The group will get Read and Write permissions
- Others will get Read Access

Breakdown of how 764 represents these permissions:

Digit	Binary Equivalent	Permission
7 (user)	111	1-Read 1-Write 1-Execute
6 (group)	110	1-Read 1-Write 0-No Execute
4 (others)	100	1-Read 0-No Write 0-No Execute

Week 2 – Teamwork and Introduction to LINUX

Why TEAM work?
Together
Everyone
Achieves
More

- "Never doubt that a small group of thoughtful, committed people can change the world: indeed it is the only thing that ever has." Margaret Mead
- "Innovation is simply group intelligence having fun" - Tom Peter

What makes an effectives team?

- Good communication and social skills
- Positive interdependence
- Individual accountability/personal responsibility
- Group processing
- Shared goals
- Processes for conflict resolution

Stages of Team Development

- Forming
- Storming

    - Conflict may emerge between sub groups over leadership
    - Tension among the team
    - Fight or flight
- Norming
    - A sense of team identity develops along with trust
    - Team members begin to share ideas and objectives
    - They agree on what is to be achieved and commitment develops.
- Performing
    - Energy is now directed towards the task
    - It needs to be channelled and coordinated well
    - Vigilance re team processes is important
    - Give credit where it is due
    - Remember the introduction of any new members returns the team to the "forming" state
    - used-by-date

NOTE: Teams are dynamic

Deciding on Goals
- Charter or Constitution
- The Survey-Feedback method
- Critical Path Method

Building a team
- Get acquainted and feel comfortable with fellow members
- Develop rules and norms for the team
- Communicate and work cooperatively
- Facilitate the sharing of information and expectations between members
- Begin trusting each other

Roles of Team Members
- Clarity at the start helps to reduce friction-roles/ shared goals/ conflict resolution
- Allows people to get credit for their achievement's
- Clear responsibility and timelines for tasks avoids undue last minute pressure
- Roles need to be shared where possible to avoid boredom and assist in retention.

Factors critical for strong teams
- Team Goals
- Team Structure
- Roles within Teams
- Timelines for teamwork

Basic Team Skills
- Trust - Meet all commitments and maintain confidentiality
- Coaching - Using skills, knowledge and experience to assist others or ask for help
- Sharing Information- Assist others do their job
- Flexibility - Show a willingness to cooperate and help other when possible
- Good Manners: doing small, simple things

Team Communication
- Team members must communicate effectively amongst one another, Rely on each other as they are each other's internal customers.

- Internal Customers - Communicate with other teas at work
- External customers - Communicate directly

Communication Behaviours
- Assertiveness
- Listening Responsively
- Speaking Confidently
- Contributing to decisions

Communication Choices
- Aggressive - anger, blame and insensitivity to others.
- Dominating - Bossy and puts people's backs up
- Passive - Let others trample over you
- Restrained - may be inoffensive but does not fully take part in a team
- Assertive should be the aim in communicating within the team

Assertiveness
- Communicates clearly and honestly
- Expects that s/he has as much right as anyone else in team to be heard
- Can say 'no'
- Respects and listens to others
- Admits to errors without feeling s/he has lost face
- knows s/he deserves respect
- Gives the same rights to others as s/he claims for her/himself

Listen Responsively
- Part of assertive behaviour
    - Aggressive - always talks
    - Assertive - Listens and talks appropriately
    - Passive - Always listens

Speaking Confidently
- Team members contribute with honesty and integrity even though they disagree
- Be assertive - always think what could be right and wrong
- 'play the ball but not the person' - disagree with an idea not the person who thought of it.
- Acknowledge other people's ideas and contributions to help build the team
- Speak with enthusiasm, not emotion

Conflict Resolution
- Inability to resolve conflict the team may be splinter and sub-groups may form.
- Anticipate conflict - know what arises and have team strats to deal with it
- Importance of protocols to manage and conflict other problems
- "Don't blame the people. Blame the system."

Team Maintenance
- Coming together is a beginning
- Working together is a progress
- Staying together is a triumph

Week 3 – Password attacks and Defences

Password Attacks

- Username and password – main method of authentication to a computer system
    - Password – combination of letters and numbers only known to use
        - Not Considered strong

Password Weaknesses

- Humans memorise limited items = difficult memorisation on more complex passwords
    - Limited to few passwords for multiple accounts
- To combat this = Companies do a password cycle (forced to change)
- Characteristics:
    - Common Words
    - Short
    - Predictable
    - Memorisable
    - Repeated

Password Attacks

Type	Explanation
Digest	• Passwords stored on computer or website create a hash algorithm. This is attacks try to steal the file of the passwords on which it is stored.
Brute Force Attack	• Attackers attempt to guess a combination of letters and numbers to access someone's account, slowest but through.
Dictionary	• Attackers creates file of common words and is compares digests to stolen password fil.

Personal Security Defences for passwords

- Use strong passwords, which can be enhanced using password managers, such as;
    - Password generators
    - Online-Vaults
    - Password management applications

Creating strong passwords

- Avoid having dictionary words in password

- Avoids sequences or repeated characters
- Avoid nouns
- Avoid short passwords
- Use special characters that do not appear on keyboard such as hold alt + numeric pad (windows)

Week 4 – Social Engineering attacks and defences

Understanding Social Engineering attacks (Examples)

- Unexpected emails which usually ask the user to click the link
    - Clicking link may lead to your computer installing malware

- Call for help on someone you know
    - Sending money to attackers account

- Threats, intimidation through the use of texts
    - May provide bank details which will now be accessible to attackers

- A video showing a disaster and may ask for donations or download
    - Download may contain malware

Social Engineering

Gathering information needed for an attack by relying on human weaknesses, this is done by manipulating users to perform an action or gather information which will then be used by the attacker

Types of social engineering attacks

Term	Explanation
Phishing	• Spear phishing – Target specific users • Whaling – Target wealthy individuals • Vishing – Voice phishing (using voice) • Common Traits • Official logs • Web links • Urgent Requests
Type Squatting	• User accidentally making a typing error in an URL. Attackers may set up malware on that website.
Pretexting	• Attackers create a made-up scenario, persuading the victim to perform an action or provide information
Hoaxes	• Typically, first step in attack • Hoaxes can be seen as fake warnings, such as warn users that there may be harmful software on pc, forcing them to take action
Dumpster Diving	• Whenever attacks gain access to some user files, they may scan through it to see if there is any useful information that can be used to perform an attack, such as; • Calendars • Memos

	• Organisation charts • Directories
Shoulder Surfing	• Information entered is observed by another person

Identity Theft

The act of using someone's personal information to commit financial fraud

- Typical Actions of identity thieves
    - Produce counterfeits (Remove money from accounts)
    - Establish phone service under user's name
    - File bankruptcy under victim's name to avoid eviction
    - Purchase items with stolen cards or open bank under victim's name

Avoiding Identity Theft

Steps:

1) Deter theft by safe guarding information
2) Monitor financial statements and accounts

Best Practices:

- Shred documents
- Avoid carrying important identity cards in wallet
- Place personal information in a secured location
- Do follow up calls on suspicious purchases/activities
- Review Financial and billing statements on arrival

Legislations to assist users monitor financial information:

- Fair and Accurate Credit Transactions Act (2003) – allowing consumers free access to credit reports, finding any inaccuracies an agency has 30 days to respond with a corrected report

Social Networking Risks

- Due to computer gathering data on user, it may group individuals and organisations based on likes and interests. Linking them with one another
- Risks;
    - Malicious sue of personal data
    - Too trusting
    - Consequences of accepting friends

Defences for social Networking

- Mindful on what you post. E.g.
    - Travelling posts – promote burglary on your property
- Attention to information about new or updated security settings

Week 5 – Remote Hosts attacks and Defences

Ping of death history

- Known as **Denial of service (DoS)** – 1996
- Crashed computers when attackers send an IP packets larger than 65,536 bytes, they were malicious
- Only IP address was needed
- Countered by operating system vendors creating patches to solve the problem
- Many web sites continue to block **Internet Control Message Protocol (ICMP)** to prevent any future variations of this kind of attack

ICMP – Internet control message protocol

- Utilised by network devices
- Sends error messages and operational information

Blocking ICMP requests

- Adds a layer of security
    - Filter outbound ICMP
- Attackers can gain information in very little time if something is open

Firewalls

- Software-based personal firewall
    - Prevent malware entering computer
    - Analyses incoming data from the internet or local network
    - Filters content
    - Users manipulate permissions on programs to communicate across network

- Hardware-based network firewall
    - Protect entire network
    - Located at the edge of the network “First line of dense”

Function	Personal firewall	Network firewall
Location	Runs on a single computer	Located on edge of the network
Scope of protection	Protects only computer on which it is installed	Protects all devices connected to the network
Type	Software that runs on computer	Separate hardware device
Filtering	Based on programs running on the computer	Provides sophisticated range of filtering mechanisms

SSH – Secure Shell

It is a Cryptographic Network Protocol for operating network services secured over an unsecured network, purpose was to replace telnet.

- Access to shell accounts on Unix-like operating systems
- Encryptions for SSH intends to provide **confidentiality and integrity**

SSH History

- Edward Snowden leaked files – showing that SSH can sometimes be decrypted
- 6 July 2017 – US CIA developed hacking tools to crack SSH protocols

Attacks on SSH

Type	Explanation
Brute Force Attack	• Used to compromise accounts and passwords, which is often done by an automated program that tests combinations one at a time of usernames and passwords. • "Low and Slow tactic" recent trend – botnets that attack large numbers of servers = Large scale attacks

Defence on SSH

Type	Explanation
Brute Force Attack	• Utilise basic security practices • Make root password inaccessible via SSH connections: 'DenyUsers root' and 'PermitRootLogin no' in sshd_config file

Week 6 – Malware and Application Attacks and Defences

Malware

Defined as software that enters a computer system without owner's knowledge or consent, which would then perform unwanted and harmful actions

Primary trait of Malware

- Circulation/Infection
- Concealment
- Payload capabilities

Circulation of Malware

- Affect other devices connected to the same network
- USB flash drives can hold malware
- Send malware as an email attachment
    - If successful to connect, malware must implement itself into the system
- Types of malware include – Virus', worms and Trojans;

Action	Virus	Worm	Trojan
What does it do?	Inserts malicious code into a program or data file	Exploits a vulnerability in an application or operating system	Masquerades as performing a benign action but also does something malicious
How does it spread to other computers?	User transfers infected files to other devices	Uses a network to travel from one computer to another	User transfers Trojan file to other computers
Does it infect a file?	Yes	No	It can
Does it require user action to spread?	Yes	No	Yes

SHELLshock (Bashdoor)

Shell

Refers to a program that various Unix-based systems use to execute command lines and command scripts.

- Used in many internet-facing services – use bash to process certain task

SHELLshock

- Group of security bugs in the Unix Bash Shell
- Disclosed to public on 24th Sept. 2014
- Allows attackers:
    - Cause vulnerable versions of Bash to execute arbitrary commands
    - Gain unauthorised access to a computer system
- Privilege escalation – Offers users of a system to execute commands that should be unavailable

Concealment

- Rootkit
    - Set of software tools used by attacker
    - Conceals presence of malware
    - Change operating system to ignore malicious activity

- Tornkit rootkit
    - Set of programs – attacker gains unrestricted access to a compromised Linux system

Rootkit Hunter (RKhunter)

Unix-based tool that scans for rootkits, backdoors and possible local exploits

- Compare SHA-1 hashes of important files with known good ones in online databases
- Searching for default directories of rootkits

Payload Capabilities {

Primary emphasis of malware – focus' on what actions the malware performs

- Primary payload capabilities
    - Execute commands
        - Arbitrary code execution – payload allows an attacker to execute commands on victim's computer using shellcode which is a computer code.

    - Collect data
        - Malware designed to collect data from the user's computer by collecting information without consent – spyware, adware and ransomware

    - Delete data
        - Logic bomb – computer code – added to a legitimate program but lies dormant until triggered by specific event
        - Based on specific time or date

    - Modify system security settings
        - Backdoor - software code – access to program or service that circumvents normal security protections
            - Allows attackers to come back at another time

    - Launch attacks
        - Zombie – infected "robot" computer
            - Infected computer can be placed under remote control of an attacker
            - Botnet
            - Bot herder (attacker) controls zombies using HTTP commands

Technology	Description	Impact
Automatic download software	Used to download and install software without the user's interaction	May be used to install unauthorized applications
Passive tracking technologies	Used to gather information about user activities without installing any software	May collect private information such as websites a user has visited
System modifying software	Modifies or changes user configurations, such as the web browser home page or search page, default media player, or lower-level system functions	Changes configurations to settings that the user did not approve
Tracking software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information	May collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

Table 3-2 Technologies used by spyware

Keyloggers

Type of spyware that can capture keystrokes which is then sent to the attacker.

- **Hardware keylogger**
  - Installed between computer keyboard and USB port
- **Software keylogger**
  - Hides itself from detection by the user

Adware

Collects **user information** and delivers advertising content **unwanted** by user

- Done by – tracking function – monitors and tracks online activity – sends logs to third parties – deliver ads to users
- Bad because;
  - Display objectionable content
  - Slow down computer
  - Nuisance

Ransomware

The ability to prevent a user's device from properly functioning until a fee is paid

- Bad because
  - Locks up user's computer/device
  - Impersonates law enforcement agency
  - Official statements tell us that authorities do not ask for money over the internet

}

Malware that profits

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets. Zombies have the ability to download and execute a file sent by the attacker.
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.
Denying services	Botnets can flood a web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests.

Computer Defences

Users should implement;

- Managing patches
- Configure personal firewalls
- Install antimalware software
- Monitoring User Account Control
- Creating data backups
- Know how to recover from an attack

Managing Patches

- Patch
    - Software updates > improve/repair vulnerabilities

- Feature update
    - Enhancements software that add functionality

< Modern operating systems can perform automatic updates>

Installing Antimalware software

- Antivirus software
    - Scans computer for infections
    - Monitor computer activity
    - Examines documents
    - Matches known virus'
    - Update frequently

- Antispyware
    - Assist in preventing computers from becoming infected by different types of spyware

Monitoring User Account Control (UAC)

User account

- Indicates privilege level of a user

Types of user account

- Guest accounts
    - Allows least computer control
- Standard accounts
- Administrator accounts
    - Allows highest level of computer control

User Account Control

- Alerts user to operate system events
- Asks permission to perform tasks
- Assist – prevent Trojan from making changes
- Administrator can authorise changes
- **Reccommended config**
    - Set UAC to Always notify
    - Give standard accounts to other users on pc

Creating Data Backups

Term for **copying** data from computer's hard drive onto other digital media preferably in a secured location.

- These backups then can be used to restore computer to properly functioning state
- Assist in protecting against:
    - Hardware Malfunctions
    - User error
    - Software corruption
    - Natural Disasters

- **Backup Strats**
    - What data should be backed up
    - What media should be used
    - Where the backup should be stored
    - Frequency

- **Continuous Backups**
    - Performed continually without an intervention by the user
    - Performed online

- **Internet Services Available**
    - Automated continuos backups
    - Universal access
    - Delayed deletion
    - Online/disc-restore

    Advantage is that they can be performed automatically and stored at remote location

Recovering from Attacks

- Preperation
    - Key to recovering from an attack

- Windows systems
    - Recovery drive or system repair disc
    - Help repair windows in the event of a serious error

- Various software vendors provide free rescue discs
    - Downloadable images used to create bootable DVD

Week 7 - Web Application Attacks and Defence

How internet works

- Global network – devices connect to it can exchange information
- Not owned or regulated by any organisation or government entity
- Computers > co-op > make internet a global information resource

Internet Tools

- World Wide Web (WWW)
    - A.K.A web
    - Provides online information in specific format

- Hypertext Markup Language (HTML)
    - Web Authors = create websites using various tools

- Web Browser
    - Displays words, pictures and other elements on user screens

- Hyper Transport Protocol (HTTP)
    - Standards/Protocol utilised by webservers = HTML documents
    - Subset of Transmission Control Protocol/Internet Protocol Standards (TCP/IP)

- Web browser >>>>>> requests to a remote web server – Responds by sending the HTML document to users' local computer = Display

- Transfer-and-store process
    - Entire document >>>> stored on the local computer before display
    - This creates opportunities for sending different types of malicious code to the user's computer

Web Application Attacks

- Client-server software application – UI runs on web browser
- Common web app threats:
    - Cross site scripting (XSS) – Majority of attacks
    - SQL injections – Majority of attacks
    - DDoS
    - Cookie Poisoning

SQL Injection attack

- Gain access to Web apps by SQL code or statements to a web forum input box in a form of SQL query. Attacks can request for specific actions to be performed on a database
- Mostly known as **attack vector**
- Allows:
    - Spoof identity
    - Tamper with existing data
    - Cause repudiation issues such as voiding transactions or changing balances
    - Allow the complete disclosure of all data on the system
    - Destroy data = unavailability
    - Become admins

SQL Injection Defence

- Limit User access privileges
- Ensure employee security awareness
- Reduce debugging information
- Test web applications

XSS (Cross-site scripting)

Refers to web application making use of unvalidated or unencoded user input within the output it generates.

- Attacker execute malicious scripts (a.k.a malicious payload) into legitimate website or web application
    - Does not target user directly
- Aims to exploit vulnerability within a website or web application that the victim would visit

XSS Attack

- Attackers > Alter the HTML that controls the page by using Web forms that return error messages with user-input data
- Insert code – into a link in a spam message or use email spoofing in order to trick the user into thinking he or she is a legitimate, trustworthy source.

XSS Defence

- Prevention process must be developed during development
    - Web applications with solid secure development lifecycle methodology = Less likely to exhibit vulnerabilities
    - Test application code before deployment

    - **Threat Modelling**
        - Evaluates and Identifies risks
        - Increase Web developer's security awareness

    - **Scanning**
        - Source-code-scanning tools and Web application-vulnerability scanners
        - Custom application code must still be reviewed manually

- Web Developers filter user input
    - Remove possible malicious characters and browser
    - Install user-input-filtering code to remove malicious characters

- Administrators able to configure browsers – accept scripts from trusted sites or disable browser scripting

Week 8 – Configuring the Web Browser and Server

Directory Traversal

- Type of HTTP exploit which aims to access files and directories that are stored outside the web root folder
- Security mechanisms that web servers use to restrict user access:
    - Root Directory
        - Top-most directory on server file system /var/www
        - User access – confined to root directory meaning cannot access directories outside of the root

- Access Control Lists (ACLs)
    - Utilised by administrators – define user access rights and privileges for viewing, modifying and execute files.

Directory Traversal Vulnerability

- Insufficient filtering/validation of browser input from users
- Located in web server software/files or application code that is executed on the server
- Variety of programming languages
- Detection of vulnerability scanning and manual penetration testing techniques

Directory Traversal Prevention

- Trained programmers that are able to validate user input from browsers
- Filter out certain user inputs
- Web Server software – keep up-to-date with current patches

Email

Types of Email Systems

- Simple Mail Transfer Protocol (SMTP)
    - Handles outgoing mail

- Post Office Protocol
    - Responsible for incoming call

- Internet Mail Access Protocol (IMAP)
    - Recent and advanced system
    - + Remains on email server and does not downloaded to user's computer
    - Organised into folders on server
    - Read any device
    - Version 4

- Email Attachments
    - Docs attached to an email message
    - Encoded in a special format
    - Single transmission when send

Email Risks

- Spam
    - Unsolicited email
    - Lucrative business = cost little to send
    - Botnets
- Can be countered using spam filters – however image spam can bypass this
- Effects of spam
    - Loss of productivity
    - Lost of money on spam filter software

- Malicious attachments
    - Files sent with email
    - Once opened = infected computer
    - Replicate themselves
- Embedded Hyperlinks
    - Hyperlink within email
    - Directs users to a website (may look legitimate) and trick user into providing personal info

Internet Security Risks

- Variety of risks from using the internet
    - Browser Vulnerabilities
    - Malvertising
    - Drive-by-downloads
    - Cookies
    - Email risks

Browser Vulnerabilities

- Static content viewed early days (information does not change)
- Dynamic Content is commonly used now
- Script code – computer executing commands – most popular javascript
- **Javascript** Embedded in HTML Doc | Executed by browser |
    - Defence mechanism to avoid harm – cannot read, write or delete from local comp
    - Malicious = capture and sent information without users knowledge

Defense	Explanation
Limit capabilities	JavaScript does not support certain capabilities. For example, JavaScript running on a local computer cannot read, write, create, delete, or list the files on that computer.
Sandboxing	By only permitting JavaScript to run in a restricted environment ("sandbox") this can limit what computer resources it can access or actions it can take.
Same origin	This defense restricts a JavaScript downloaded from Site A from accessing data that came from Site B.

Extensions

- Expand normal capabilities of web browser for a specific webpage
- Mostly written in JS
- Wider access privileges when running webpage
- Browser-Dependent
- Plugin - Adds Functionality
- Java – Programming language and create applets
    - Applet – Stored on web server but downloaded on pc
    - Performs tasks

Add-Ons

- Adds functionality to entire browser and can;
    - Create web browser toolbars
    - Change browser menus
    - Process content

Name	Description	Location	Browser Support	Examples
Extension	Written in JavaScript and has wider access to privileges	Part of web browser	Only works with a specific browser	Download selective links on webpage, display specific fonts
Plug-in	Links to external programs	Outside of web browser	Compatible with many different browsers	Audio, video, PDF file display
Add-on	Adds functionality to browser itself	Part of web browser	Only works with a specific browser	Dictionary and language packs

- HTML5 standardizes sound and video formats

- Some web browser block plug-ins

Malvertising

- Attacks use third party advertising networks – distribute malware on users web browsers
- Advantages:
    - Utilisation of big named networks
    - Web owners unaware
    - Difficult to determine if advertisement was culprit of attack

Drive-By Downloads

- Term used for an attacker attempting to directly infect website
- Users computer = infected by viewing
- Attackers – Inject malicious content
- Invisible to naked eye

Cookies

- User – specified files – created on server
- Stored locally
- First party cookie
    - Created by website user is viewing
- Third Party
    - Come from web site advertisers
- Locally shared Object (LSO)
    - More complex than regular cookie

Security and privacy risks of cookies

- First party cookies – stolen and impersonal user
- Third party cookies – track users browsing

Defences related to internet security

- Defence against Internet-based attacks happens by having computer properly secured
    - e.g. patches, configure firewalls, anti-malware software and etc
- Once secured, few extra steps to consider:
    - Securing web browser
    - Maintaining email defences
    - Follow internet security best practices

- **Securing Web Browsers**
    - Configure Web browser settings
        - such as; browsing data, extensions and etc

- **Types of Defences**
    - Spam filtering
    - Setting security options in client-based email programs and web email

- **Internet Security Best practices**
    - Downloading files from well-established organisations
    - Controlling cookies
    - Private browsing

Week 9 – General Cryptography Concepts

Privacy:

- The state or condition of being free from public attention to the degree that you determine
- **Today** data is collected on almost all actions performed by the user through web surfing, purchases, user surveys and questionnaires

Risks associated with Private Data

1. Individual inconveniences and identity theft
    - Impersonate victim for personal gain

2. Associations with groups
    - Use personal data to place individuals in groups based on similar interests

3. Statistical inferences
    - More in-depth than groupings

Issue	Explanation
The data is gathered and kept in secret.	Users have no formal rights to find out what private information is being gathered, who gathers it, or how it is being used.
The accuracy of the data cannot be verified.	Because users do not have the right to correct or control what personal information is gathered, its accuracy may be suspect. In some cases, inaccurate or incomplete data may lead to erroneous decisions made about individuals without any verification.
Identity theft can impact the accuracy of data.	Victims of identity theft will often have information added to their profile that was the result of actions by the identity thieves, and even this vulnerable group has no right to see or correct the information.
Unknown factors can impact overall ratings.	Ratings are often created from combining thousands of individual factors or data streams, including race, religion, age, gender, household income, zip code, presence of medical conditions, transactional purchase information from retailers, and hundreds more data points about individual consumers. How these different factors impact a person's overall rating is unknown.
Informed consent is usually missing or is misunderstood.	Statements in a privacy policy such as "We may share your information for marketing purposes with third parties" are not clearly informed consent to freely allow the use of personal data. Often users are not even asked for permission to gather their information.
Data is being used for increasingly important decisions.	Private data is being used on an ever-increasing basis to determine eligibility in significant life opportunities, such as jobs, consumer credit, insurance, and identity verification.

Privacy Protections

- Protections may be implemented to reduce the risks associated with private data
    - **Cryptography**
        - Provides five basic protections
            - Confidentiality
                - Secrecy
            - Integrity
                - Resistance to changes
            - Availability
                - Should be accessible to only the person
            - Authentication
                - Verifying Identity of the person
            - Nonrepudiation
                - Sender cannot deny that he/she has sent something

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key.
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key.
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information.
Authentication	Provides proof of the genuineness of the user	Proof that the sender was legitimate and not an imposter can be obtained.
Nonrepudiation	Proves that a user performed an action	Individuals are prevented from fraudulently denying that they were involved in a transaction.

Cryptography (Broader)

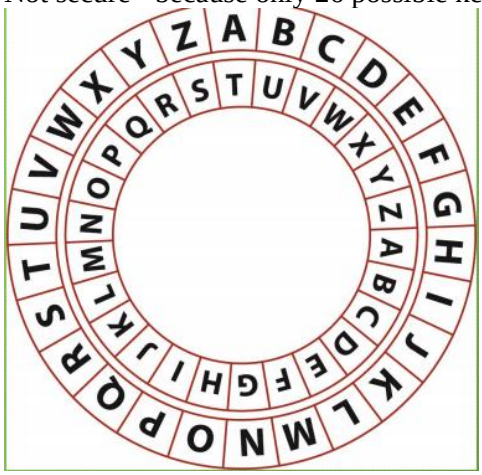
- It is the art and science of secret writing, encrypting or hiding information from attackers
- Cryptanalysis process of attempting to break a cryptographic system and return the encrypted message to its original form
- Plain text to Ciphertext is known as encryption

Terms	**Explanation**
Plaintext	A piece of data that not encrypted
Ciphertext	Output of an encryption algorithm
Cipher	A cryptographic algorithm
Algorithm	Step-by-step, recursive computational procedure
Key	Sequence of characters or bits used by an algorithm to encrypt or decrypt a message
Encryption	Change plaintext to ciphertext
Decryption	Changing ciphertext to plaintext

- **Cryptographic Algorithms**
  - Every encryption scheme = algorithm
  - A.K.A Encryption Algorithm or cipher

- **Keys**
  - Special pieces of data used in both the encryption and decryption processes
  - Algorithms stay the same - different key is sued
    - Ensures data is secure even with algorithm is known
  - Complex key = greater security
  - Key space - Possible
    - Key complexity is achieved by giving the key a large number of possible values

        - Defined as bits
        - 1024 bits = 2^1024 different keys

- **Types Of Ciphers**
    - Shift
        - Used algoprithm and a key
        - Specifies that you offset the alphabet either to the right (forward) or to the left (Backward) - Specified how many letters the offset should be
        - A.K.A Caesar Cipher
        - Not secure - because only 26 possible keys
        - 

        - $x \mapsto x + k \pmod{26}$
    - Substitution
        - Developed because more complex then shift
        - Ciphers work on the principle of substituting a different letter for every letter
    - Transposition
        - Letters of original message are rearranged by applying some sort of permutation
    - Affine Ciphers
        - Similar to shift cipher but strong than Caesar
    - Vigeneres
        - Complex cipher as it corrects the issues with more simplistic keys
        - Works as a polyalphabetic substitution cipher dependent on a password

Type of Cryptography - Hashing

- Hash Algorithms
    - Hashing functions
    - Collision attacks
    - Algorithms: SHA, Message Digest
- Hash Algorithm is secure if:
    - Fixed size
    - Unique
    - Original
    - Secure
- Hashing functions used for:
    - Storage of comp passwords
    - Ensure message integrity
- Reproducible by anyone IF running the same algorithm against same data
    - Leading too:
        - Creating file – get hash – send has file to someone – run file and get hash value – hash values match = success

Collision Attack

- Attack used to compromise a hash algorithm
- Occurs when attack = discovers two different messages with same hash value
- Requires generating a separate algorithm = Very difficult
- Hash functions suffers from collision = loss of integrity
- Attacker trick people into running malicious code by making two different inputs hash to the same value

SHA

- SHA = Secure Hash Algorithm
- *National Institute of Standards and Technology (NIST)* and *National Security Agency (NSA)* published four hash algorithms
    - FIPS – 180-2
- Applies compression function to data input
    - Accepts 2^64 bits or less then compresses it down to smaller number of bits

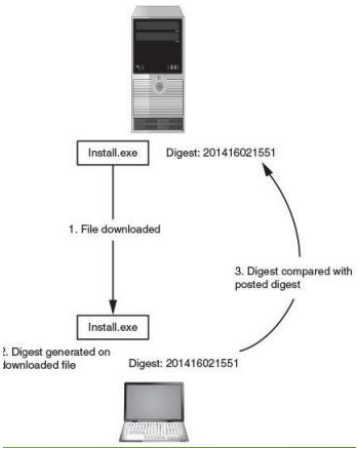
Variants of SHA

- SHA-1 secure hash function however most vulnerable to collision attack
- SHA 2 = SHA 224, 256, 384,512
    - Longer hash = more difficult to attack
    - Requires more processing power
- SHA – 3 standards released by NIST – August 5, 2015

Block Method

- Algorithms use block mode = process data to create the hash
- Breaking down data into sets of bits (512 bits)
- E.g. 1400 bits long creates three blocks

Message Digest



- Used for comparison
- Algorithms: SHA series and Message Digest (MD)
- Versions: MD2, MD4, MD%
- Message Digest (MD) generic version of one of several algorithms that are designed to create message digest or hash from data input into the algorithm.
- MD work similar to SHA
- Developed by Ronald L. Rivest
- MD2
    - Dev. 1989
    - Takes data of any length – produces hash output off 128 bits
    - Optimised for 8-bit machines
- MD4
    - Developed in 1990
    - Optimised = 32-bit computers
    - Faster algorithm however more subject to attacks
    - Vuln. To collision
- MD5
    - Developed 1991
    - Slow but more secure
    - Creates 128-bit hash of a message of any length
    - Segments message into 512-bit blocks

Week 10 – Cryptography 2

Symmetric Encryption = Definite on exam

- Both keys for encryption and decryption are the same
- Designed = encrypted and decrypt cipher text
- a.k.a private key cryptography
- It is a copy of a physical lock - analogy
- Weakness';
  - You can intercept the key, anyone can open the post or misplaced
  - Simple keys can be brute-forced
  - Secure key exchange = maybe issue
- Asymmetric encryption = Different keys to encrypt and decrypt the message, slower because of complex algorithm but more secure

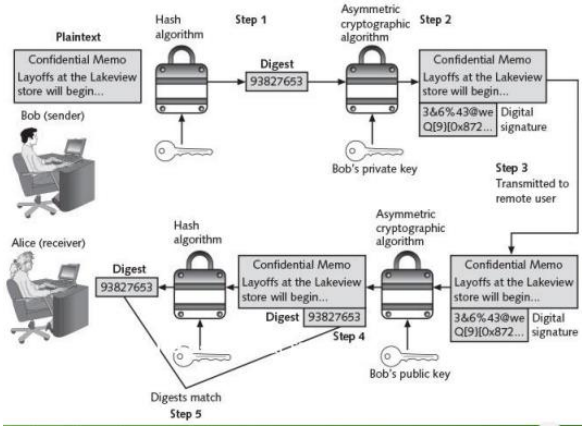
- **Data Encryption Standard (DES)**
  - Dev. 1983 | Federal standard in 1976
  - Block cipher - 64 bits block cyber
  - 56-bit key length = Brute force, attacker only needs to attempt 2^56 to get into
  - Performs a substitution and permutation based on key 16 times on every 64-bit block

- **3DES**
  - Triple DES = Variation of DES
    - Uses either two or three
    - Multiple Encryption = 3
    - Longer key length = greater resistance - brute force attack

- **Advanced Encryption Standard (AES)**
  - Block cipher - separates data into 128-bit blocks
    - configured to 192 or 256 bits
    - Longer key versions known as AES-192 and AES-256
    - Secure - No efficient attacks

Asymmetric Encryption = Definite on exam

- A.K.A = Public key cryptography
- Uses two keys - 1 public, 1 private
- Mathematically related = Prime number theory = numbers divisible by 1 or by itself only
  - Works by using hard math problems
  - Common method relies = factoring large numbers
  - Comps = cannot easily factor the product
  - Public key = known to everyone
  - Private key = known to individual
  - Security relies = reducing to one key
  - Works in both directions (encryption and decryption)
- When sending confidential messenger sender > recipient, always use recipients key
- Ability to send messages securely WITHOUT prior contact
- Asymmetric Algorithms;
- Creates possibility of digital signatures and corrects the main weakness of symmetric cryptography
  - RSA

- **RSA**
  - Founded = Ron Revest, Adi Shamir and Leonard Adelman
  - First Public Key system = 1997
  - Encryption and digital signatures
  - Uses product of two primary number (Between 100 and 200 digits long and of equal length)
  - Larger prime umber = more secure
  - Slow = does not replace DES
  - Asymmetric encryption = Exchange symmetric Keys = makes RSA faster
- **Diffie-Hellman**
  - Created 1976 - Whitfield Diffie and Martin Hellen
  - Most common
  - Used for:
    - Electronic key exchange
- **Digital Signature**
  - Electronic verification of the sender
  - Verify sender
  - Prevent sender from disowning the mess
  - Prove integrity of message
  - Based on both hashing functions and asymmetric cryptography
  - Aim to achieve authenticity
  - Enable faster and more efficient exchange
  - 

Using Cryptography

- Encryption through software
  - Methods;
    - Individual files
    - File system
    - Whole disk encryption
- **Hardware based encryption**
  - Cannot be exploited like software
  - Cryptography embedded in hardware = higher security
  - Will not connect to computer until correct password is submitted
  - All data = automatically encrypted
  - Admins. control and track activity
  - Compromised/stolen can be deleted

Responsibilities of Organisations

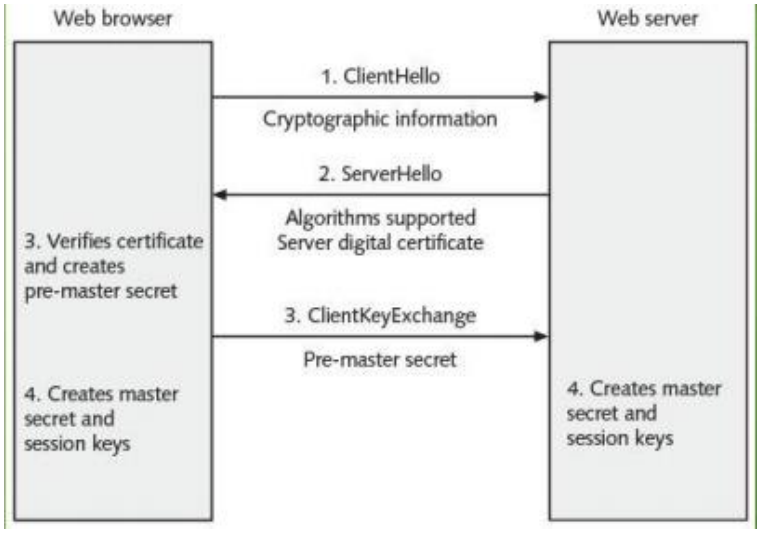
Example of misuse	Responsible action	Explanation
During the online registration process the organization required new users to provide both their email address and the password to that email account, and then stored the information in cleartext.	Collect only necessary personal information.	Organizations should not collect any personal information unless it is absolutely necessary, and the information that is collected should be limited.
An organization collected customers' credit and debit card information to process transactions in its retail stores but then stored that information for 30 days, long after the sale was complete.	Keep personal information only as long as necessary.	Unless there is a legitimate business need, personal information should be securely disposed of as soon as any transactions are completed.

Example of misuse	Responsible action	Explanation
An organization used actual personal information in employee training sessions and then failed to remove the information from employees' computers after the training was completed.	Do not use personal information when it is not necessary.	Fictitious information should be used for any for training or development purposes.
Over 7,000 files containing users' personal information were inadvertently sent to a third party by an organization that had failed to restrict employee access to sensitive personal information.	Restrict access to sensitive information.	If employees do not need to use customers' personal information as part of their job function, access to such information should be denied.

Action	Whose key to use	Which key to use	Explanation
Bob wants to send Alice an encrypted message	Alice's key	Public key	When an encrypted message is to be sent, the recipient's, and not the sender's, key is used.
Alice wants to read an encrypted message sent by Bob	Alice's key	Private key	An encrypted message can be read only by using the recipient's private key.
Bob wants to send a copy to himself of the encrypted message that he sent to Alice	Bob's key	Public key to encrypt Private key to decrypt	An encrypted message can be read only by the recipient's private key. Bob would need to encrypt it with his public key and then use his private key to decrypt it.
Bob receives an encrypted reply message from Alice	Bob's key	Private key	The recipient's private key is used to decryp received messages.
Bob wants Susan to read Alice's reply message that he received	Susan's key	Public key	The message should be encrypted with Susan's key for her to decrypt and read with her private key.
Bob wants to send Alice a message with a digital signature	Bob's key	Private key	Bob's private key is used to encrypt the hash.
Alice wants to see Bob's digital signature	Bob's key	Public key	Because Bob's public and private keys work in both directions, Alice can use his public key to decrypt the hash.

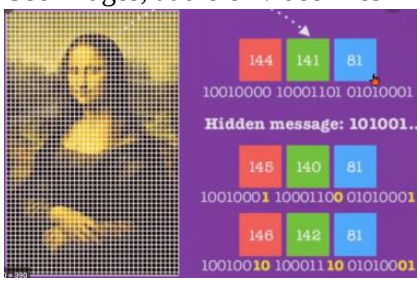
Using Cryptography

- Encrypt through software
    - Individual Files
    - File system
    - Whole Disk Encryption
- Hardware Encryption
    - Harder to exploit
    - Cryptography embedded on hardware = higher security
- Digital Certificates
    - Technology = associate a user's identity to a public key
    - Digitally signed – third party trusted
    - Server digital certificates often issued from a web server to a user's client computer
        - Ensure ethnicity of web server
        - Ensure authenticity of cryptographic connection to the web server
    - Extended Validation SSL Certificate (EV SSL)
        - Enhanced type
        - More extensive Verification
        - Web browsers – Indicate to users



Steganography

- Term used for hiding text messages through pictures
- Difficult to detect
- Does not attract attention
- Tools to detect: Stegdetect, StegSecret, SegSpy and SARC tools

- Hides existence of data
- Use images, audio or video files
- 

Week 11 – Wireless Devices

- 4/5 web searches performed on mobile devices
- Wireless networks = prime target because unprotected wireless signal = attackers capture packets

Mobile Attacks

- Attacks directed to wireless networks = Affect mobile Devices

Attacks Through Wireless Networks

- Wireless networks (popular)
  - **Wi-fi** - Wireless local area network - works by using radio frequency for wireless transmissions
  - **Bluetooth**
    - Short range - 10 metres
    - Bluetooth attacks:
      - Blue Jacking - Sending unwanted messages to blue-tooth enabled devices
      - Bluesnarfing - Accessing unauthorised information

- IEEE - responsible for establishing Wi-Fi standards
-

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 & 5 GHz	5 GHz
Nonoverlapping channels	3	3	23	3	21	21
Maximum data rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	7.2 Gbps
Indoor range (feet/meters)	65/20	125/38	115/35	115/35	230/70	115/35
Outdoor range (feet/meters)	328/100	460/140	393/120	460/140	820/250	460/140
Standard ratification date	1997	1999	1999	2003	2009	2014

- Wi-fi Equipment
  - Wireless Adapter - For mobile to connect to internet
  - Software - Translate between device and adapter
- Wireless broadband router
  - Base station - send and receive signals
  - Gateway to internet

- Access Point
  - Used in business or school setting
  - Signal - transmitted ONLY several hundred feet

    - Multiple AP's = providing cells (area of coverage)
    - Moving from one cell to another = Roaming

- Risks from attacks on home-based Wi-Fi networks:
    - Reading wireless transmissions
    - Viewing or stealing computer data
    - Inject malware
    - Download Harmful content
- War Driving
    - Terms used for when searching for wireless signals from a vehicle or on foot using computing device
- Free wireless = rarely protected
- Evil Twin
    - Mimics authorised Wi-Fi device
    - Users unknowingly connect to mimicked wi-fi device
    - Attackers - send malware to victims computer

Category	Bluetooth Pairing	Usage
Automobile	Hands-free car system with cell phone	Drivers can speak commands to browse the cell phone's contact list, make hands-free phone calls, or use its navigation system.
Home entertainment	Stereo headphones with portable music player	Users can create a playlist on a portable music player and listen through a set of wireless headphones or speakers.
Photography	Digital camera with printer	Digital photos can be sent directly to a photo printer or from pictures taken on one cell phone to another phone.
Computer accessories	Computer with keyboard and mouse	A small travel mouse can be linked to a laptop or a full-size mouse and keyboard that can be connected to a desktop computer.
Gaming	Video game system with controller	Gaming devices and video game systems can support multiple controllers, while Bluetooth headsets allow gamers to chat as they play.
Medical and health	Blood pressure monitors with smartphones	Patient information can be sent to a smartphone, which can then send an emergency phone message, if necessary.

Portable computers

- Web-based computers e.g. laptops
- Additional risk: Theft - common in airports

- **Tablets**
    - Portable computing device
    - Touch screen
    - Designed for user convenience
    - Have OS

- **Smartphone**
    - Features of phone with additional stuff to access apps and internet
    - 2/3 = smartphones

- **Wearable Technology**
    - Worn by user
    - Commonly used as fitness tracker
    - A glancing machine ?

Mobile Device Risks

- Installing unsecured apps
    - Apple IOS - difficult for attackers = proprietary architecture
    - Good Android OS - open and not proprietary - easier for attackers
- Limited Physical Security

    - Devices - easily stolen or lost = unprotected data could be stolen
- Connecting to public networks
    - Attackers eavesdrop data transmission
- Location Tracking
    - Increased risk of targeted physical attacks
- Accessing Untrusted Content
    - Phones - can access untrusted content

Mobile Defences
- Protect wireless networks
- Protect Wireless devices

Wireless Network Security
- Secure configure home wireless network
    - Turn on Wi-Fi Protect Access 2 (WPA2)
        - Provides - optimum wireless security
        - Encrypts the signal
        - Prevention of unauthorised users from accessing network

- Secure the wireless Router
    - Use password - protect access to its internet configuration settings

- Router remote management settings
    - Configure through internet

- Disallow remote management unless needed

- Wi-Fi protected setup (WPS)
    - Methods of configuring security
        - PIN
        - Push-button

- Security settings that strengthen WPA2 security
    - Changing SSID to anonymous value
    - Turn guest access - Isolate main network from guest network
        - Users connected to guest network only access internet directly and other devices in the guest network

- Public Network Security
    - Watch for evil twin
    - Limit the type of activity
        - Simple web surfing - watch videos
    - Use Virtual Private network
        - Uses unsecured public network as if it were a secure private network
    - Configure Bluetooth
        - Disable/enable only when necessary
        - Set device as undiscoverable

Securing Mobile Devices
- Device setup
    - Disable unused features - threat vectors
    - Enable lock screen
- Best Practices
    - No jailbreaking
    - Do not sideload unapproved apps

    - Dispose devices properly
    - Back up data properly
    - Never call phone numbers contained in unsolicited emails or text messages
    - Be aware of threats using mobile devices

- Device Loss or theft
    - Keep phone out of sight
    - Avoid distraction on device
    - Use both hands holding device
    - Change to less conspicuous colour
    - Contact organisation and wireless carrier to change all passwords on device if stolen

Security feature	Explanation
Alarm	The device can generate an alarm even if it is on mute.
Last known location	If the battery is charged to less than a specific percentage, the device's last known location can be indicated on an online map.
Locate	The current location of the device can be pinpointed on a map through the device's GPS.
Remote lockout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen.
Thief picture	A thief who enters an incorrect passcode three times will have her picture taken through the device's onboard camera and emailed to the owner.