

Tutorial 1: Introduction

1.

Vulnerability	A weakness in the security system. For example, as in the case of procedures, design and implementation that can be exploited easily to cause loss or harm to the information security.
Threat	A set of circumstances to the computing system that possess the potential to cause loss or harm to the computing system.
Control	A control is an action, device, procedure, or technique that reduces or removes the vulnerability.

2.

Data integrity	System integrity
Assures that information and programs can be changed only in a specified and authorized manner	Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

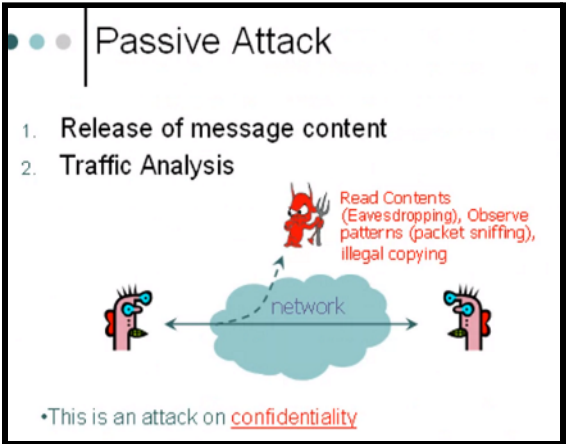
3.

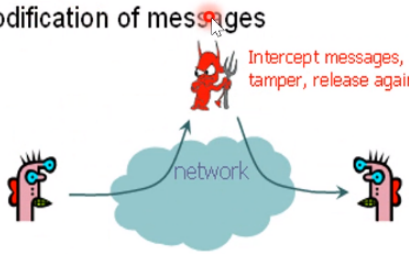
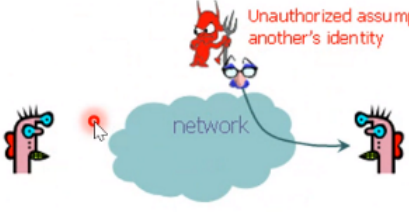
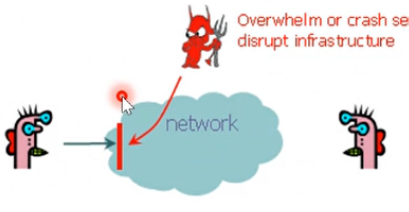
Threat	Attack
Threat is a potential violation of security (or potential security harm to an asset) which exists when there is a circumstance, capability, action or event that could breach security and cause harm.	<p>An attack is a threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security, or threat consequence. The agent carrying out the attack is referred to as an attacker, or threat agent</p> <p>An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt to evade (avoid) security services and violate the security policy of a system.</p>
Unauthorized disclosure	Modification of message

4.

Passive attacks	Active attacks
<p>Passive attacks have to do with eavesdropping on, or monitoring, transmission. Electronic mail, file transfer, and client/server exchanges are examples of transmission that can be monitored.</p> <p>The threat of unauthorized disclosure of information without changing the state of the system.</p>	<p>Active threats include the modification of transmitted data and attempts to gain unauthorized access to computer systems.</p> <p>The threat of the deliberate unauthorized change to the state of the system.</p>

5.

No.	Attacks	Image Explained
Passive Attacks		
1.	<p>Release of message contents - files or data with confidential information is leaked to an attacker during transit.</p> <p>Traffic Analysis - Monitoring information traffic (even if the message is encrypted) in or to determine the location and identity of communicating hosts, and the frequency and length of messages being exchanged. This information can be used to guess the nature of the communication that was taking place.</p>	

Active Attacks		
2.	Replay - passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.	<div data-bbox="938 277 1523 730"> <div> <div>Active Attack</div> <div> <div>2. Replay (without tampering)</div> <div>3. Modification of messages</div> </div> <div>  <p>Intercept messages, tamper, release again</p> <p>•This is an attack on <u>integrity</u></p> </div> </div> </div>
3.	Modification of Messages - some portion of a legitimate message is altered, or messages are delayed or reordered, to produce an unauthorized effect.	
4.	Masquerade - takes place when one entity pretends to be a different entity.	<div data-bbox="938 772 1523 1226"> <div> <div>Active Attack</div> <div>1. Masquerade</div> </div> <div>  <p>Unauthorized assumption of another's identity</p> <p>•This is an attack on <u>authenticity</u></p> </div> </div>
5.	Denial of Service - prevents or inhibits the normal use or management of communication facilities.	<div data-bbox="938 1268 1523 1722"> <div> <div>Active Attack</div> <div>4. Denial of Service</div> </div> <div>  <p>Overwhelm or crash servers, disrupt infrastructure</p> <p>•This is an attack on <u>availability</u></p> </div> </div>

6.

- **Confidentiality** - To access the account, he/she must provide the password which is available only to authorized users and aimed at further enhancing the level of security. This system must ensure privacy whenever communication happens between the online internet banking system and bank server. The entire transaction needs to be secured properly to avoid harm. Proper encryption of password ensures a high level of confidentiality. The policy related to changing password after regular intervals will help boost the customers and keep data and information secure.
- **Integrity**- The online banking system should update chronologically with authentic data and does not affect the data in the customer account in any manner.
- **Availability** - Availability is required to ensure timely and reliable access for making payments, online instant transfer and many more. So that it is able to improve the satisfaction of the customer who uses the online banking system

Sample answer from tutor:

- The system must keep personal identification numbers confidential, both in the host system and during transmission for a transaction.
- It must protect the integrity of account records and of individual transactions.
- Availability of the host system is important to the economic well-being of the bank, but not to its fiduciary responsibility. The availability of individual teller machines is of less concern.

7.

Network attack surface	Software attack surface
<ul style="list-style-type: none">- Vulnerabilities over an enterprise network, wide-area network, or the Internet.- Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.	<ul style="list-style-type: none">- Vulnerabilities in application, utility, or operating system code. [Web server software.]

Past year questions

8. (i)

Computer security	Internet security
Protects the confidentiality, integrity and availability (CIA) of the information system assets (i.e hardware, software, firmware, and information/data being processed, stored and communicated)	It is one of the types of computer security that measures to prevent, detect and correct security violations that involve information transmission over the internet.
E.g. <i>Antivirus and Antimalware programs</i> which protect computers from viruses and malicious applications.	E.g. <i>Firewall</i> which controls the incoming and outgoing traffic over the network according to the predetermined security rules. Intrusion Detection/Prevention System

(ii)

The importances of understanding computer security and internet security are:

- May help to understand what and which appropriate security approaches to be applied correctly.
- To tackle and prevent future threats and attacks
- To ensure our data is safe and secure both in computer and Internet

9. Yes, I agree with this statement. This is because insiders (employees) can access the sensitive information on a regular basis and know how the data (trade secret, intellectual property, customer and vendor list, etc) is protected and security measurement of the organization. They can remove or damage the information easier than the outsider.

Sample answer: Agree. Insider attack is hard to detect and prevent because the attacker knows the system well to cover up an attack.

10.

Authentication	Authorization
The determination of the identity or role that someone has.	The determination if a person or system is allowed access to resources, based on an access control policy.
Smart card, password, biometric - fingerprint, etc	Role based access control, discretionary access control, mandatory access control

Tutorial 2: Malicious Software

1. Explain three **broad mechanisms** that malware can use to **propagate**(传播).
 - Infection of existing viruses that is then spread to other systems.
 - Exploit of software vulnerabilities either locally or over a network by worm, SQL Attack or drive-by-downloads to replicate malware.
 - Social engineering attacks that convince users to bypass security mechanisms to install Trojan or to respond to phishing attacks.
2. Explain four **broad categories of payloads** that malware may carry
 - Corruption of system or data files.
 - Theft of service in order to make the system a zombie agent of attack as part of a botnet (僵尸网络).
 - Theft of information from the system such as logins, password and personal information by keylogging or spyware programs.
 - Stealthing(潜伏者) where the malware hides its presence on the system from attempts to detect and block it.
3. What characteristics of an advanced persistent threat give it that name?

Attackers use a variety of intrusion technologies and malware to attack the target victim. Sometimes, a customized malware will be developed if it is required. The individual components may not necessarily be technically advanced but are carefully selected in order to suit the chosen target. Moreover, APT uses a slow approach to maximize the chance of success, continuously monitoring data communications. The main purpose of the attackers is to gain intellectual property, security and infrastructure.

Sample answer:

- **Advanced:** Use of a wide variety of intrusion technologies and malware, including the development of custom malware if required.
- **Persistent:** Application of attacks over an extended period against the chosen target in order to maximize the chance of success.
- **Threats:** A result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets.

4. Describe the phases of operation of a virus or worm.

Dormant phase: The virus is inactive until an event causes it to be activated. Note that not every virus will have this stage.

Propagation phase: The virus places a copy of itself into more programs or system areas on the disk.

Triggering phase: The virus is activated to perform the planned function.

Execution phase: The virus carries out some target functions such as destruction of programs and data files.

5. Describe the mechanisms that a virus uses to conceal (隐藏) itself.

There are 4 mechanisms for the virus to conceal itself which are encryption, stealth, polymorphism and metamorphism.

Encryption - The virus will use a random encryption key to encrypt itself.

Stealth - The virus hides itself from being detected by the system.

Polymorphism - The virus will change with each infection to avoid being detected by a signature.

Metamorphism - The virus will rewrite itself entirely at each iteration to increase the complexity of detection.

6. Suggest various ways a worm uses to access remote systems to propagate.

- **Electronic email attachments or instant messages file transfer** that include macro or script code that allow worms to copy itself.
- **File sharing** on removable media such as USB drives, CD and DVD data disks.
- **Remote execution** explicitly or through a program error in a network service.
- **Remote file access or transfer capability** to copy from one system to another.
- **Remote login capability** acts as a user and uses commands to copy itself from one system to another.

7. Differentiate between machine executable and macro virus.

Machine executable viruses infect executable program files to carry out their work in a manner that is specific to a particular operating system and specific hardware platform whereas macro viruses infect files with macro or scripting code that is used to support active content in a variety of user document types, and is interpreted by an application.

8. Explain the meaning of the term clickjacking and discuss its implications(effect).
Clickjacking, also called UI redress attack, is a vulnerability in which keystrokes can be hijacked. The implications of clickjacking includes mirroring a usual form that lets the user believe they are typing in the password in that input form but they're actually entering the fields that are already controlled by the attacker.
9. Differentiate “drive-by-download” with a worm.
- A drive-by-download exploits vulnerabilities in the browser so that when a user views a web page or HTML email message controlled by an attacker, it contains code that exploits the browser bug to download and install malware on the system without user consent or knowledge.
 - It differs from a worm since it does not actively propagate as a worm does, but rather waits for unsuspecting users to visit the malicious web page in order to spread to their systems.
10. Describe a botnet.
- Botnet (aka robot network) is defined as a network of computers infected with bot malware without users’ knowledge. It enables the attacker to use the computer to launch distributed denial-of-service attacks, phishing campaigns or spam.

Sample answer:

- Collection of bots capable of acting in a coordinated manner.
 - Takes over another internet attached computer and uses that computer to launch or manage attacks.
11. Differentiate between a backdoor, a bot, a keylogger, spyware and a rootkit. Can they all be present in the same malware?
- Backdoor:** A back door is a piece of software that allows access to the computer system by passing the normal authentication procedures. There are two groups of backdoors. The first group works much like a Trojan which is manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload.
- Bot:** A bot is a remotely controlled malware program that is installed onto a computer without the knowledge or consent of the computer's owner secretly taking it over. This type of program may have complete control over the operation of that computer and its Internet functions, but usually does not reveal its presence to the computer's owner or users, or try to interfere with the normal operation of that computer.

Keylogger: Captures keystrokes on the infected machine to allow an attacker to monitor this sensitive information. Since this would result in the attacker receiving a copy of all text entered on the compromised machine, keyloggers typically implement some form of filtering mechanism that only returns information close to desired keywords (e.g., "login" or "password" or "paypal.com").

Rootkit: A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding. This provides access to all the functions and services of the operating system. With root access, an attacker has complete control of the system and can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand.

Spyware: Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.

12. Differentiate between “phishing” attack and “spear-phishing” attack, particularly in terms of who the target may be?

Phishing attack uses a spam email to exploit social engineering to leverage user’s trust by masquerading as communications from a trusted source, that may direct a user to a fake website or to complete some enclosed form and return in an email accessible to the attacker.

Spear-phishing attack is an email claiming to be from a trusted source. However, the recipients are carefully researched by the attacker, and each email is carefully crafted to suit its recipient specifically, often quoting a range of information to convince them of its authenticity. This greatly increases the likelihood of the recipient responding as desired by the attacker.

The difference between “phishing” and “spear-phishing” attacks is the matter of victim targeting. To illustrate, the phishing attack targets any possible recipients which is not customized to every recipient (low effort) whereas spear phishing takes much effort as the recipients are carefully researched by the attacker to suit the recipient specifically.

13. Suggest some malware countermeasures.

- **Prevention** which does not allow malware to get into the system in the first place or blocking its ability to modify the system through policy, awareness, vulnerability mitigation and threat mitigation.
- **Detection** to determine that the malware has occurred and locate it.
- **Identification** to identify the specific malware that has infected the system.
- **Removal** to remove all traces of malware virus from all infected systems.

14. Propose places malware mitigation mechanisms may be located.

- On the infected system, where some host-based “antivirus” program is running, monitoring data imported into the system, and the execution and behaviour of programs running on the systems.
- As part of the perimeter security mechanisms used in an organizations firewall and intrusion detection systems
- Use distributed mechanisms that gather data from both host-based and perimeter sensors, potentially over a large number of networks and organizations.

15. Explain four generations of antivirus software.

First generation: Simple Scanners

- Requires virus signature to detect/identify a virus
- Limited to known virus
- Maintain record of the program and monitor changes

Second Generation: Heuristic Scanners

- Does not rely on specific signature and use heuristic rules to search for probable virus
- For example, it looks for code fragment that often associated with virus, beginning of encryption loop and encryption key

Third Generation: Activity Traps

- Memory-resident program that identify a virus by its action rather than its structure
- Not necessary to develop signature and heuristics for wide array of viruses

Fourth Generation: Full-featured protection

- Packages consists of a variety of antivirus techniques
- Include scanning and activity trap components and access control capabilities

Past year question

16. (i)

Rootkit	Backdoor
A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding. This provides access to all the functions and services of the operating system. With root access, an attacker has complete control of the system and can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand.	A back door is a piece of software that allows access to the computer system by passing the normal authentication procedures. There are two groups of backdoors. The first group works much like a Trojan which is manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload.

(ii) It is because the attacker can gain access to a system without going through the security access procedures to perform an attack on the targeted victim.

Sample answer:

- Backdoor is a secret which bypasses all security mechanisms and allows attackers easy access without getting caught.

(iii)

- Ensure security policy is in place
- Ensure all systems are as current as possible, with all patches applied
- Set appropriate access controls on the applications and data stored on the system, to reduce the number of files that any user can access and hence potentially infect or corrupt, as a result of them executing some malware code
- User awareness and training - aims to equip users to be more aware of these attacks, and less likely to take action that result in their compromise.

17.

(i) Phishing is the act of sending an email and claiming to be a legitimate organization that tricks users into giving their personal information.

(ii) The credential information such as pin number/password, credit number number, name, social security number, etc

(iii) slide 57

- Install an antivirus software and keep it up-to-date
- Call the company or institution to verify the email
- Never click on the link that are suspicious
- Add suspicious email to spam email

(iv)

- Research the recipients carefully
- Craft the email carefully to better suit its recipient specifically, often quoting a range of information to convince them of its authenticity.

(v)

- Personalized greetings with the recipient's name
- Inconsistencies in Email Addresses, Links & Domain Names
- Information quoted closely match the recipient's environment

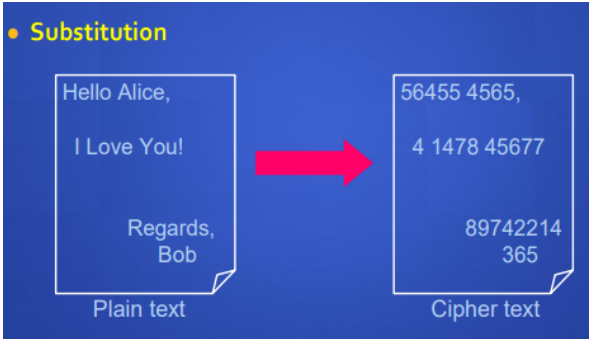
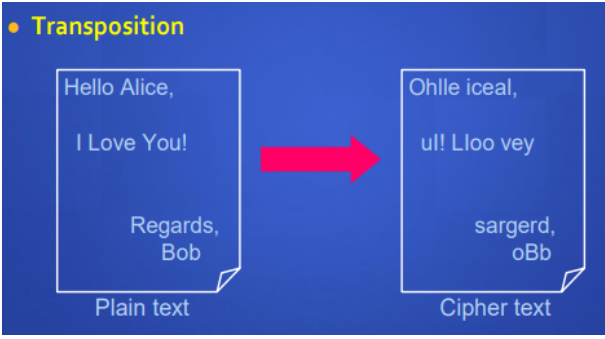
Tutorial 3

1. Explain the essential ingredients of a symmetric cipher.
 - Plaintext: Original message
 - Encryption algorithm - Perform various substitution and transformations
 - Secret key - Input to algorithm
 - Cipher text - Coded message or scramble message as output
 - Decryption algorithm - Algorithm run in reverse

2. Describe TWO (2) basic functions used in encryption algorithms.
 Permutation/ Transposition & Substitution

3. How many keys are required for two people to communicate via a symmetric cipher?
 One secret key/ shared key or single key.

4. Substitution and transposition are two types of operation in the cryptography process.
 Describe these two operations and provide ONE (1) example for each operation with a diagram which is from the state of plain text to cipher text.

Types of operations	Diagram
<u>Substitution</u> An operation in which the letters of plain text are being substituted by other letters, numbers or symbols.	 <p>• Substitution</p> <p>Plain text: Hello Alice, I Love You! Regards, Bob</p> <p>Cipher text: 56455 4565, 4 1478 45677 89742214 365</p>
<u>Transposition</u> An operation that rearranges the letters in the plain text.	 <p>• Transposition</p> <p>Plain text: Hello Alice, I Love You! Regards, Bob</p> <p>Cipher text: Ohlle iceal, ul! Lloo vey sargerd, oBb</p>

5.

Decrypt the following message using Caesar cipher: Key = 3

FRPSXWHU VHFXULWB LV IXQ

Original arrangement:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Cipher key = 3,

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Cipher text to be decrypted:
FRPSXWHU VHFXULWB LV IXQ

Plain text: COMPUTER SECURITY IS FUN

6.

Decrypt the following message using Caesar cipher: Identify the Key = ??

BPQA QA MDMV UWZM NCV

Method 1: Try all possible arrangement (n=26) to find out the key

<p>Key 1: BCDEFGHIJKLMNOPQRSTUVWXYZA ABCDEFGHIJKLMNOPQRSTUVWXYZ AOPZ PZ LCLU TVYL MBU (NO MEANING)</p> <p>Key 2: CDEFGHIJKLMNOPQRSTUVWXYZAB ABCDEFGHIJKLMNOPQRSTUVWXYZ ZNOY OY KBKT SUXK LAT (NO MEANING)</p> <p>Key 3: DEFGHIJKLMNOPQRSTUVWXYZABC ABCDEFGHIJKLMNOPQRSTUVWXYZ</p>	<p>Key 5: FGHIJKLMNOPQRSTUVWXYZABCDE ABCDEFGHIJKLMNOPQRSTUVWXYZ WKLV LV HYHQ PRUH IXQ (NO MEANING)</p> <p>Key 6: GHIJKLMNOPQRSTUVWXYZABCDEF ABCDEFGHIJKLMNOPQRSTUVWXYZ VJKU KU GXGP OQTG HWP (NO MEANING)</p> <p>Key 7: HJKLMNOPQRSTUVWXYZABCDEFG ABCDEFGHIJKLMNOPQRSTUVWXYZ</p>
--	---

<p>YMNX NX JAJ S RTWJ KZS (NO MEANING)</p> <p>Key 4: EFGHJKLMNOPQRSTUVWXYZABCD ABCDEFGHIJKLMNOPQRSTUVWXYZ XLMW MW IZIR QSVI JYR (NO MEANING)</p>	<p>UIJT JT FWFO NPSF GVO (NO MEANING)</p> <p>Key 8: JKLMNOPQRSTUVWXYZABCDEFGH ABCDEFGHIJKLMNOPQRSTUVWXYZ THIS IS EVEN MORE FUN Conclusion: This sentence has meaning thus the key is 8.</p>
--	--

Method 2:

1 2 3 4 5 6 7 8

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

K L M N O P Q R S T U V W X Y Z A B C D E F G H I J

key = 8

1. Choose the shortest cipher text from the message given
2. For example, QA, find the Q and put A at below
3. Continue the order of alphabet
4. After write out all the order of alphabet, check which sentence is make sense
5. In this case, IS looks make sense
6. Count how many step "I" arrive at "Q" (ans = 8)
7. Done

7. Differentiate a block cipher and a stream cipher.

Block cipher	Stream cipher
A block cipher is one in which a block of plain text is treated as a whole and used to produce a ciphertext block of equal length.	A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

8. Complete the table below according to the types of cryptanalytic attacks:

Type of Attack	Plaintext	Ciphertext	Algorithm	Key	Comments
Ciphertext-only	N	Y	Y	N	<ul style="list-style-type: none"> One block of ciphertext Most difficult
Known plaintext	Y	Y	Y	N	<ul style="list-style-type: none"> One or more pair of plaintext-ciphertext Use brute force to find the link between key
Chosen plaintext	Y	Y	Y	N	<ul style="list-style-type: none"> Run chosen plaintext to see the result of ciphertext
Chosen ciphertext	Y	Y	Y	N	<ul style="list-style-type: none"> Similar to chosen plaintext Run chosen ciphertext to find key Attacker can modify ciphertext prior to put to algorithm

9. List down the strengths and drawbacks of 3DES.

Strengths:

- Longer key length, 168-bit key length overcomes the vulnerability to brute-force attack of DES (secure)
- Very resistant to cryptanalysis

Drawbacks:

- The algorithm is relatively sluggish in software.
- 3DES, which has three times as many rounds as DES, is correspondingly slower.
- Both DES and 3DES use a 64-bit block size which is not large enough for efficiency and security

10. Explain how AES overcome the drawbacks of 3DES

- Is symmetric block cipher
- Uses a block length of 128 bits
- A key length that can be 128, 192 or 256 bits
- Does not use a Feistel structure but processes the entire data block in parallel during each round using substitution and permutations

11. Differentiate between link and end-to-end encryption

Link encryption	End-to-end encryption
Each vulnerable communications link is equipped on both ends with an encryption device	The encryption process is carried out at the two end systems. The source host or terminal encrypts the data; the data is encrypted form is then transmitted unaltered across the network to the destination terminal or host.

12. List ways in which secret keys can be distributed to two communicating parties.

- A can select a key and physically deliver to B.
- A third party can select the key and physically deliver it to A and B.
- If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
- If A and B each have an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

13. Differentiate between a session key and a master key.

- A session key is a temporary encryption key used between two principals.
- A master key is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys.

14. Describe a key distribution center.

- A key distribution center is a system that is authorized to transmit temporary session keys to principals.
- Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal.

Past year question

15. "Assume that a cryptanalysis successfully cracked the Data Encryption Standard (DES) algorithm, therefore, the possibility of the cryptanalysis cracking the Triple Data Encryption Standard (3DES) cannot be ruled out."

a. Is the above statement valid? Justify your answer.

Yes, both DES and AES have similar Feistel cipher structure, therefore once the cryptanalysis is able to break Feistel Cipher Structure, therefore 3DES has the potential to be cracked.

- b. Define ONE (1) characteristic of Advanced Encryption Standard (AES).
 AES is not a Feistel structure which processes the entire data block in parallel during each round using substitution and transportation.

16. Compare and contrast cryptanalysis and brute force. Propose ONE (1) countermeasure to prevent the success of these attacks.

Cryptanalysis	Brute force
<p>Cryptanalysis attack relies on the nature of the algorithm with some knowledge on the general characteristics of the plain text or plaintext-ciphertext pair. It attempts to deduce a specific plaintext or to deduce the key being used.</p> <p>Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.</p>	<p>In brute force attack, the attacker tries every possible shared key on a cipher text until an understandable plain text is obtained. On average, half of all possible key must be tried to achieve success</p>
<p>Frequently change key used</p>	<p>Implement a large key space for the plain text to be encrypted so that it consumes a lot of effort (i.e time and cost) to accomplish the intent of the brute-force attack.</p>

17. Describe the purpose of substitution and permutation in Feistel cipher

- **Substitution** : Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
- **Permutation** : A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

Tutorial 4: Elementary Cryptography (Asymmetric)

1. Describe the principal ingredients of a public-key cryptosystem.
 - **Plaintext** - Readable message or data that is fed into the algorithms as input.
 - **Encryption algorithms** - Performs transformations on the plaintext.
 - **Public and private keys** - pair of keys, one for encryption, one for decryption.
 - **Decryption algorithms** - Accepts cipher text and the matching key to produce the original plain text.
 - **Cipher text** - Scrambled message produced as output.
2. Briefly define three uses of a public-key cryptosystem
 - **Encryption/decryption** - The sender encrypts a message with the recipient's public key.
 - **Digital signature** - The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
 - **Key exchange** - Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.
3. Differentiate private key with secret key
 - The key used in conventional/symmetric encryption is typically referred to as a secret key.
 - The two keys used for public-key encryption are referred to as the public key and the private key.
4. Compare DES with RSA.
 - RSA in software can be 100 times slower than DES, and in hardware it can be even slower
 - RSA can be used to perform both regular encryption and digital signatures.
 - DES can only be used for encryption
 - RSA and the other public key systems are used in conjunction with symmetric key cryptography. Public key, the slower protocol, is used to exchange the symmetric key (or shared secret), and then the communication uses the faster symmetric key protocol. This process is electronic key exchange.

5. Describe four approaches to attacking the RSA algorithm.
- Brute-force
 - Mathematical attacks
 - Timing attacks
 - Chosen ciphertext attacks
6. How can public-key encryption be used to distribute a secret key?
- Several different approaches are possible, involving the private key(s) of one or both parties.
 - One approach is Diffie-Hellman key exchange
 - Another approach is for the sender to encrypt a secret key with the recipient's public key.

Past year Questions

7. Public key and private key are used in public key cryptography. One of the processes is that a user can encrypt a message using a public key and the receiver can decrypt it using a private key and vice-versa.
- (i) Provide ONE (1) reason for each of these two processes that allow the keys to be used alternately by the users and provide ONE (1) example of application or usage for each process.

Encrypt by public key/ Decrypt by private key

Reason: This process is intended for the receiver to decrypt the message privately and not to others who do not have the owner's private key.

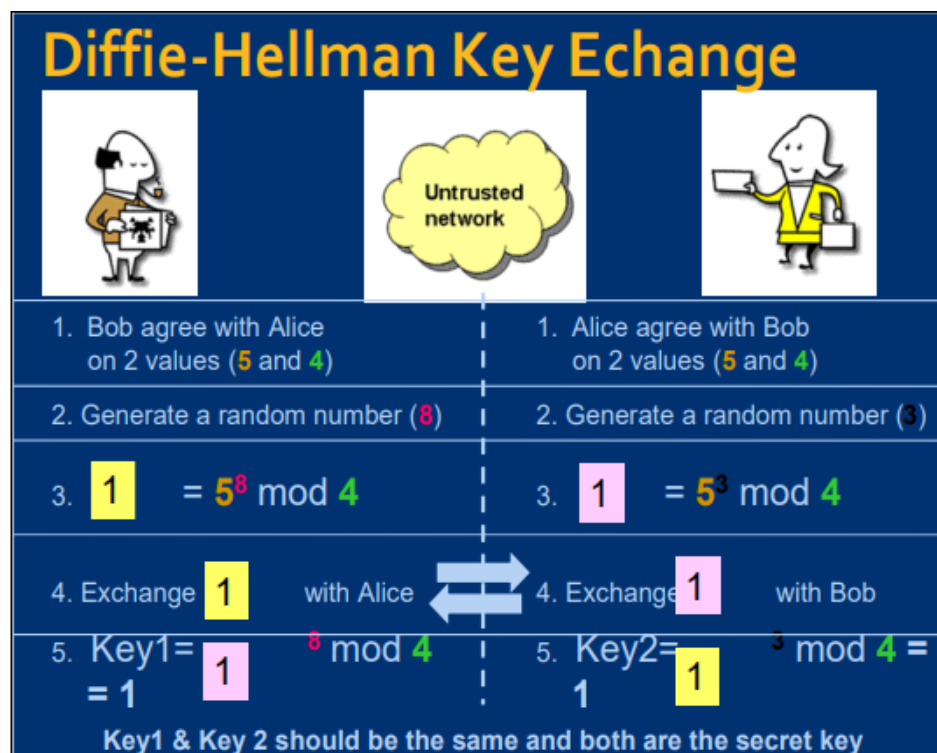
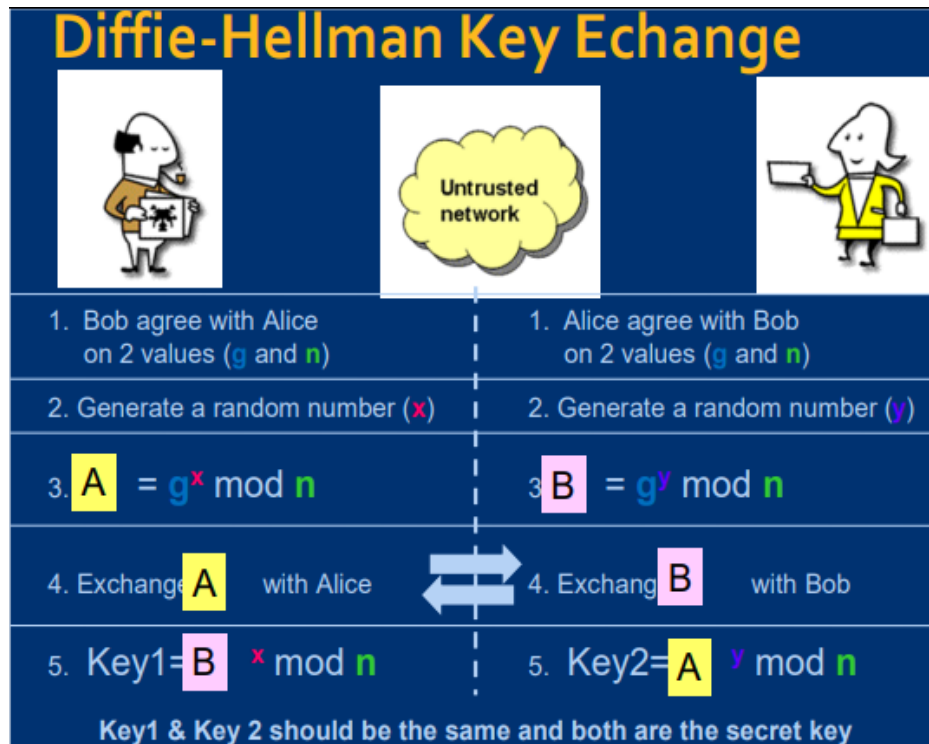
Example: Any confidential message / contract

Encrypt by private key/ Decrypt by public key

Reason: This process is intended to prove the authenticity of the sender by using the sender private key. Receiver can reassure the received message is genuine or fake

Example: Digital Signature / Proof of nonrepudiation

(ii) Explain the FIVE (5) steps on how Bob and Alice exchange their keys securely and compute discrete algorithms in **Diffie-Hellman** key Exchange.



8. Bob wishes to send a message to Alice and to prove the message is really sent from Bob, he wishes to use a digital signature. Illustrate the steps Bob needs to do to create the digital signature.
- Bob uses a secure hash function such as SHA-512 to generate a hash value for the message and then encrypts the hash code with his private key, creating a digital signature. Bob sends the message with the signature attached.
9. Explain why digital signature is unable to provide confidentiality of a message.
- Digital signatures are created by encrypting hash code with a private key, so anyone can get its corresponding public key to decrypt the hash code.
 - Hashing a message does not provide full encryption to a message. Even though the whole message is encrypted with a private key instead of encrypting the hash code, anyone can still get its corresponding public key to decrypt the message.
10. Discuss TWO (2) functions that only asymmetric encryption can achieve but not symmetric encryption
- **Key distribution** - how to have secure communication in general without having to trust a KDC with your key
 - **Digital signatures** - how to verify a message comes intact from the claimed sender
11. Although asymmetric encryption has more functions, why is symmetric encryption still the most preferred solution?
- Asymmetric algorithms are relatively slow because they are based on difficult computational algorithms.
 - That is why symmetric algorithms is still preferred as the more efficient encryption as they are faster (based on simple math algorithms)

12. Figure 1 shows a process of encryption that Bob used to send a confidential message to Alice. The encryption process is using Public-key cryptography.

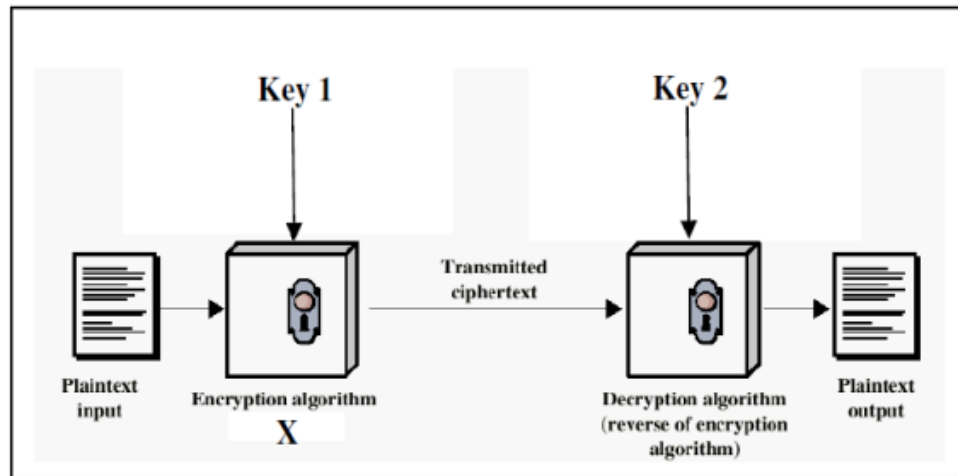


Figure 1: Encryption using Public-key cryptography

By referring to Figure 1, answer the following questions

- (i) State who is the owner for Key 1 and the owner for Key 2.
 - (ii) What type of key that is used in Key 1 and Key 2?
 - (iii) By referring to X, state **ONE (1)** suitable example of encryption algorithm that can be used in the encryption of public-key cryptography.
 - (iv) Briefly describe **FIVE (5)** examples that use public-key cryptography in the Internet environment.
- (i) The owner for key 1 and key 2 is Alice which is the recipient in this process.
 - (ii) Key 1: Alice's public key ; Key 2: Alice's private key
 - (iii) RSA
 - (iv)
 - Digital cheque
 - Contact document
 - Credit card payment
 - Confidential email/document
 - Digital signature

Tutorial 5

1. Describe FOUR (4) means of authenticating a user's identity.
 - Something the individual **knows**
 - Something the individual **possesses**
 - Something the individual **is** (static biometrics)
 - Something the individual **does** (dynamic biometrics)
2. Explain the principal threats to secrecy of passwords.
 - Offline dictionary attack
 - Specific account attack
 - Popular password attack
 - Password guessing against single user
 - Workstation hijacking
 - Exploiting user mistakes
 - Exploiting multiple password use
 - Electronic monitoring
3. Describe two techniques used to protect a password file.
 - Restrict access to the password file using standard access control measures
 - Force users to select passwords that are difficult to guess
4. Explain FOUR (4) techniques for selecting or assigning passwords.
 - User education
 - Computer generated passwords
 - Reactive password checking
 - Proactive password checking
5. Differentiate a simple memory card and a smart card.
 - Memory cards can store but not process data
 - Smart cards have a microprocessor
6. Describe the principal physical characteristics used for biometric identifications.
 - **Facial characteristics:** Most common means of human-to-human identification
 - **Fingerprints:** A means of identification for centuries and the process has been systematized and automated particularly for law enforcement purposes.
 - **Hand geometry:** Hand geometry systems identify features of the hand, including shape, and lengths and widths of fingers

- **Retinal pattern:** The pattern formed by veins beneath the retinal surface is unique
- **Iris:** Another unique physical characteristic is the detailed structure of the iris

7. Describe the operation of a biometric system

- **Enrollment** is analogous to assigning a password to a user. For a biometric system, the user presents a name and, typically, some type of password or PIN to the system.
- **Verification** is analogous to a user logging on to a system by using a memory card or smart card coupled with a password or PIN.
- For an **identification** system, the individual uses the biometric sensor but presents no additional information.

8. List and define the three classes of subject in an access control system

- **Owner:** This may be the creator of a resource, such as a file
- **Group:** In addition to the privileges assigned to an owner, a named group of users may also be granted access rights, such that membership in the group is sufficient to exercise these access rights
- **World:** The least amount of access is granted to users who are able to access the system but are not included in the categories owner and group for this resource.

9. In the context of access control, what is the difference between a subject and an object?

- A subject is an entity capable of accessing objects. Generally, the concept of subject equates with that of process. Any user or application actually gains access to an object by means of a process that represents that user or application.
- An object is anything to which access is controlled. Examples include files, portions of files, programs, and segments of memory.

10. Describe access matrix.

- An access right describes the way in which a subject may access an object

11. Differentiate access control list and a capability ticket.

- For each object, an access control list lists users and their permitted access rights
- A capability ticket specifies authorized objects and operations for a user

Past Year

12. Compare and contrast discretionary access control (DAC) with mandatory access control (MAC)

Discretionary access control (DAC)	Mandatory access control (MAC)
In DAC, the file access is controlled by the owner of the file (i.e the user).	In MAC, the file access is controlled by a central authority such as the security officer.
Flexible because there are no rules and regulations in DAC	Inflexible because MAC contains a lot of strict rules and regulations
Easier to implement	Difficult to implement

Sample answer:

- Discretionary access control (DAC) controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.
- MAC controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources)

13. Identify TWO (2) advantages of Role-Based Access Control (RBAC) over Discretionary Access Control (DAC).

Ease of management / Security management is simplified - In RBAC, we can just grant each of the users the correct role and automatically they are able to access the resources based on the access capabilities. While for DAC, where for each new user, we have to go through all the resources and add them as a new user into the list.

Easy to enforce enterprise-specific security policies - RBAC allows us to implement standardized enforcement policies which demonstrate the control required for compliance. It provides appropriate access capabilities to the user based on the role assigned to access the resource.

14. Exploiting user mistakes is one of the popular methods to attack password-based authentication.

- a. Illustrate a scenario on how this attack can take place in an organization
If the user is currently using a computer generated password to create a password for him/her to access the system, then the user is more likely to write it

down on a paper as the password is difficult to remember. The user might write the password on a paper and share it with his/her colleagues to ease file sharing between them. After completing the file sharing, the colleague might throw the paper with the password written to the rubbish bin. At this point, the attacker can exploit the user's mistake in which they are able to get the password written in the paper and use it to compromise the organization network to access the organization and perform malicious actions such as stealing the sensitive data.

- b. Suggest ONE (1) countermeasure against this attack
 - **User training** - Educate the staff to implement good safety and security habits such as never writing the password on a paper or any electronic device and change the password regularly (2 months).
 - Intrusion detection system
 - Simpler passwords combined with another authentication mechanism
- c. Describe TWO (2) examples of bad passwords
 - A password which use own, wife, husband, child, colleague name
 - A password which use the dictionary or encyclopedia word

15.

- a. Explain the general concept of a challenge-response protocol.
 - A user attempts to logon to a server
 - The server issues some sort of challenge that the user must respond to in order to be authenticated.
- b. Illustrate the steps of the challenge-response protocol for a **token protocol** for authentication.
 - User transmits identity to the remote host
 - Host returns a random number and identifiers
 - Token either stores a static passcode or generates a one-time random passcode
 - User activates passcode by entering a password
 - Password is shared between user and token and does not involve remote host

16. Figure 1 shows the relationship among Role Based Access Control (RBAC) models.

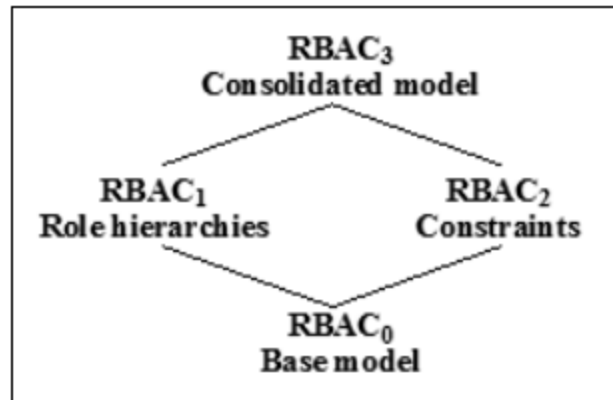


Figure 1: The relationship among RBAC models

- a. Describe FOUR (4) types of entities in an RBAC0 system.
- **User** : An individual that has access to this computer system. Each individual has an associated user ID.
 - **Role** : A named job function within the organization that controls this computer system. Typically, associated with each role is a description of the authority and responsibility conferred on this role, and on any user who assumes this role.
 - **Permission** : An approval of a particular mode of access to one or more objects. Equivalent terms are access right, privilege, and authorization.
 - **Session** : : A mapping between a user and an activated subset of the set of roles to which the user is assigned.
- b. Discuss the function of role hierarchies in RBAC1 system
- Role hierarchies provide a means of reflecting the hierarchical structure of roles in an organization. Typically, job functions with greater responsibility have greater authority to access resources. A subordinate job function may have a subset of the access rights of the superior job function. Role hierarchies make use of the concept of inheritance to enable one role to implicitly include access rights associated with a subordinate role

1. Describe THREE (3) elements of Information System Security.
 - **Logical security** - Protects computer-based data from software-based and communication-based threats.
 - **Physical security** - Protects the information systems that contain data and the people who use, operate, and maintain the systems.
 - **Premises security** - Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations.
2. Explain human-caused physical threats.
 - **Unauthorized physical access** - Those without the proper authorization should not be the allowed access to certain portions of a building or complex unless accompanied with an authorized individual.
 - **Theft** - This threat includes theft of equipment and theft of data by copying.
 - **Vandalism** - This threat includes destruction of equipment and data.
 - **Misuse** - This category includes improper use of resources by those who are authorized to use them, as well as use of resources by individuals not authorized to use the resources at all.
3. Describe the principal concerns with respect to inappropriate temperature and humidity.
 - Room temperature too hot or too cold for equipment.
 - Internal equipment is too hot.
 - Humidity too high or too low.
4. Explain the direct and indirect threats posed by fire.
 - The direct threat is the damage caused by the fire itself.
 - The indirect threats are from heat, release of toxic fumes, water damage from fire suppression, and smoke damage.
5. Describe the threats posed by loss of electrical power
3 groups of power utility problems: **Undervoltage, overvoltage, noise.**
 - **Undervoltage** events range from temporary dips in the voltage supply to brownouts, to power outages. There is no damage occurring but it performs inefficiently as service is interrupted.
 - A surge of **overvoltage** caused by a supply anomaly, some internal wiring fault or lightning can destroy electrical components.
 - **Noise** can interfere with signals inside electronic devices, causing logical errors.
6. Describe some measures for dealing with water damage.

- With knowledge of the exact layout of water supply lines, measures can be taken to locate equipment sensibly.
 - The location of all shutoff valves should be clearly visible or at least clearly documented, and responsible personnel should know the procedures to follow in case of emergency.
 - To deal with both plumbing leaks and other sources of water, sensors are vital.
 - Water sensors should be located on the floor of computer rooms, as well as under raised floors, and should cut off power automatically in the event of a flood.
7. Describe some measures for dealing with power loss.
- To deal with brief power interruptions, an uninterruptible power supply (UPS) should be employed for each piece of critical equipment.
 - UPS units can also function as surge protectors, power noise filters, and automatic shutdown devices when the battery runs low.
 - For longer blackouts or brownouts, critical equipment should be connected to an emergency power source, such as a generator.

Past Year questions

8. "Human-caused threats are more difficult to deal with than the environmental and technical threats." Do you agree with the statement? Justify your answer.
- Yes, I agree.
 - Human-caused threats are less predictable than other types of physical threats.
 - Worse, human-caused threats are specifically designed to overcome prevention measures and/or seek the most vulnerable point of attack.
9. Unauthorized physical access can lead to other threats, such as theft, vandalism, or misuse. Briefly explain these three threats
- **Unauthorized physical access** - Those without the proper authorization should not be the allowed access to certain portions of a building or complex unless accompanied with an authorized individual.
 - **Theft** - This threat includes theft of equipment and theft of data by copying.
 - **Vandalism** - This threat includes destruction of equipment and data.
 - **Misuse** - This category includes improper use of resources by those who are authorized to use them, as well as use of resources by individuals not authorized to use the resources at all.

PYQ Question (to be discussed):

10. Physical Access Control Systems (PACS) are deployed in most US government buildings.

Source: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-116.pdf>

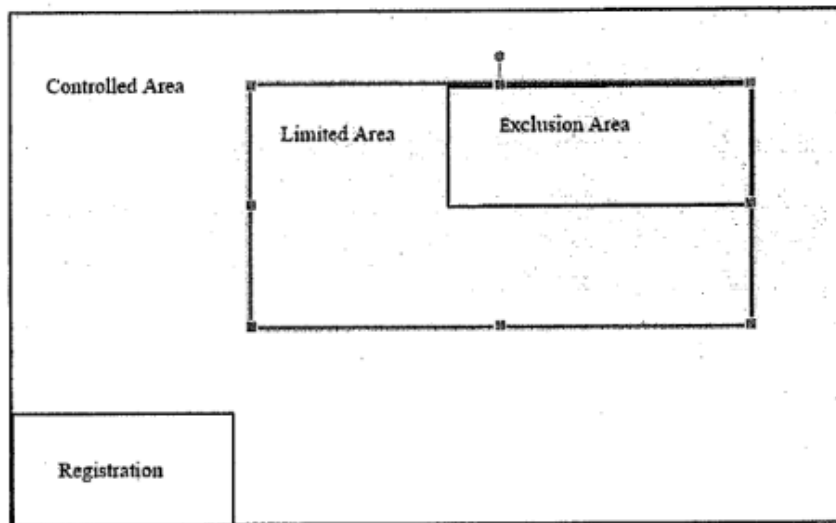


Figure 1: Access Control Model Example Use

- i. Based on the model specified by SP 800-116 and Figure 1, provide THREE (3) appropriate security measures to identify a person's identity when accessing the Controlled Area after the Registration Area.

Visual (VIS)

Cardholder Unique Identifier (CHUID)

Card Authentication Key (CAK)

- ii. Provide TWO (2) security measures to enter the Limited Area from the Controlled Area.

Biometric (BIO)

PIV Authentication key (PKI)

- iii. Provide ONE (1) security measure to allow access to the Exclusion Area

Adding third authentication factor which different from those used at access point A and B such as attended biometric (BIO-A)

1. Suggest rules to help protect passwords from pilfering.

Rules to help protect passwords from pilfering:

1. Use a long password with the combination of letters, capital letters, digits, symbols and do not use dictionary words, common names and dates.
 2. Do not reveal your password to anyone you don't know.
 3. Change passwords periodically and do not reuse old passwords.
 4. Do not use the same password for different accounts.
 5. Do not use remote login software that does not encrypt user passwords and other important personal information.
 6. Shred all discarded papers using a good paper shredder.
 7. Avoid entering any information in any popup window and avoid clicking on any unknown link in the suspicious email.
2. Discuss THREE (3) threats that exist in a distributed network.
 - User impersonation
 - Network address impersonation
 - Eavesdropping, replay attack, DOS
 3. Describe identity spoofing
 - Attacker uses a fake source address that does not represent the actual address of the packet.
 - Spoofing may be used to hide the original source of an attack
 - Identify spoofing attacks allow attackers to impersonate a victim without using the victim's passwords.
 4. What is a man-in-the-middle attack? How to defend against this attack?
 - Compromise a network device between two or more users.
 - Using this device to intercept, modify, or fabricate data transmitted between users.
 - Defense measures - Encrypting and authenticating IP packets
 5. Discuss message replay attack and its defense mechanisms.
 - First intercepts a legitimate message, keeps it intact, and then retransmits it at a later time to the original receiver

Defense Mechanisms

- Attach a random number (nonce) to the message
- Attach a timestamp to the message
- The best method is to use a nonce and a timestamp together

6. Illustrate the general steps of buffer-overflow attack.
 - a. Find a program that is prone to buffer overflows (e.g. Programs using functions that do not check bounds are good candidates)
 - b. Figure out the address of the attacker's node
 - c. Determine the number of bytes long enough to overwrite the return address
 - d. Overflow the buffer that rewrites the original return address of the function call with the address of the attacker's code

Past Year Question

7. Illustrate **TCP hijacking** that could happen between an attacker X and an employee Y who is going to remote logon to server S
 - a. Y send a SYN packet to S for remote login
 - b. Attacker X hijacks the packet and uses SYN flooding to mute server S so that the server cannot complete the 3-way handshake
 - c. Attackers predict the correct TCP sequence number for ACK supposed to be sent from server S to Y. Then the attacker X crafts the ACK packet with the sequence number and server's IP address then sends it to Y.
 - d. Y verify the ACK packet and send back an ACK packet to the attacker to complete the 3-way handshake with the attacker X
 - e. TCP connection between user Y and server S is now hijacked by the attacker X. (TCP connection is now established between Y and X, instead of between Y and S)
8. A distributed denial-of-service (DDoS) attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system to cause it out-of-service. Suggest THREE (3) **countermeasures for DDoS**
 - Apply the latest service packs.
 - Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and empty dynamic backlog mechanisms to ensure that the connection is never exhausted.
 - Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks
 - Backup system
 - Monitoring system
 - System log
 - Close all unnecessary ports to deny IP scans

- Automatically disconnect when not in use
 - Detect and remove zombie ware
9. Illustrate how an attacker uses **SYN flooding technique** in causing a target computer unable to establish connections with other computers.
- a. Attacker sends to the target computer a large number of crafted SYN packets
 - b. The victim's computer is obliged to send an ACK packet to the crafted source IP address contained in the SYN packet
 - c. Because the crafted source IP address is unreachable, the victim's computer will never receive the ACK packet it is waiting for, making the crafted SYN packet remain in the TCP buffer
 - d. The TCP buffer is completely occupied by the crafted SYN packets

1. Explain IT security management.

IT security management is a process used to achieve and maintain the appropriate level of confidentiality, integrity, availability, accountability, authenticity and reliability.

2. List THREE (3) fundamental questions IT security management tries to address.

- a. What assets need to be protected?
- b. How are those assets threatened?
- c. What can be done to counter those threats?

3. Explain FOUR (4) steps in the iterative security management process

- Plan establish security policy, objectives, processes and procedures
- Do implement the risk treatment plan
- Check monitor and maintain the risk treatment plan
- Act maintain and improve the information security risk management process in response to incidents, review, or identified changes

4. Illustrate FOUR (4) approaches to identifying and mitigating IT risks.

- **Baseline approach** - goal is to implement agreed controls to provide protection against the most common threats. It forms a good base for further security measures. It is easy, cheap and can be replicated. Baseline approach also gives no special consideration to variations in risk exposure and it may give too much and too little security. Recommended for small organisations without the resources to implement more structured approaches
- **Informal approach** - It involves conducting an informal, pragmatic risk analysis on organization's IT systems. The judgments can be made about vulnerabilities and risks that the baseline approach would not address. It Exploits knowledge and expertise of analysts Some risks may be incorrectly assessed but it is fairly quick and cheap. Informal approach Skewed by analyst's views, varies over time and it is suitable for small to medium sized organizations where IT systems are not necessarily essential.
- **Detailed risk analysis**- It is the most comprehensive approach, it assesses using formal structured processes such as number of stages, identify threats and vulnerabilities to assets and identify likelihood of risk occurring and consequence. Detailed approach is a significant cost in time, resources and expertise. It may be a requirement to use. Recommended for large organizations with IT systems critical to their business objectives.

- **Combined approach** - Combines elements of the baseline, informal, and detailed risk analysis approaches. It provides reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time. It also starts with the implementation of suitable baseline security recommendations on all systems. systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment. A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements. Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted. Over time, this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems

5. Describe the FIVE (5) alternatives for treating identified risks.

- Risk acceptance
- Risk avoidance
- Risk transfer
- Reduce likelihood
- Reduce consequences

Past year question

6. Security risk assessment is an important process of identifying and mitigating risks.

(i) Compare and contrast Baseline Approach with Detailed Risk Analysis in security risk management

- Baseline approach uses industrial best practices whereas Detailed risk analysis implements more structured approaches.
- Detail risk analysis provides the more accurate evaluation of an organization's IT system's security risks compared to Baseline approach.
- Higher cost for Detail risk analysis compared to baseline approach.

(ii) Assuming that there is a risk identified in the risk assessment which cannot be mitigated using the available controls. Suggest ONE (1) possible risk treatment alternative for this risk.

- **Risk transfer.** We can buy the insurance so that we can share the responsibility with the insurance company together whereby if the system was attacked, the insurance company can help to afford 30% to 50% of the cost to recover the system.

- **Risk Acceptance.** We can only accept the risk if they currently don't have available control to mitigate the risk. / We should accept the risk when the cost to implement the control is greater than the loss.

(iii) After the completion of risk assessment, outline the subsequent processes that are required to be carried out according to a PDCA cycle for ensuring the risks identified have been addressed appropriately.

- **PLAN: Develop IT Security Plan.**
- **DO: Implementing IT Security Plan.**
- **CHECK: Maintaining and monitoring of implemented controls.**
- **ACT: Take corrective and preventive actions for continual improvement.**

7. Explain how a combined approach in identifying and mitigating risks utilizes the baseline, informal, and detailed risk analysis approaches. Why do you think the combined approach is highly recommended?

The combined approach combines elements of other approaches:

- Implementation of a suitable initial baseline on all systems.
- Conduct an immediate informal analysis to identify critical risks.
- An ordered process of formal assessment of detailed analysis on these systems.

Highly recommended because:

- Results in the development of a strategic picture of the IT resources and where major risks are likely to occur.
- Ensures that a basic level of security protection is implemented early.
- For most organizations, this approach is the most cost-effective.

8. For treating identified risks, an organization can choose to reduce consequences or reduce likelihood of the risks. Discuss the differences between reducing consequence and reducing likelihood of risk with appropriate example each

- **Reduce consequence:** By modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur. This could be

achieved by implementing controls to enable the organization to quickly recover should the risk occur.

- Examples include implementing an off-site backup process, developing a disaster recovery plan, or arranging for data and processing to be replicated over multiple sites.
- Reduce likelihood: By implementing suitable controls to lower the chance of the vulnerability being exploited.
- These could include technical or administrative controls such as deploying firewalls and access tokens, or procedures such as password complexity and change policies. Such controls aim to improve the security of the asset, making it harder for an attack to succeed by reducing the vulnerability of the asset

Tutorial 9: Security control, plan, procedure

1. Describe security control or safeguard

An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action.

2. Illustrate THREE (3) broad classes of controls and the THREE (3) categories each can include.

- **Management control** - security policies
- **Operational control** - implementation and use of policies
- **Technical control** - correct use of hardware and software
- **Supportive controls**: Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls.
- **Preventative controls**: Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability.
- **Detection and recovery controls**: Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.

3. List THREE (3) ways that implementing a new or enhanced control can reduce the residual level of risk.

- Reduce the vulnerabilities such as flaws or weaknesses in the system
- Add a targeted control

- Reduce the magnitude of the adverse impact of the threat occurring in an organization
4. Describe the items that should be included in an IT security implementation plan
 - Risks (asset/threat/vulnerability combination)
 - Recommended controls (from the risk assessment)
 - Action priority for each risk
 - Selected controls (on the basis of the cost-benefit analysis)
 - Required resources for implementing the selected controls
 - Responsible personnel
 - Target start and end dates for implementation
 - Maintenance requirements and other comments.
 5. What checks does the organizational security officer need to perform as the plan is being implemented
 - The implementation costs and resources used stay within identified bounds
 - The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved
 - The controls are operated and administered as needed

Past Year questions

6. Discuss THREE (3) elements that security policy needs to address.
 - The scope and purpose of the policy
 - The relationship of the security objectives to the organization's legal and regulatory obligations, and its business objectives
 - IT security requirements in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability, particularly with regard to the views of the asset owners
7. Describe the purpose of IT Security Plan and discuss THREE (3) important elements that the plan should include
 - The purpose of the IT security plan is to detail the actions needed to improve the identified deficiencies in the risk profile. An IT security plan should provide details of what will be done, what resources are needed and who is responsible for.
 - Risks, recommend controls, action priority
 - Selected controls, resources needed
 - Responsible personnel, implementation dates
 - Maintenance requirements

8. Describe technical controls and give ONE (1) example of technical control measures

- Technical controls: Involve the correct use of hardware and software security capabilities in systems. These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions.
- Example :
 - Authentication
 - Authorization
 - Access control
 - Audit
 - Intrusion detection

9. Security controls or safeguards are practices, procedures or mechanisms that may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, or detect unwanted incidents and facilitate recovery.

(i) “Management Controls” is one type of security control. Explain about “Management Controls”.

Management control focuses on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization’s mission.

(ii) Provide TWO (2) examples of preventive “Management Controls”.

- User registration
- User agreement
- Non-disclosure agreement (NDA)
- Separation of duties
- Warning banner
- Security awareness training