Computer Security

Lectures Notes

Introduction

The requirements of information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. An example of the former is the use of rugged filing cabinets with a combination lock for storing sensitive documents.

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is computer security.

The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. In fact, the term network security is somewhat misleading, because virtually all business, government, and academic organizations interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet.

There are no clear boundaries between these two forms of security. For example, one of the most publicized types of attack on information systems is the computer virus. A virus may be introduced into a system physically when it arrives on a diskette or optical disk and is subsequently loaded onto a computer. Viruses may also arrive over an internet. In either case, once the virus is resident on a computer system, internal computer security tools are needed to detect and recover from the virus.

The purpose of the course is to provide the principles and practices of cryptography and cybersecurity.

1- Protect yourself, your device.

2- Understanding attackers' mindset.

3- Test the security of a company

4- Find a job: 350,000 cybersecurity jobs are currently unfilled in USA in 2019

According to 2016 Internet Security Threat Report by Symantec. More than four hundred twenty-nine million identities were exposed as a result of errors or direct cyberattacks. More than

four hundred thirty million of new variants of malicious software were discovered. That makes more than one million per day. The number of new vulnerabilities discovered raised to more than fifty-five hundred, which means that more than fifteen are discovered every single day and this does not include those vulnerabilities that someone discovers and does not report. When it comes to web sites, one in approximately three thousand sites were found to contain malware, and around seventy eight percent of all scanned web sites were vulnerable. By the end of the year 2020, it is expected to have fifty billion connected devices many of which will need to interoperate much in the way that already connected systems do, or even more, we have software everywhere:

- software that has become extremely complex.
- software that has not been developed to be secure.
- software that interacts with people who do not and cannot understand all ways in which things could possibly go wrong.
- On top of that, cyberattackers can get value out of their attacks, normally in the form of economic gain. All this, the huge number of interconnected systems, their complexity, our software and the human element creates a substantial attack surface for attackers, who can exploit victims for economic or political gain.
- In the last years attacks have become not only more complex, but also easier to conduct, because of the commercialization of attack components and services.

Economy of Cybercrime

Cybersecurity or Computer security is the protection of computer systems and networks from the theft, disruption, misdirection, or damage to their hardware, software, or electronic data. **Cybercrime**: Offences that are committed against individuals or groups of individuals using modern telecommunication networks such as Internet.

There are marketplaces where tools and data required to conduct cybercrime operations can be bought and sold. Many of these marketplaces are just web-based forums, openly accessible to everyone. So, everything be sold and bought in these market places.

For example, according to some reports from 2015, you can buy one thousand compromised hosts for as little as two hundred dollars. If you are interested in proxy servers, you can get one hundred fifty of them for twenty-five dollars a month. And if what you look for is online social engagement, you might get one thousand followers in Twitter for twenty dollars and one thousand retweets for three hundred and fifty.

Popular cybercrime activities

- Spamvertised products: The word is a combination of the words "spam" and "advertising", in which products are sold online in which potential clients are contacted through spam. Historically, email has been the main venue to contact potential clients, but in recent years spam is also present in other prominent venues, such as online social networks. Fighting spam can be done at several levels, including technical measures, such as blacklisting IPs and email accounts used by spammers and also using spam filters.

- Scareware: This refers to attacks in which the victim is tricked into purchasing a fake security product. Normally, a fake anti-virus that is either not functional at all or contains malware. The fake antivirus attacks were replaced by ransomware around four years ago. Ransomware is a generic term referring to malicious software that prevents victims from accessing their systems, for example, by encrypting the contents of the hard drive. If the victim wants to get back access to the system, he/she must pay a bail (generally a few hundred dollars). Ransomware has proliferated lately, starting with the infamous case of Cryptolocker in late 2013 and 2014, which is believed to have extorted up to four million dollars.

- Click Fraud: Online advertisement is a multi billion dollar industry. To conduct this attack the attacker first registers as a publisher in an advertisement network. Once he gets up posted in his network, he derives fake traffic to them, that is, he gets fake clicks on those adds, which will resort in a revenue from the advertisers. Those fake clicks can come from different sources, including manual workers bought deployed on compromised hosts that are instructed to click on certain adds, and also malware designed to redirect clicks. According to some studies, up to twenty percent of all clicks are fake.

- Attacks against Online Payment and Banking: In this case, attackers are ultimately after payment credentials, most notably credit card details that can be later used to buy goods elsewhere, or even to cost money out of ATMs. The means to obtain such payment credentials include the use of malware installed in point of sales Devices that in some cases can read both the credit card details and the PIN number. In other cases, the attacker directly steals from payment databases, such as in the infamous attacks suffered by the Sony PlayStation Payment Network in 2011, in which the attackers stole data belonging to seventy-seven million of victims. Malware has been also designed on purpose to steal banking credentials such as in the case of Zeus, who read the username and password entered by victims in online banking sites.

Cyberthreats classification

- The term cyberthreat refers to a wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contains. Threats can be classified according to multiple criteria and this is useful for many reasons, particularly when doing a risk assessment to prepare defenses.
- Threats with no or little structure, threats with substantial structure and threats with very high structure.
- Threat is said to be **unstructured** if it refers to individuals or small groups with little or no organization at all an almost negligible funding. The attacks they execute are often easy to detect and are based on freely available tools and documented vulnerabilities. These attacks are generally opportunistic, which means that they exploit wherever vulnerable system is found and do not go after a particular target. Motivations for this class of attackers arrive from simply claiming the authorship of the attack to acquire resources that can later be traded in the underground economy for cybercrime activities.
- Contrarily to the previous one, **structured threats** refers to attackers that are well organized, planned or funded. Attacks carried out by them are often targeted against particular individuals or organizations, and they usually involve an extensive campaign of information gathering to choose the particular elements that will later be used during the attack. Another important feature of these threats is the attack sometimes counts on the help from insiders to get the information.
- The term **highly structured threat** is reserved for those whose organization and funding are remarkable. It is often associated with nation states and other attackers who have long-term strategic goals that go beyond one specific victim or one particular attack campaign. In this case, the attacks often involve multiple infection vectors, both technical and social and also exploit help from insiders. Some particular operations could even be coordinated actions by multiple groups.

.

ATTACKS AND MECHANISMS

To assess the security needs of an organization effectively and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. One approach is to consider three aspects of information security:

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service[1].

Security Attacks

Attacks on the security of a computer system or network are best characterized by viewing the function of the computer system as providing information. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination, such as another file or a user. This normal flow is depicted in figure 1. The remaining parts of the figure show the following four general categories of attack:

- **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on **availability.** Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.
- **Interception:** All unauthorized party gains access to an asset. this is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network, and the illicit copying of files or programs.
- **Modification:** An unauthorized party not only gains access to but tampers with an asset. This is an attack on **integrity.** Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.
- **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on **authenticity.** Examples include the insertion of spurious messages in a network or the addition of records to a file.

Reference : Stallings, W. (2017). *Cryptography and network security: principles and practice* (pp. 92-95). Upper Saddle River: Pearson.

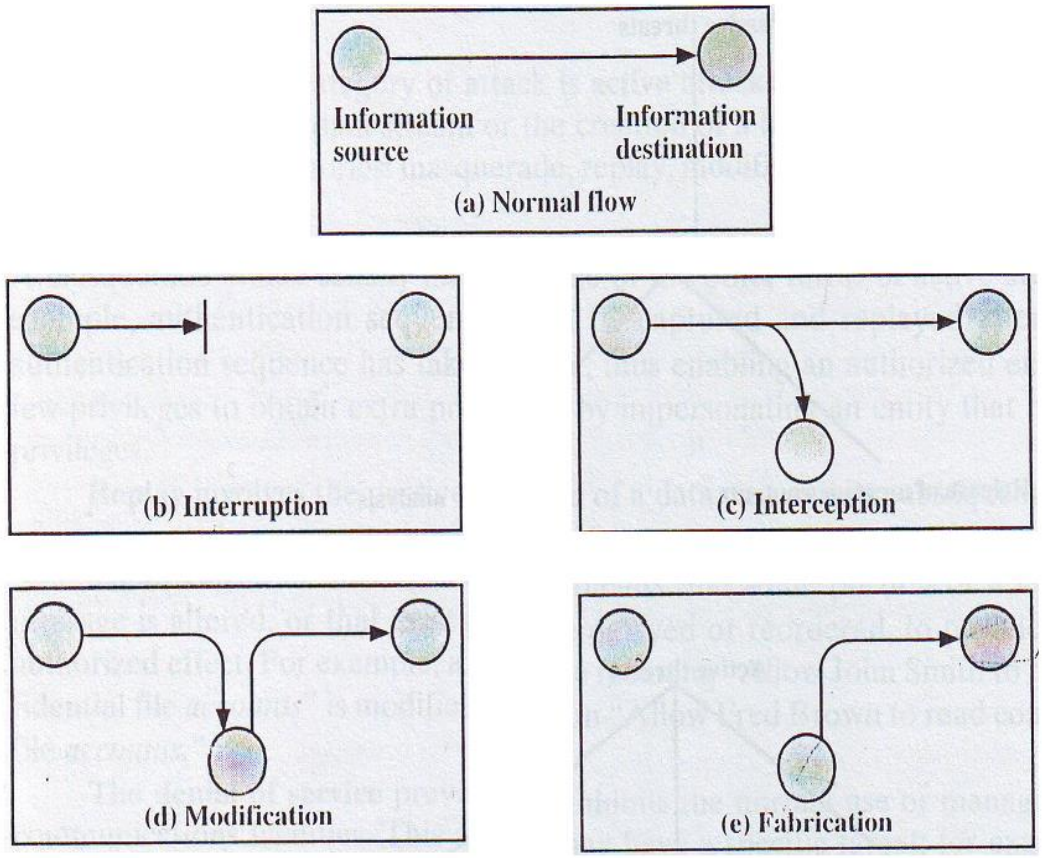


Figure 1:Security Attacks

A useful means of classifying security attacks is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

The release of message contents is easily understood (Figure 2). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

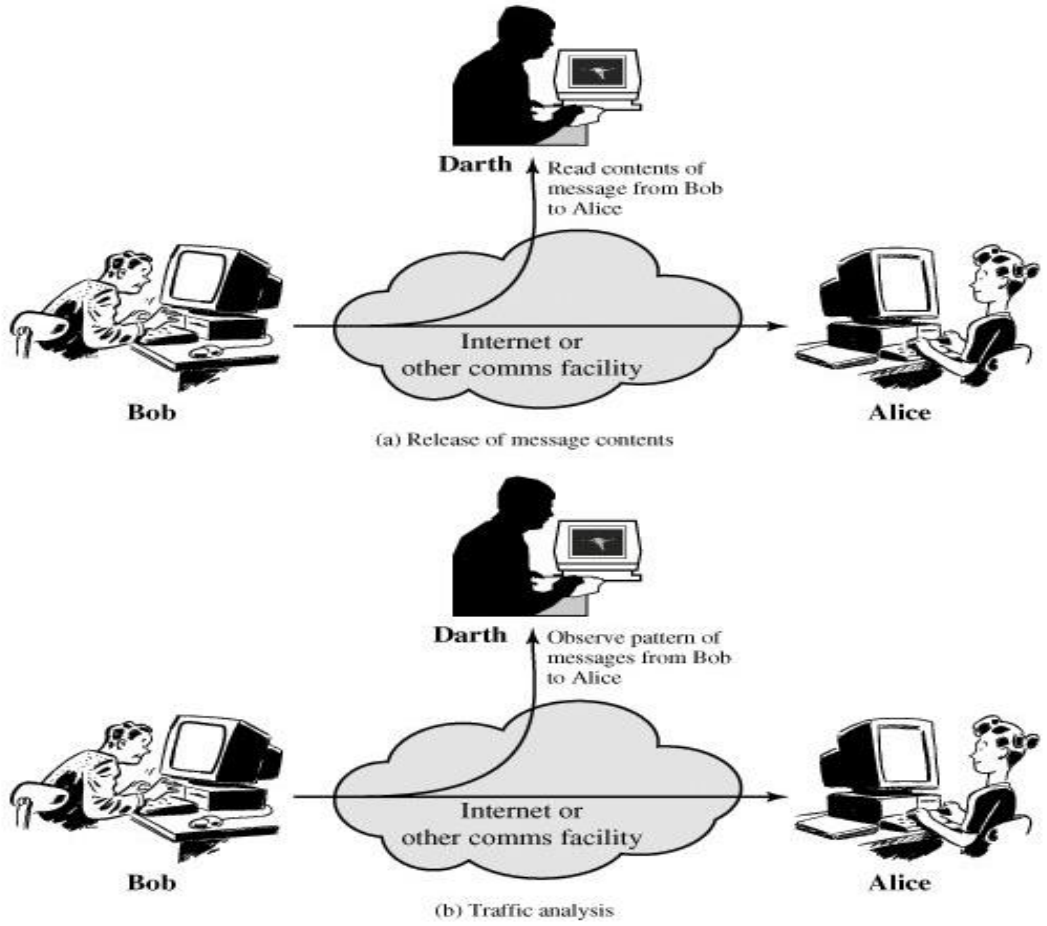


Figure 2:Passive Attacks

Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

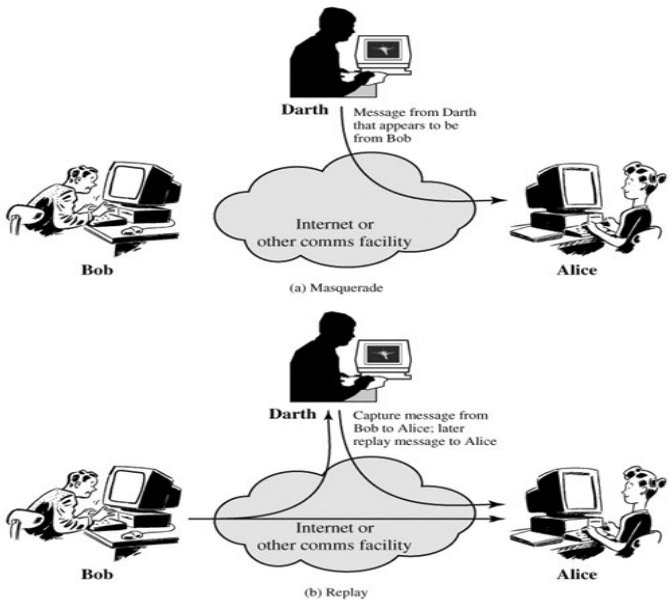
A **masquerade** takes place when one entity pretends to be a different entity (Figure 3.a). A masquerade attack usually includes one of the other forms of active attack.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 3.b).

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 3.c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure 3.d). This attack may have a specific target; for example, the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.



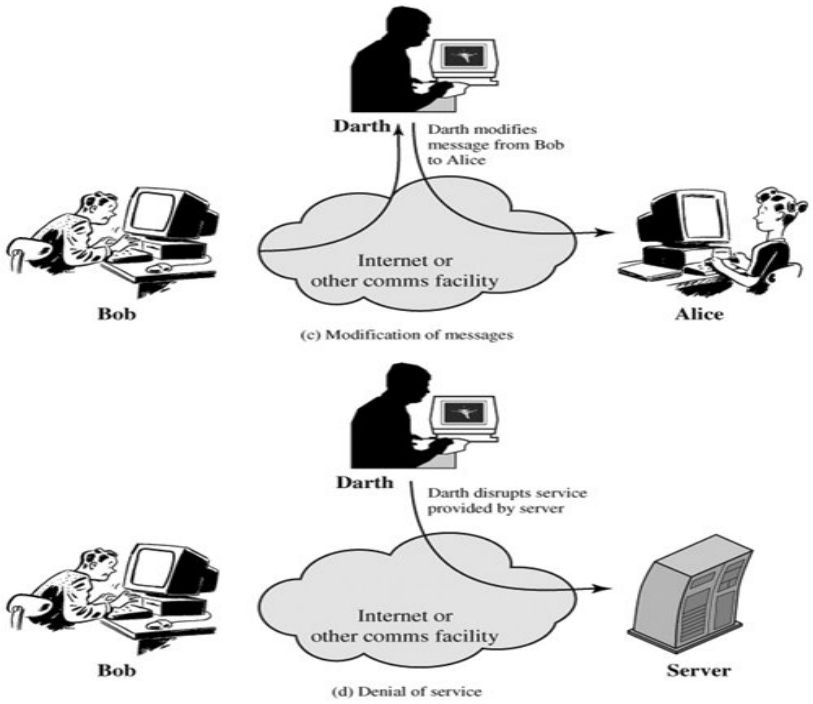


Figure 3:Active Attacks

Cryptography:

Cryptographic systems are characterized along three independent dimensions:

The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Requirements for secure use of conventional encryption:

- A strong encryption algorithm. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
- Sender and receiver must have obtained copies of the secret key in a secure fashion
- The algorithm doesn't need to be secret; only the key should be secret.

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients (Figure 4):

- Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- Ciphertext: This is the message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

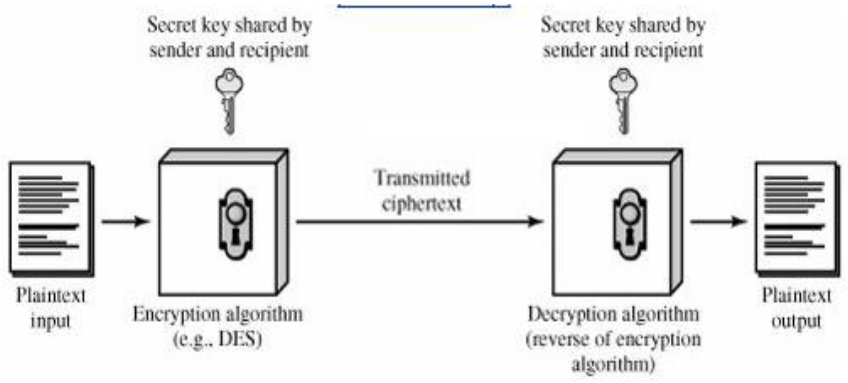


Figure 4. Symmetric Encryption

Caesar Cipher

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

plain: meet me after the party
cipher: PHHW PH DIWHU WKH SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

plain: 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: 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

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	M
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	W	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:

$C = E(3, p) = (p + 3) \bmod 26$

A shift may be of any amount, so that the general Caesar algorithm is

$C = E(k, p) = (p + k) \bmod 26$

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$p = D(k, C) = (C - k) \bmod 26$

If it is known that a given ciphertext is a Caesar cipher, then a **brute-force** attack (in which the attacker tries all possible keys or passwords until the correct one is found) is easily performed, simply try all the 25 possible keys.

Example:

CIPHER Text	GSQTYXIVIRKMRIIVMRK
Try Key=1	FRPSXWHUHQJLQHHULQJ
Try Key=2	EQORWVGTGPIKPGGTKPI
Try Key=3	DPNQVUFSFOHJOFFSJOH
Try Key=4	COMPUTERENGINEERING

Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Playfair Cipher

The best-known multiple-letter encryption cipher is the Playfair, which treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams.

The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. It works as follows:

1- Create a 5×5 grid for all English letter except one. (Usually i or j).

2- Add a keyword with no repeated letters.

3- Read the plain text as couple of letters each time.

The location of each couple of letters can be one of the following three:

- The two letters are located on the same column (Choose the one beneath).
- The two letters are located on the same row (Choose the letter on the right).
- The two letters located in different rows and columns (Choose the letter which is located on the same row of the first letter and on the same column of the second)

Example: Encrypt the word “SAFELY” using the keyword “LIZARD”

Solution:

1- Creating the grid

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

2- Separating the letters SA FE LY
3- a- SA=XE The same column.
   b- FE= DF The same row.
   c- LY=RU=Neither the same row nor the same column

The cipher text for the word SAFELY is XEDFRU by playfair encryption using the keyword LIZARD.

Notes:

For repeated letters. Example: SPEED, it becomes SPEXED.

For odd number of letters: add X to fill the final letter place. CAR → CARX

For Decryption, the letter above and left are used in the first and second case.

The Data Encryption Standard

The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

The Simplified DES (S-DES) is considered a good academic instance for better understanding of the full DES encryption. S-DES is a 10 bits key and 8 bits plaintext.

S-DES key generation:

Step 1:P10

3	5	2	7	4	10	1	9	8	6

Split the result into two 5 bits groups

Step 2:

LS-1 (Circular Left Shift)

For K1:

Step 3: P8 =

6	3	7	4	8	5	10	9

Step 4: Apply LS-2 (Circular Left Shift by 2)

For K2:

Step 5: P8

6	3	7	4	8	5	10	9

S-DES Encryption

Step 1: Initial Permutation

2	6	3	1	4	8	5	7

Step 2: Divide the result to 2 groups of 4 bits each, L and R

Step 3 : f_k (L,R) = (L+ F(R,S_k), R). F(R,S_k) is found using the following steps:

a: E/P On R

4	1	2	3	2	3	4	1

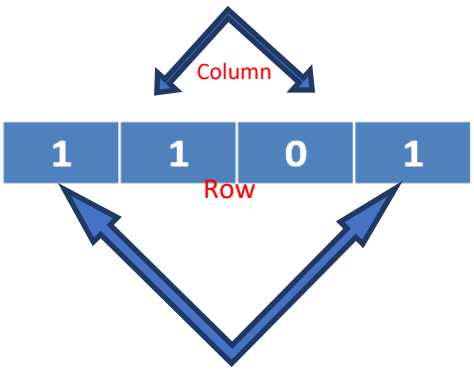
b: XOR with the sub Keys (K1)

c: Sboxes

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

For instance , if the four left bits are 1101, they mapped to R=11_b=3 , C=10_b=2 S0(3,2)=1 = 01_b

d: P4



2	4	3	1

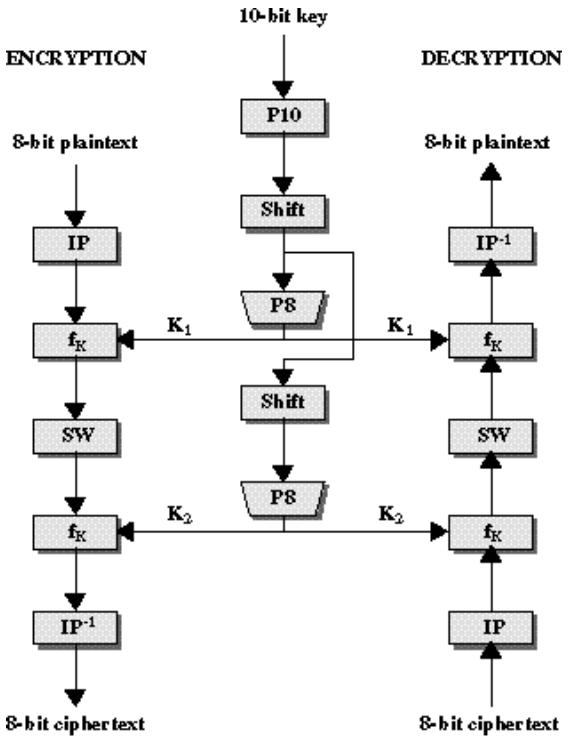
Step 4: Swap L,R in the final result (d)

Step 5: Repeat Step 3 on K2

Step6: Apply IP^{-1}

4	1	3	5	7	2	8	6

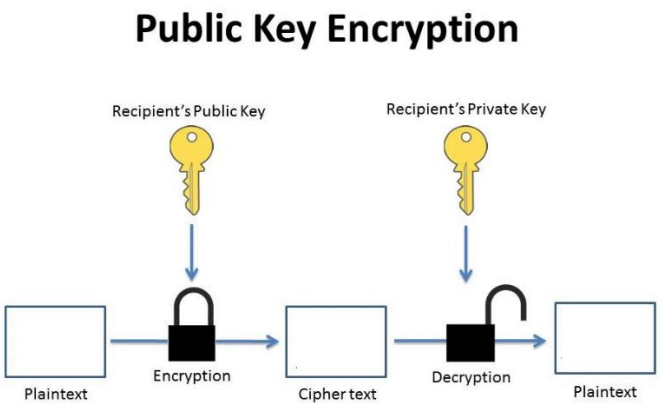
For decryption the same procedure is applied in reverse order, as depicted in Figure (6)



S-DES Encryption/Decryption

Public Key Cryptography

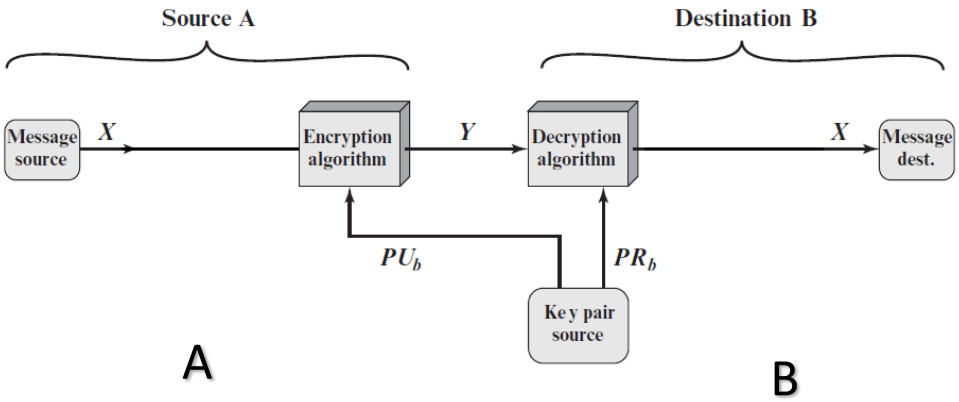
Public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. Public-key algorithms are based on mathematical functions rather than on substitution and permutation.



Public key encryption

Public-Key Cryptography Requirements:

1- It is computationally easy for a party B to generate a key pair (public key PUb, private key PRb)



Private and Public keys in Public-key cryptography

2- It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:

C = E(PUb, M)

3- It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:

M = D(PRb, C) = D[PRb, E(PUb, M)]

4- It is computationally infeasible for an adversary, knowing the public key, PUb, to determine the private key, PRb.
5- It is computationally infeasible for an adversary, knowing the public key, PUb, and a ciphertext, C, to recover the original message, M

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption.	***Needed to Work:*** 1. One algorithm is used for encryption and a related algorithm for decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must share the algorithm and the key.	2. The sender and receiver must each have one of the matched pair of keys (not the same one).
Needed for Security: 1. The key must be kept secret.	***Needed for Security:*** 1. One of the two keys must be kept secret.
2. It must be impossible or at least impractical to decipher a message if the key is kept secret.	2. It must be impossible or at least impractical to decipher a message if one of the keys is kept secret.
3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Is the public-key encryption being more secure from cryptanalysis than is symmetric encryption?

The RSA Algorithm

A number of algorithms have been proposed for public-key cryptography. Some of these, though initially promising, turned out to be breakable. One of the first successful responses to the challenge was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman, and first published in 1978. The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.

RSA Procedure:

1-Choose two prime numbers p,q.

Let p=3, q=7.

2-Calculate n, n=p*q

N=21

3-Calculate Ø= (p-1)(q-1)

Ø=12

4-Choose **e** : 1<e< Ø and prime to Ø

Let e=5

5-Calculate **d** : d*e= 1 mod Ø

d is calculated using the extended Euclid's algorithm.

D=5.

Encryption: Encryption public key pairs: (e,n)

C= M^e mod n

If M=2 then C=11

Decryption: Decryption private key pairs: (d,n)

M=C^d mod n

If C=11 then M=2

Q : Analyze the encryption/ Decryption complexity of RSA algorithm.

Security Services

1-Authentication:

to assure the recipient that the message is from the source that it claims to be from. It aims to verify that received messages come from the alleged source and have not been altered.

2-Confidentiality:

Protecting the information from disclosure to unauthorized parties. The data kept unreadable by unauthorized parties.

3-Access Control:

The ability to limit and control the access to host systems and applications via communications links.

4-Data Integrity:

Protecting information from being modified by unauthorized parties.

Authentication Functions

Message authentication (or digital signature) mechanism has two levels of functionality:

Level 1: Function that produces an authenticator: a value to be used to authenticate a message.

Level 2: Authenticator is used as a primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

To achieve authentication, one of the following functions can be employed:

1 -**Message encryption**: The ciphertext of the entire message serves as its authenticator

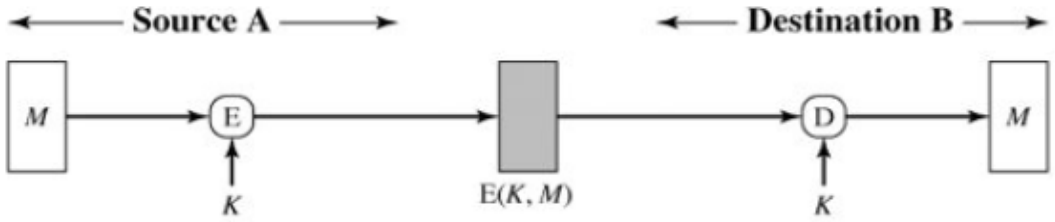
2-**Message authentication code (MAC)**: A function of the message and a secret key that produces a fixed-length value that serves as the authenticator.

3-**Hash function**: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.

1-Message Encryption:

It can be used in one of the following scenarios:

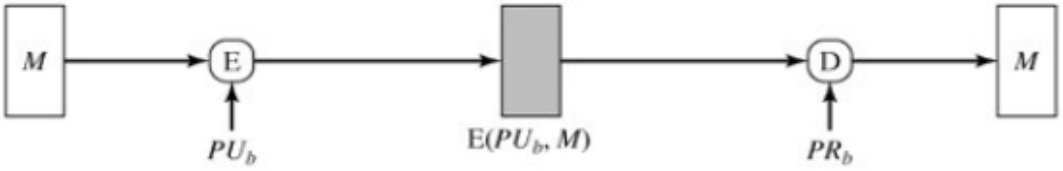
I- Symmetric Encryption



Does the confidentiality achieved? Why?

Does the Authentication achieved? Why?

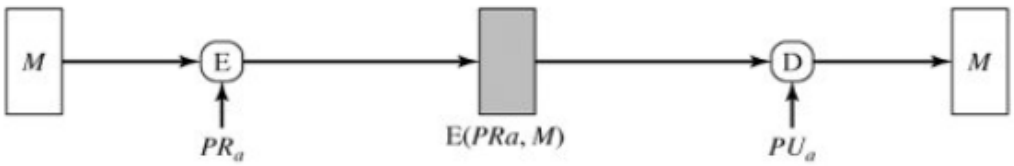
II- Public Key Encryption (a)



Does the confidentiality achieved? Why?

Does the Authentication achieved? Why?

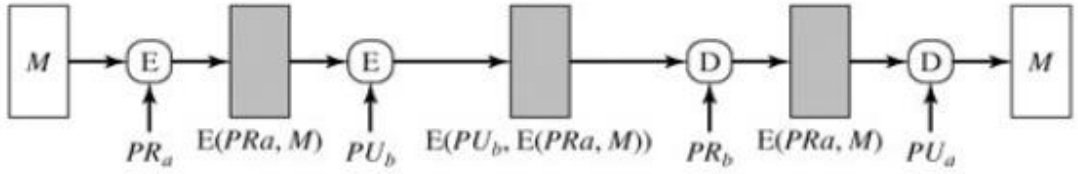
III- Public Key Encryption (a)



Does the confidentiality achieved? Why?

Does the Authentication achieved? Why?

IV- Public Key Encryption (c)



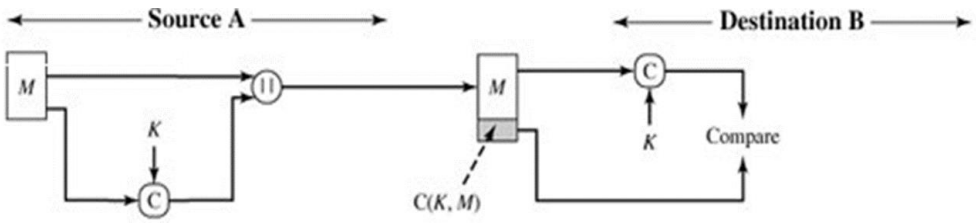
(d) Public-key encryption: confidentiality, authentication, and signature

Does the confidentiality achieved? Why?

Does the Authentication achieved? Why?

2-Message Authentication Code (MAC)

A function (C) of the message (M) and a secret key (K) that produces a fixed-length value that serves as the authenticator.



Does the confidentiality achieved? Why?

Does the Authentication achieved? Why?

3- Hash Code

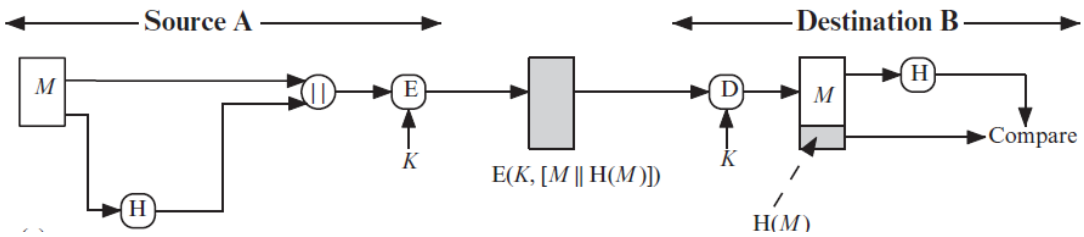
Hash function accepts a variable-size message M as input and produces a fixed-size output, referred to as a hash code H(M). Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value. Hash functions provide an error-detection capability, where a change to any bit or bits in the message results in a change to the hash code.

Hash Function Requirements:

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find y x such that H(y) = H(x). This is sometimes referred to as weak collision resistance.
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). This is sometimes referred to as strong collision resistance.

Hash code scenarios:

I- The message plus concatenated hash code is encrypted using symmetric encryption.



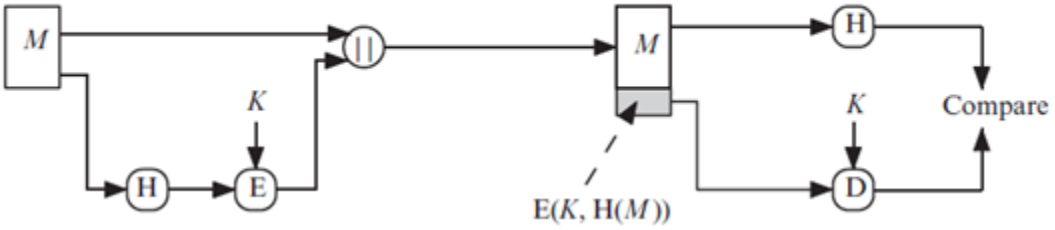
The hash code provides the structure required to achieve authentication. Why?

Because only A and B share the secret key, the message must have come from A and has not been altered.

Confidentiality is provided in this scenario. Why?

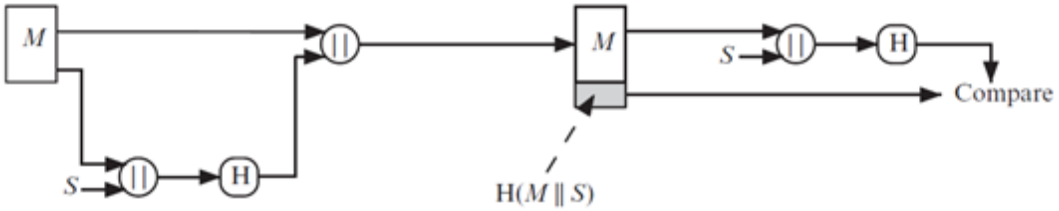
Because encryption is applied to the entire message plus hash code.

II- Only the hash code is encrypted, using symmetric encryption.



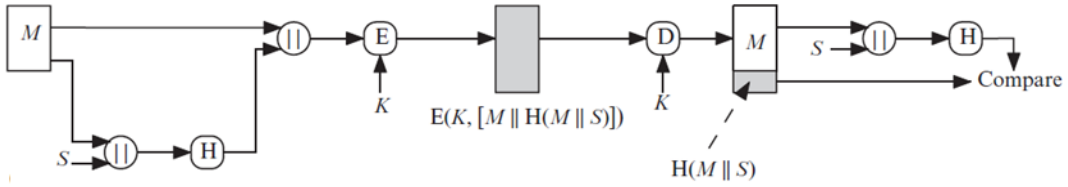
This reduces the processing load for those applications that do not require confidentiality. Why?

III- The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to M. (No encryption)



Is the confidentiality achieved?

IV- Confidentiality can be added to the approach of (III) by encrypting the entire message plus the hash code.



Digital signature:

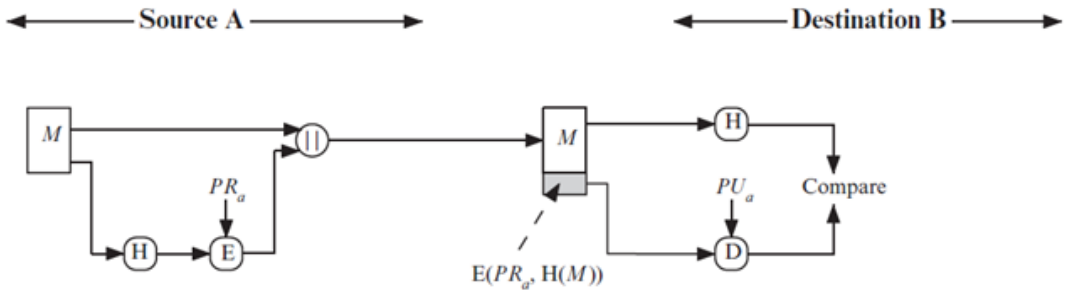
Digital signature is a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity. It is used in situations where there is not complete trust between sender and receiver, something more than authentication is needed.

The digital signature must have the following properties:

- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

Hash code for providing digital signature scenarios:

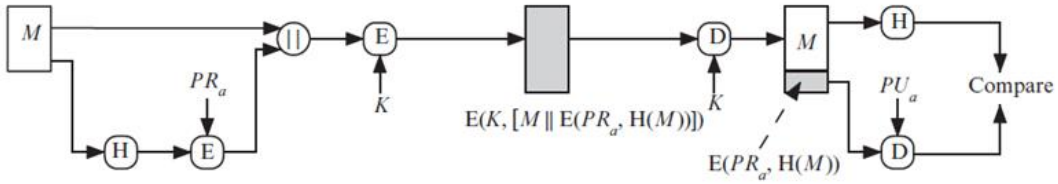
I- The hash code is encrypted, using public-key encryption with the sender's private key.



This provides authentication, and Digital signature, Why? Is the confidentiality achieved?

Because only the sender could have produced the encrypted hash code. this is the essence of the digital signature technique. No, because the message is not encrypted, it can be read by anyone.

II- If confidentiality as well as a digital signature is desired, then the message plus the private-key-encrypted hash code can be encrypted using a symmetric secret key. This is a common technique.



Simple Hash Function

Simple Hash function is performed using the following general principle. The input (message, file, etc.) is viewed as a sequence of n-bit blocks, and the input is processed one block at a time in an iterative fashion to produce an n-bit hash function.

XOR is true if the inputs differ
XOR is true if an odd number of inputs are true

```
 input: 00111011 11101101 00101000 00101011 01011000 11001110

chunked: 00111011
         11101101
         00101000
         00101011
         01011000
         11001110
xor of
columns: 01010011 (output)
```

Intrusion Detection and Intrusion Prevention Systems

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible threats. An intrusion detection system (IDS) is software that automates the intrusion detection process, while intrusion prevention system (IPS) is software that has all the capabilities of an IDS and can also attempt to stop possible incidents.

Motivations to create an intrusion detection system:

1. Certainly, the best intrusion prevention system will fail. A system's second line of defense is intrusion detection.
2. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
3. An effective intrusion detection system can serve as a warning, so acting to prevent intrusions.
4. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Fundamental Concepts[1]

IPS technologies offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as IDSs. Accordingly, for brevity the term intrusion detection and prevention system (IDPS) can be used.

IDPSs are primarily focused on identifying possible events. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting a weakness in the system. Many IDPSs can also be configured to recognize violations of acceptable use policies and other security policies example.

Example: The use of prohibited peer-to-peer file sharing applications and transfers of large database files onto removable media or mobile devices.

IPS technologies differ from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which can be divided into groups listed below.

---

[1] Scarfone, K., & Mell, P. (2010). Intrusion detection and prevention systems. In *Handbook of Information and Communication Security* (pp. 177-192). Springer, Berlin, Heidelberg.

IPS Response Techniques

1. The IPS stops the attack itself.

Example: the IPS terminating the network connection being used for the attack and the IPS blocking access to the target from the offending user account, Internet Protocol (IP) address, or other attacker attribute.

2. The IPS changes the security environment.

Example: IPS reconfiguring a network firewall to block access from the attacker or to the target, and the IPS altering a host-based firewall on a target to block incoming attacks.

3. The IPS changes the attack's content.

Example: IPS is removing an infected file attachment from an e-mail and then permitting the cleaned e-mail to reach its recipient.

False positive and False negative

A common attribute of all IDPS technologies is that they cannot provide completely accurate detection Incorrectly identifying benign activity as malicious is known as a false positive. The opposite case, failing to identify malicious activity, is a false negative It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other.

Evasion: Evasion is modifying the format or timing of malicious activity so that its appearance changes but its effect is still the same. Attackers use evasion techniques to try to prevent IDPS technologies from detecting attacks. Example, an attacker could encode text characters in a particular way that the attack is applied, hoping that IDPSs monitoring the activity will not.

Cloud Computing

Cloud computing is a model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly reached and released with minimal management effort or service provider interaction.

Cloud services can be classified into the following three types:

1- Software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser. Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service. SaaS saves the complexity of software installation, maintenance, upgrades, and patches. Example of services at this level are Gmail.

Platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. It is like SaaSs, except instead of delivering the software over the internet, PaaS provides a platform for software creation. Example is Google App Engine.

Infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources. As opposed to SaaS or PaaS, IaaS clients are responsible for managing aspects such as applications, runtime, OSes, middleware, and data. However, providers of the IaaS manage the servers, hard drives, networking, virtualization, and storage. Example is Google Compute Engine (GCE)

Shared Responsibility Model		
IaaS	**PaaS**	**SaaS**
Physical	Physical	Physical
Infrastructure	Infrastructure	Infrastructure
Network	Network	Network
Virtualization	Virtualization	Virtualization
Operating System	Operating System	Operating System
Application	Application	Application

Data	Data	Data
Service Configuration	Service Configuration	Service Configuration

Some cloud security threats and suggested countermeasures :

1- Abuse and nefarious use of cloud computing: For many cloud providers (CPs), it is relatively easy to register and begin using cloud services, some even offering free limited trial periods. This enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and denial of service.

The problem is on the CP to protect against such attacks, but cloud service clients

must monitor activity with respect to their data and resources to detect any malicious behavior.

Countermeasures include the following:

(1) Stricter initial registration and validation processes.

(2) Enhanced credit card fraud monitoring and coordination.

(3) Comprehensive introspection of customer network traffic.

(4) Monitoring public blacklists for one's own network blocks.

2- Insecure interfaces and APIs: CPs expose a set of software interfaces or APIs[1]

that customers use to manage and interact with cloud services. The security and availability of general cloud services are dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to evade policy.

Countermeasures include the following:

(1) analyzing the security model of CP interfaces;

(2) ensuring that strong authentication and access controls are implemented in concert with encrypted transmission;

(3) understanding the dependency chain associated with the API.

[1]A Cloud Application Programming Interface (Cloud API) is a type of API that enables the development of applications and services used for the supplying the cloud hardware, software, and platforms.

3- Shared technology issues: IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture.

Countermeasures include the following:

(1) implement security best practices for installation/configuration.

(2) monitor environment for unauthorized changes/activity.

(3) promote strong authentication and access control.

4- Data loss or leakage: For many clients, the most devastating impact from a security breach is the loss or leakage of data. Data must be secured while at rest, in transit, and in use.

Countermeasures include the following:

(1) Implement strong API access control.

(2) Encrypt and protect integrity of data in transit.

(3) Analyze data protection at both design and run time.

(4) Implement strong key generation, storage and management, and destruction practices.

Physical Security

Most recent physical security strategies make use of both technology and specialized hardware to achieve its safety goals, for example the finger print. Any company needs to protect it self from intruders, internal threats, and any time of accident, which in turn requires a mix of technology and in-person monitoring that requires careful planning and placement of security staff and other tactics. Physical security protects the company's physical computer and networking building, server room, backup media, and hence, your people. Biometric devices as the fingerprint, get the visitor's finger print and compare it with the traits on file to determine whether they are who you claim to be. It provide an important first defense against intruders.

There are a number of physical security controls available in the market that the organization should consider for implementing physical access controls both inside and outside of the facility. Some of the controls include*:

Security Guards at each of the entry and exit points

ID cards and badges to all employees, and contractors

Electronic Access cards for all the major door

Electronic monitoring and Surveillance camera

Metal Detectors

Electric Fencing

Alarms and Alarm systems

Specialized access to computer labs, data centers, server rooms, and R&D labs

Biometrics

Automatic Locks and keys.

*Rao U.H., Nayak U. (2014) Physical Security and Biometrics. In: The InfoSec Handbook. Apress, Berkeley, CA