**Exam Review**

**Chapter 1 – The Threat Environment**

* **Confidentiality**: unauthorized people cannot read sensitive information, whether it is on a computer or over a network
* **Integrity**: attacker cannot change or destroy information, in worst case, the data will still able to retrieve or recover
* **Availability**: authorized person have access to what they are given
* Employees know about the system, avoid detection, also have permission to access sensitive data, sabotage, financial theft, theft of Intellectual Property
* **Malware**: generic name for any “evil software”
* **Viruses**: insert malicious code into a legitimate software, transfer infected file into victim’s device, infect others file
* **Worm**: exploit vulnerabilities on apps or OS, travel via network, can affect victim device without interaction
* **Trojan**: malicious code hidden in a program, require user action to activate the trojan
* **Payloads**: code that will do heavy damage, carried by viruses or worm
* **Trojan** **Horse**: replace existing file on device, remotely control the device, use the device to download more trojan, including spyware (collect personal information, cookies, keystroke, password,…), rootkits (taking root control, hard to detect since it is hidden)
* **Social** **Engineering**: attempt to trick user to do something against security policies, such as spam, phishing email, hoaxes, demand for personal information, spamming email with trojan embedded
* **Espionage**: attack on confident, steal information and public it, can be done via multiple way, including bribe employee, hacking, hire ex-employee
* **Cyberwar**: attacks by national governments, only target to damage financial and communication infrastructure
* **Cyberterror**: attack by organized terrorist, usually attack on government website to express an opinion or to give a certain situation an attention

**Chapter 2 – Planning & Policy**

* Required a formal procedures to secure the hosts, must taken all methods attacker could use to exploit, must renew and review procedures at least once a year, as it could be old and affect operational use.
* Security Developer must have a vision and acknowledge the role, cooperate with other security at another firm to strengthen the systems. They must treat user to understand the role of security and never underestimate them. Most of the time, user are the one that cause the vulnerability, so working with user is the best option.
* Identify security gap, develop a plan compliance with corporation or provincial laws and regulations, determine the solution and execute
* **PIPEDA** (Chapter 2 Slide 21)
* Chief Security Officer (CSO) or known as Chief Information Security Officer (CIO), located within IT dept. requires compatible technical skills, responsible for security, located outside IT dept. will have less control, more independence to provide protection. Hybrid is place planning, policy making and auditing outside, operational aspect inside IT
* Risk analysis weights the probable cost of compromises against the costs of countermeasures. (Chapter 2 Slides 36-49). Traditional risk analysis couldn’t calculate the exact value as all the related value are flexible, therefore it is hard to estimate the ARO
* **Total Cost of Incident (TCI)** related to many other cost such as lawsuits, related factor not just the asset itself
* One countermeasure could protect many resources, one resources could have many countermeasure
* **Risk Reduction**: install countermeasure to avoid attacks or threats
* **Risk Acceptance**: accept the lost of countermeasure is too much compared to ARO
* **Risk Transference**: buy insurance to cover the lost, security must still taken seriously and do not depend on insurance company to cover the lost amount
* **Risk Avoidance**: avoid taking risky action, but sometimes risky action in security could bring a huge return
* **Defense in depth**: multiple independent countermeasure must be defeated in series
* **Weakest link**: single countermeasure with multiple interdependent components must succeed for the countermeasure to succeed.
* Always apply security to all part of IT, do not assume attacker might ignore some part
* Security policies required multiple department who is related, such as legal department, business department, IT department to involves and come up with a policies. Since security developer only focus on security but not other aspect, this will help them to have a better viewpoint when applying security
* Control the **policies making**, decided if it should be a guidelines or standard. Provide flexibility in planning and doing but ensure not to much room for flexibility. Exception is allow but required confirmation and approve from many people
* **Governance Frameworks** (Chapter 2 Slide 76)

**Chapter 3 – Cryptography**

* **Cryptography**: use mathematical operations to encrypt the data when travelling from one host to another
* **Confidentiality**: someone who intercept has the data cannot read it
* **Integrity**: cannot intervene with data or else it will leave a mark and notice the sender/receiver
* **Authentication**: proving identity to decrypt and read the data
* **Cipher** is mathematical method to encrypt and decrypt data, each host need to know the key to decrypt the data
* **Substitute** **Cipher**: substitute one letter/bit for another in each place
* **Transposition** **Cipher**: change the order of the string
* **Standard public key** are 512 or 1024 bit long
* Step for Key Encryption for Confidentiality (Chapter 3-2 Slide 1)
* **Cryptographic System Handshake Stage (Chapter 3-2 Slide 2)**
  + **Stage 1**: **Selecting Security Methods and Parameter** (Chapter 3-2 Slide 4)
  + **Stage 2**: **Authentication** use hash as a way to compare password for authentication (Chapter 3-2 Slide 5),
  + **Stage 3**: **Keying** (Chapter 3-2 Slide 6)
  + **Stage 4: On Going Connection** message end-to-end encryption. User know opponent’s public key and decrypt the message when it arrives.
    - **Digital Signature:** apply hash and sender’s private key so that supplicant know the true party’s private key. Supplicant when receive the message can use the hash provided by sender to test with hash received in text, then decrypt the message using true party’s public key.
    - **Message Authentication Code (MACs):**

**Chapter 4 – Security Network**

* **Availability:** users have access to information service and network resources
* **Confidentiality:** prevent unauthorized users from gaining information about the network
* **Functionality:** preventing attackers from altering the capabilities or normal operation of networks
* **Access Control:** keep attackers or unauthorized employees from access internal resources
* **Denial-of-Service (DoS)**: send a flood of attack message to victim, shutdown server or network by overloading it.Harms could include loss of sales, reputation, productivity,… DoS has 2 means of attack: to stop critical service (usually happen between competitor) and slowly degrading service (bring the harm to a company without their notice yet).
* Condition to perform a DoS is attack must have more resources than the victim**.** Usually, the attacker generate the resources via botnet which control the affected computer and perform the attack as the attacker command. A bot or botnet can “represent” the attack to perform the action commanded by the attacker (Chapter 4 Slide 18)
* **Direct DoS:** flood victim with a stream of packet directly from attacker’s computer
* **Indirect DoS**: spoof own IP, use chain-of-attack to flood the victim (Chapter 4 Slide 14)
* **DoS attack step:** Chapter 4 Slide 22
* **Defense DoS:** limit traffic in one host to the server, perform TCP handshake (incoming connection sending an SYN, firewall confirm and send back SYN/ACK to server, when server response with a legitimate ACK back, original SYN will be send from firewall)
* **Address Resolution Protocol (ARP) Poisoning:** manipulate host to reroute LAN traffic, require a person to be on LAN system to intervene (Chapter 4 Slide 28).Since all host are in LAN traffic, they are considered “trusted” to each others so authentication or verification is require. Step by step procedure is at (Chater 4 Slide 31).Preventing ARP can be done by limiting the local access to each others IP or manually apply static ARP table
* **Corporate Lan** (Chapter 4 Slide 34), **Ethernet and 802.1x** (Chapter 4 Slide 35), **Extensible** **Authentication** **Protocol (EAP)** (Chapter 4 Slide 36), **Wireless Network Access** (Chapter 4 Slide 37), **Unauthorized Wireless Access** (Chapter 4 Slide 39), **Evil Twin Access Point** (Chapter 4 Slide 40), **VPN Protection Against Evil Twin Aps** (Chapter 4 Slide 41), **Wireless DoS** (Chapter 4 Slide 42), **Extended EAP Protocol** (Chapter 4 Slide 44), **802.11 Core Security Protocol** (Chapter 4 Slide 45)
* **Wired Equivalent Privacy (WEP):** each station use the same access point use the same share key. All encryption is done by that key and knowing the key can authenticate the user.Dangerous because it provide almost no protection for user and WEP doesn’t provide automatic rekeying and reapply new key to system. Since one key is shared among group, somebody could leak it out
* **False 802.11 Security:** (Chapter 4 Slide 49)

**Chapter 5 – Access Control**

* **Authentication:** supplicant sends credentials to verifier to authenticate the supplicant
* **Authorization:** determine permission authenticated user have and only allocate those resources
* **Auditing:** record what is happening in log file to understand what is going on with the system
* **Credential =** password = fingerprint = access card = location
* **Mandatory Access Control (MAC):** no departmental or personal ability to alter access control rules set by higher authorities
* **Discretionary Access Control (DAC):** departmental or personal ability to alter access control rules set by higher authorities
* **MultiLevel Security:** data has multiple level such as Public: Sensitive but unclassified, Confidential, Secret, Top Secret
* **Piggybacking:** follow an authorized user to access into the system
* **Verification:** compare access data to single template for identity check
* **Identification:** compare supplicant data to all templates in DB to find result
* **Deception:** when a subject is trying to fool the system, such as fingerprint or face recognition
* **Fingerprint:** simple, inexpensive, convenience, popular but can easily be defeated by glass copied or tape, however, generally it is better than traditional password
* **Iris Scanner:** pattern colored part of eye, required a camera, expensive and low FAR
* **Face Recognition:** use to fully detect a person, very low chance of deception, high error rate (human face change all the time, they can look similar to many person)
* **Least Permission:** Authentication (proof of identity), Authorization (specific authorization and permission) and Auditing (what the person did). Authenticated doesn’tmean Authorizied. It is better to not give a permission than giving an extra. Logging will be used to monitor action.

**Chapter 6 – Firewalls**

* **Firewall** must have a strong capacity as well as speed to handle all of the incoming connection, especially for corporation when they can process millions of connection at the same time. When there is bottleneck at Firewall, Firewall will automatically drop all of the packet and treat them as threat (safety purpose)
* **Static Packet Filtering:** check one packet at a time, look at the transport header, can avoid packet using spoof IP or non-sensical field setting
* **Stateful Packet Inspection:** connections has distinct states and stages. Different states use different filtering rules and therefore can avoid different type of attack.
  + **Access Control List (ACL):** series of rules to allow or disallow connection. Rules are followed by order and when there is a rule apply, it will send the packet to follow that rule. If the firewall reach the last rule in ACL it will follow that rule.
  + If a connection specified more than 1 port, allow all connection within the port. If the connection specified a port and an IP, only allow single connection. The rest disallow
* **Firewall** will automatically hidden user’s IP and replace that with the firewall IP to protect user from getting attack.
* **Intrusion Detection Systems (IDSs)** check for suspicious traffic and send an alarm to notify user. Almost all incoming packet are treated as suspicious traffic, user usually ignore because there are too many alarm. Always update program and attack signature to prevent further event. Increase speed performance and storage hard drive to keep up with network traffic and log file written
* **Intrusion Prevention System (IPSs)** use IDS filtering mechanisms to filter incoming packet with potential of “somewhat likely”,”very likely” or “provable” dangerous. User can stop the traffic to avoid a possible attack
* **DMZ** required all incoming traffic to pass through it before heading to the firewall, it is known as a subnet for servers and application proxy firewalls. It must be strong to handle all of the incoming connection because that will be the first point attacker will attack

**Chapter 7 – Host Hardening**

* **Host** is any device that contain an IP address
* Minimize application running to minimize the attack, install patch when available, manage permission carefully, encrypt data, add extra firewall, check log file
* Determine a baseline and specification to harden, use different baseline for different OS and different server functions.
* **Use VM** to reduce the attack chance, to share resources if necessary
* **Vulnerabilities**: a security weakness spot allow attack to create an exploit, can only determine if an attack is planted. Apply patches and fixes to fix the issue. Sometimes, patching can cause problem and must be select careful which one to use
* Always do **vulnerability testing** (with permission) to exploit any security issue, ensure to run on a separate machine that if there is something happen, it doesn’t affect the system

**Chapter 8 – Application Security**

* Many application are running with super user (root) permission, therefore, when an attack takes over an application, they can execute command with the same privileges
* **Application hardening** require more work than OS hardening (1 OS hardening can protect many application). Careful with the services running on PC, especially hidden ones
* Minimize the **permission** and avoid default installation from unknown program
* Add **extra layers** of authentication, authorization and auditing
* Always **filter user input** for safety purpose, especially place where it connect with server
* **Buffer Overflow Attacks**: specified action are needed in some coding language to avoid attack, however, some doesn’t.
* **Login Bypass**: enter a URL or SQL query to bypass the server, to trick the premade query
* **Cross-Site Scripting (XSS)**: One user send an anonymous data type or script to server. The server store the information and when somebody request an access to that data, the server will send the scripting packet to the user company and damage the computer
* **SQL Injection**: use a SQL query to execute command in database. If the attacker known the structure of SQL, they can easily perform an attack using just SQL query to extract and read the data
* User who understand directory structure can use URL as a way to access into root data of a server and access many more detail of the root, including file contain secret information
* Avoid user to perform any action, especially in URL to traverse around the system. Action such as .. is dangerous and should be filter out in multiple way (character, hex, unicode)
* Apply patch for software, or component software patch, use vulnerability assessment tool, read error log or place the webserver as DMZ are protection should apply for website
* **Dancing Pig** argument are malicious link that persuade the victim to click to. It's usually similar to what user is looking for on that page (ex. Download button)
* **File** **reading**: turn victim computer to unintended file server, executing command on CMD
* **Redirection**: automatic redirect to unwanted page
* **Cookies**: use to track users at website and their behaviour
* **Content Filtering**: filter malicious code such as HTML bodies tag, suspicious attachments (.exe or programming file)

**Chapter 9 – Data Protection**

* **Image Backup**: backs up everything and it takes some times
* **Shadowing**: backup copy of each file worked on every few minutes to a safe location
* **Full Backup**: extensive from Image Backup, include all files and directories
* **Incremental Backup**: only record changed since last backup, daily work
* Backup console 🡺 software 🡺 hardware 🡺server 🡺client
* **Continous Data Protection (CDP)**: 2 server backup data of each other continously
* Redundant Array of Independent Disks (RAID): any RAID require at least 2 disk
  + **RAID 0**: write information across multiple disk, take advantage of speed
  + **RAID 1**: write a copy on each disk, take advantage of restoration
  + **RAID 5**: combination of RAID 0 + 1, required 4 disk
* **XOR’ing**: require at least 3 disk, break the data and store across the disk. Use the part from 2 disks and apply XOR’ing to calculate the value and store in the other disk. When 1 disk is die, it can use the other 2 disk to figure out the data lost
* **Create Backup policies**, including how, which method, where to backup, restoration policies, encryption type, and most importantly, access control to backup data.
* **Restrict who can access to DB**, especially DB structure, to avoid any attack or data leak, only fetch DB data via DBMS and all data must formated before sending out. Rename admin account to something unique, disable guest or public account
* **Key Escrow**: store a copy of the key (for decryption) in a safe place
* **Data Loss Prevention (DLP)**: use policies, procedures and systems designed to avoid data leaking
* **Personally Identifiable Information (PII)**: information that can use to uniquely identify a person, include name, personal identification number, address, photo,...
* Knowing a few information can have a high chance to identify the actual person

**Chapter 10 – Incident and Disaster Response**

* At some point, the security protection is no longer work and an attack could happen. For that event, must determine the incident severity
  + **False Alarms**: an incident believe to be happening but it is not, known as false positives, will be handle by on-duty staff
  + **Major Incident**: an actual breach happen, require Computer Security Incident Response Team (CSIRT)
  + **Disaster**: nature disaster occur, must remain business activity, required experienced person to perform and handle the event to keep the business running
* The faster the **Security team response** to the event, the less damage will be. However, during such event, team members might be panic and will make a wrong decision. Therefore, accuracy is also required to save the system from an attack.
* Should **planned for such event**, decided the roles, procedures without pressure. Plan must be flexibility for any inaccuracy human decision-making. Practice and rehearse the plan when possible
* **Major Incident**
  + **Detection**: detect to determine the source of attack (by technology or human)
  + **Analysis**: analyze the attack with guildlines and plan prepared. Determine the scope is very important to determine which guildline to follow
  + **Escalation**: if the situation is getting out of hand, transfer work to CSIRT or business continuity immediately
* **Containment**: disconnect the system from network site to avoid further attack, this should be taken carefully as business operation will stop after this. Or another approach is to collect the data as the approach going on to understand the motive if it is unclear
* **Recovery**: ensure backup is always available and ready to restore. Depends on the scope of the attack, a total software reinstallation might be required to ensure no current software is suffering from malware or rootkit
* **Punishment**: depends on the sources of attack and person who is responsible, can either fire an employee or blaming the system. Seek for expert if need help
* **Honeypot**: a fake server/entire network segment with fake clients and server to simulate the attack and research on it
* When deciding for business continuity, Business and IT dept. has to work together to determine if keeping the firm operation or restore the the firm is better choice.
* **Flexibility and Communication** are the 2 factor determine if a plan is success or not. Determine the business process and prioritization processes such as downtime tolerance, have at least part of the resource running to handle the request
* As **business growing**, there will be more work for security. Therefore, always update the plan at least once a year to match with the business growing progress so that when a breach is out, everything will be under control. Always have important information available such as contacting person, people who responsible,…
* **IT Disaster Recovery**: determine a backup facilities that can get IT dept. to recover and continue the operation.
* Type of Backup Facilities
  + **Hot Site**: A **hot site** is a **backup facility** which represents a mirrored copy of the primary production center. A **hot site** is equipped with all the necessary hardware, software, and network connectivity, which allows you to perform near real-time **backup** or replication of the critical data.
  + **Cold Site**: A **cold site** is the least expensive type of **backup site** for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up.
  + **Site Sharing**: **Backup sites** can come from three different sources: Companies specializing in providing disaster recovery services. Other locations owned and operated by your organization. A mutual agreement with another organization to **share** data center **facilities** in the event of a disaster.

**Extra Chapter – Data mining and release**

* **Data Disclosure**
  + **Exact Data:** provide without any modification or protection
  + **Bound of the data:** provide a data of a range
  + **Existance:** only display if the result is true for existance or false for not
  + **Probability:** chance of something could happen
* **K-anonymity (Chapter extra – Slide 14)**
* **L-diversity (Chapter extra – Slide 15)**