CHAPTER 1

UNIT I

Security Basics

Syllabus :

At the end of this unit, you should be able to understand and comprehend the following syllabus topics :

- Introduction
- Elements of Information Security
- Basic Terminologies in Network Security
  - Categories of Security Services
  - Security Techniques / Steps / Mechanisms
  - Operational Model of Network Security (Network Security Model)
- Threats and Vulnerability
- Security Policy
- Difference between Security and Privacy

1.1 Concept Building – Security – What is it really?

– Before we begin with understanding information security and its related concepts, let's talk.

Let me ask you a question : *How do you manage your Debit Card and its PIN? Do you leave your Debit Card unattended and with PIN information available to everyone?"*

Your Response : *(Laughingly) Of course, not. I keep my Debit Card with me all the time and never share my PIN with anyone".*

My Response : *"Oh, that's nice. But, why do you need to do that?"*

Your Response : *"Because, I need to ensure that my money is safe, and no one takes it out except me. I don't trust everyone with my money these days, you know"*

My Response : *"Got it. You are a security champion".*

– If you followed our conversation, you already know what security is. Our job is easy now. Let us define some terms around our conversation above.

1. **Assets :** You were trying to protect your money, isn't it? It is called Assets. Money is your Asset in our conversation that you were trying to protect.

✍ ***Definition :*** *Assets are something that has value and is worth protecting.*

Security is all about ensuring that the assets are kept protected all the time as much as possible within your capabilities or means.

2. **Controls (or Countermeasures) :** So, how did you actually safeguard your money? You didn't leave the Debit Card around and you memorised your PIN. Isn't it?

Definition : Any countermeasures or actions that you take to safeguard an asset are called Controls.

So, in our conversation, you have put two controls in place to safeguard your money – first is to keep your Debit Card with you and second is to memorise your PIN. You are a security champion!

3. **Threat :** Hey, you told me that you don't trust everyone with your money, isn't it? That unknown everyone who can do evil to you or can harm you is called a Threat.

Definition :A threat is a person or an entity that can exploit an asset bypassing your controls (if they are weak controls and not enough to safeguard your asset).

You knew there are threats around your money, and you protected it so well. You are a security champion.

4. **Vulnerability :** What if you left your Debit Card and PIN on the table for anyone to get hold of them and use? I hear you scream, "Come on, why would I do that to myself?" Exactly you would not want to create a situation in which your assets can be harmed. This is precisely called addressing (or avoiding) a Vulnerability.

Definition : Vulnerability is the weakness or lack of controls around assets.

I am happy that you have put two good controls (keeping your Debit Card safe and memorizing your PIN) and you avoided the vulnerability around your money (asset).

5. **Risk :** So far, you would agree that leaving Debit Card and PIN unattended poses a likelihood that someone might just grab them and use them.

Definition : That likelihood of a harm occurring to an asset is called Risk.

It is this Risk that you want to reduce by applying controls around your assets. Remember one thing here, Risk can NEVER be 0 (zero). Someone can steal your Debit Card from your wallet and force you at gunpoint to tell your PIN. The core thing that you need to ensure when dealing with Risk is "to reduce it to an acceptable level". Never aim to make anything (or any asset more precisely speaking) risk free because that's not possible, really.

6. **Exposure :** Someday suppose you do accidently leave your Debit Card behind and your PIN was known to someone, you could actually lose some or all your money. That particular day or rather that particular situation of you forgetting your Debit Card behind could lead to an exposure.

Definition : Exposure is an instance of being harmed.

So, if you got exposed anytime, immediately change your PIN and take a lesson in security to apply controls always around assets so that you do not have future exposures. I am sure you won't have exposures because you are a security champion already, aren't you?

Let summaries the above terms in a simple block diagram as shown in Fig. 1.1.1.

If you are feeling good about what we talked about so far, believe me, you have started your security journey on a high note. The several chapters and topics that you read in this book (howsoever complex or dry they look at first) are all written to help you effectively do just ONE thing : **Safeguard your Assets.**

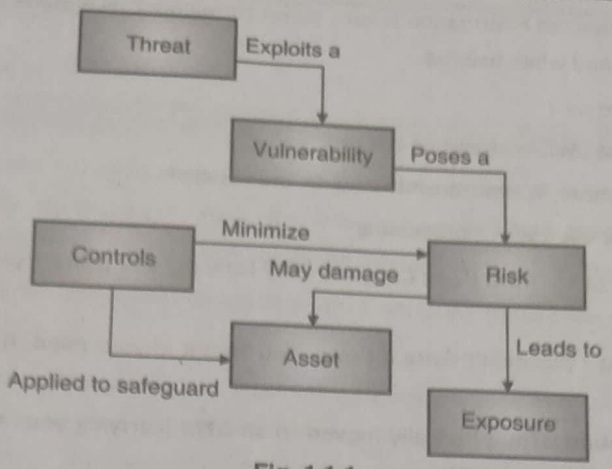

Fig. 1.1.1

- If you know what you are
  - Trying to protect.
  - And from whom.
  - And how.

  You understand security. There is nothing else to learn.

1.2 Elements of Information Security

SPPU - May 19

Q. List and explain various elements of Information Security. (May 19, 5 Marks)

- Now that you have a general understanding of security, let's set some context about Information Security. When we say information security – what exactly are we protecting? What is the asset? The asset here is "Information" or more precisely "Digital Information". The information could be about your Facebook user account, Online bank account, OS password, email or pretty much anything that touches a computer system.
- There are 3 tenets (or pillars) of security:

1. Confidentiality
2. Integrity
3. Availability

- These tenets in short are also called as the CIA triad or any other combination of the first letters in their words. These are also sometimes called **goals of security**.
- Let's dive deeper into each one of them.

1. Confidentiality

- Confidentiality can be defined as,

Definition : *An act of protecting information from unauthorised disclosure to an entity.*

- It ensures that the protected information is kept secret throughout its lifetime and is made available only to the authorised entities as and when needed.
- The information should be
  - **Protected at Rest :** When stored on the disk
  - **Protected in Motion :** When transmitted over the network
  - **Protected during Use :** When processing
- Remember our conversation from Debit Card and PIN? How did you protect your PIN and provide confidentiality to it?
  - **Protected at Rest :** You didn't write it down. You kept it in your mind. No one could know or use it except you.
  - **Protected in Motion :** You physically moved to an ATM (carrying your mind and the protected PIN there) instead of revealing it to anyone.
  - **Protected during use :** You watch out if someone is looking at your fingers as you punch the PIN on the ATM keyboard
- In terms of digital information, confidentiality is enforced using several mechanisms:
  1. Encryption
  2. Access control
  3. Data classification
- We would be studying them at depth in later chapters.

2. Integrity → modification

- Integrity can be defined as,

Definition : *An act of protecting information from unauthorised modification by an entity.*

- It ensures that the information remains intact and no unauthorised entity can modify it. Any modification to the information is allowed only if the entity is authorised to do so. The information requires maintaining its integrity throughout its lifetime.
- For example, during criminal investigations, any evidence that you collect is protected from touching or any modifications to ensure that those evidences can be used during court proceedings. If evidence is tampered, it is not admissible in the court and cannot be used. Another example is email. If I send you an email and someone changes it before you read it, you might get wrong information, or it could be severely damaging to our relations.
- In terms of digital information, integrity is enforced using several mechanisms:
  1. Hashing
  2. Access Control
  3. Data Classification
  4. Input and output sanitization
- We would be studying them at depth in later chapters.

3. Availability → Destruction

- Availability can be defined as,

Definition : *An act of protecting information from unauthorised destruction by an entity.*

- It ensures that the information is adequately protected to remain available when it is needed. Any unauthorised entity should not be able to destroy it. Also, the availability principle extends to any equipment such as computers, network devices and printers. These should be available and be able to perform as expected.
- If someone can get access to them and then prevent you from using these then that impacts availability of the system for your use.
- For example, your Windows or Linux systems track all activities done on the system via log files. If I do some mischief around your computer and then delete the log files, you would have no way to prove that I did something to your computer. The availability of log files is crucial to ensure that the system is adequately monitored and protected from any security mishaps.
- Availability is generally enforced using several mechanisms:
  1. Access control
  2. Isolation
  3. Back up
  4. Disaster Recovery
  5. Business continuity processes

C → Disclosure (unauthorized)
I → Modification
A → destruction

- We would be studying them at depth in later chapters.
- Let's summarise the above 3 security principles with the help of diagrams as shown in Fig. 1.2.1.

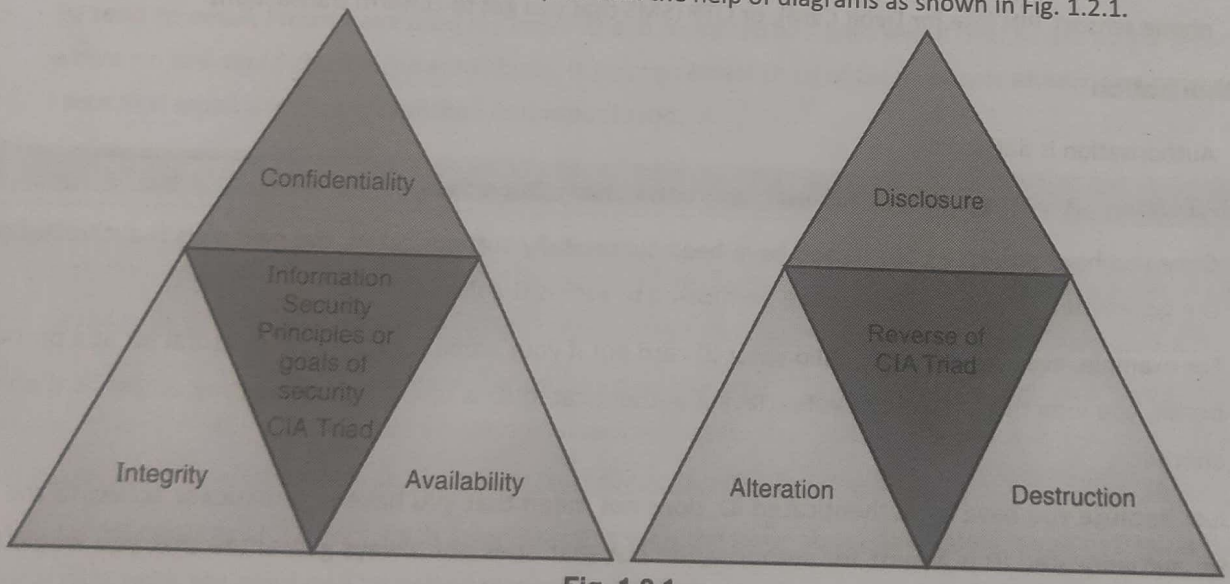

Fig. 1.2.1

- Confidentiality, Integrity and Availability are the 3 core principles of security. Ensuring that you understand the objectives behind these principles is crucial to your success in the information and cybersecurity domain.

4. Identification

- Identification (in short ID) is defined as,

Definition : A way to claim an entity's presence with respect to the process being carried out.

- This means that during a process, your presence (or your consent) is ascertained (or established).
- For example, when you try to login to your Facebook account, you provide your Email or Phone number to establish your presence during the login process.
- There are several other forms of identification that we use today such as Aadhar Card, PAN Card, Voter ID, Debit Card, Admit card, etc. All of these identification methods bring a sense of credibility that you are present, or you give your consent to complete a particular process.

5. Authentication

- Authentication is defined as,

Definition : A way to ensure that the entity is indeed what it claims to be.

- This means that providing just the ID is not enough. You must additionally prove that the ID belongs to you. For example, even if I know your Facebook email address or phone, I cannot login as you until I also know the password.
- Thus, knowing just the ID is not enough. We need to prove that the ID belongs to us and that is what is precisely called authentication. It is for this reason that you need to additionally sign when you submit Aadhar card or PAN card as an ID proof to ensure that someone didn't just use the photocopy of those IDs without your permission (or consent). Some of the ways to authenticate an ID are passwords, biometric (like your Aadhar fingerprints or phone sensor), PIN (like for Debit Card), or OTP (SMS that you get to confirm transaction).

6. Authorisation

- Authorisation is defined as,

Definition : A way to determine what resource an entity can access.

- Once you have provided your ID and have been successfully authenticated, the next step is authorisation where the system determines if you have the permission to access the desired object.
- For example, even if you have a valid voter ID card but if your name is not on the electoral list at a particular area booth, you won't be allowed to vote. Having authenticated ID is one thing and getting access to the resource is another.
- Just because you have an authenticated ID, does not mean that you have automatically access to the resources. So, authenticated ID is a must for authorisation but that does not always guarantee that you would be allowed access.

7. Accountability

- Accountability is defined as,

Definition : A way to record your actions.

- Suppose, you used a system to take print outs. That system logs this action (pretty much like you record attendance in lab or classroom) to build a trace (evidence or proof) that you used the printer.
- If you were not supposed to use the printer, the evidence can be used to find you accountable for using it without permissions and could result in particular consequences.
- Accountability is a key determinant of how securely a system is operating. The logs generated are continuously monitored and necessary alarms are raised if any entry is found to be suspicious.
- Let's summarise the 4 access control steps with the help of Fig. 1.2.2.

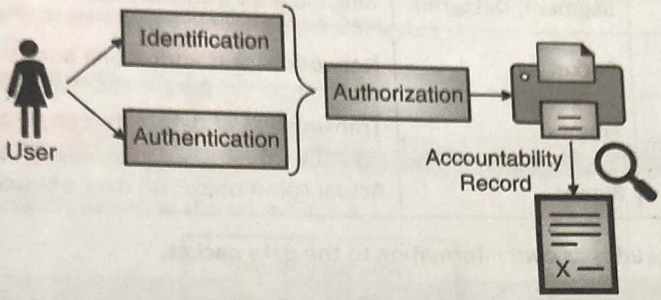

Fig. 1.2.2

8. Non-repudiation

- Non-repudiation is defined as,

Definition : *A way to prove your actions.*

- It is used in conjunction with accountability and the CIA triad. Non-repudiation provides an assurance that someone cannot deny their actions later on. For example, if I sent you an email, I cannot later deny that I did not.
- To send an email, I must have used my email ID and password and then sent it over to you over a secure network where no one could change the email body. If you can establish all of these facts truthfully, you have proven that I sent that email and thus established non-repudiation.

1.3 Basic Terminologies in Network Security (OSI Model)

Note : Discussing OSI Model in-depth is beyond the scope of this book. It is assumed that you have covered it in detail in your subjects on networking. A general high-level overview is presented here as a refresher.

Definition : *The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of networked communications without diving into complexities of protocols, architecture and the underlying technologies.*

- The OSI model consists of 7 layers. Each layer interacts with the layer above and below it and passes on the respective protocol data units encapsulated into their respective headers.

Table 1.3.1

Layer Number	Layer Name	Protocol Data Unit	Function
7	Application	Data	Application Interface – APIs, UIs
6	Presentation	Data	Data translation between networking and application
5	Session	Data	Manage communication sessions between sender and receiver
4	Transport	Segment, Datagram	Reliable data transmission
3	Network	Packet	Network packet addressing and routing
2	Data Link	Frame	Transmission of data between two nodes
1	Physical	Binary	Actual communication over physical media

- Here each OSI layer protocol adds its own information to the data packet.

✍ ***Definition :*** *The process of adding layer specific information and passing on the data to the next layer below is called encapsulation.*

- Encapsulation happens top – down (From Application to Physical Layer).

✍ ***Definition :*** *The process of removing layer specific information and passing on the data to the next layer above is called decapsulation.*

- Decapsulation happens bottom – up (from Physical to Application Layer).
- Table 1.3.2 shows quick reference summary for various protocols at the respective OSI Layers.

Table 1.3.2

Layer Name	Protocols Used
Application	HTTP, FTP, SMTP, etc.
Presentation	JPEG, MPEG, TIFF, ASCII, etc.
Session	NFS, RPC, etc.
Transport	TCP, UDP, SSL, etc.
Network	IP, ICMP, OSPF, etc.
Data Link	ARP, PPP, Ethernet, etc.
Physical	ISDN, DSL, 10Base-T, etc.

1.3.1 The OSI Security Architecture

- *The objective of the OSI model is to permit the interconnection of heterogeneous computer systems so that communication between application processes may be achieved.*

- At the various OSI layers, the security controls must be established in order to protect the information exchanged between the application processes (or the connected computers or devices). Such controls make it difficult to obtain the information in any unauthorised way.

✍ ***Definition :*** *The OSI Security Architecture identifies the basic security services and mechanisms and their appropriate placement at the various layers.*

- OSI security functions are concerned only with the OSI layers involved in the communications path. It does not include other security controls such as securing the operating system or the application process itself. Let's learn about the various security services and mechanisms placed at the OSI layers.

1.3.2 Categories of Security Services

✍ ***Definition :*** *Security services are safeguard controls recommended to be placed at the various OSI layers.*

- The various security services are listed as shown in Fig.1.3.1.

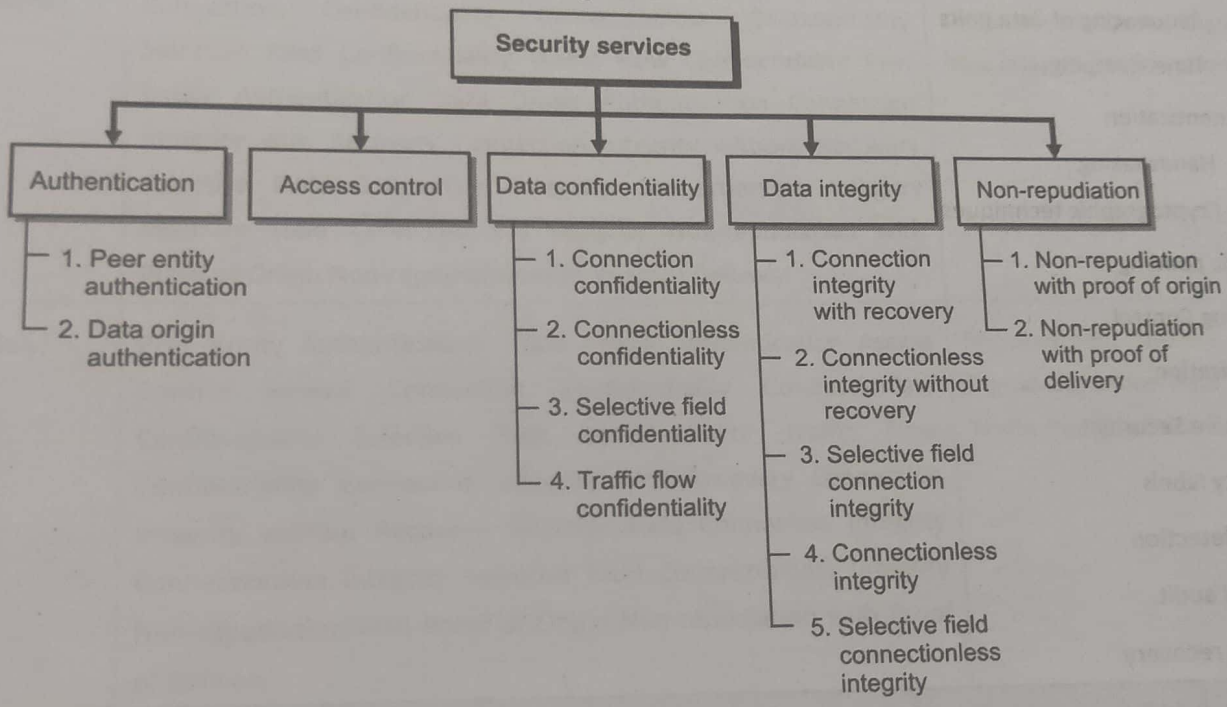

Fig. 1.3.1

1.4 Security Techniques / Steps / Mechanisms

✍ ***Definition :*** *Security mechanisms are various techniques recommended to provide security services at the various OSI layers.*

The various security mechanisms that can be applied are as following.

- Encipherment (Encryption)
  - Symmetric
  - Asymmetric

- Digital Signature
  - Signing a data unit
  - Verifying a data unit
- Access control
  - Passwords
  - Time of access
  - Duration of access
  - Access route
- Data integrity
  - Sent quantity of data
  - Received quantity of data
  - Sequencing of data units
  - Time stamping
- Authentication
  - Handshaking
  - Cryptographic techniques
- Traffic padding
- Routing Control
- Notarization
- Pervasive Security
- Security labels
- Event detection
- Security audit
- Security recovery

Note : You would learn these techniques throughout this course.

1.4.1 Placement of Security Services and Mechanisms

- Now that you have a fair understanding of the various security services and the security mechanisms that can be used at the various OSI layers, let us see recommended placement for them.

OSI Layer	Security Service	Security Mechanism
Physical Layer	Connection Confidentiality Traffic Flow Confidentiality	Encipherment
Data Link Layer	Connection Confidentiality Connectionless Confidentiality	Encipherment

OSI Layer	Security Service	Security Mechanism
Network Layer	Peer Entity Authentication Data Origin Authentication Access Control service Connection Confidentiality Connectionless Confidentiality Traffic Flow Confidentiality Connection Integrity without recovery Connectionless Integrity	Authentication Encipherment Digital Signature Access control Routing control Traffic Padding Data integrity
Transport Layer	Peer Entity Authentication Data Origin Authentication Access Control service Connection Confidentiality Connectionless Confidentiality Connection Integrity with recovery Connection Integrity without recovery Connectionless Integrity	Authentication Encipherment Digital Signature Access control Data integrity
Session Layer	No security services are provided in the session layer	Not Applicable
Presentation Layer	Connection Confidentiality Connectionless Confidentiality Selective Field Confidentiality Traffic Flow Confidentiality Peer Entity Authentication Data Origin Authentication Connection Integrity with Recovery Connection Integrity without Recovery Selective Field Connection Integrity Connectionless Integrity Selective Field Connectionless Integrity Non-repudiation with Proof or Origin Non-repudiation with Proof of Delivery	Encipherment Digital Signature Data integrity Notarization
Application Layer	Peer Entity Authentication Data Origin Authentication Access Control Service Connection Confidentiality Connectionless Confidentiality Selective Field Confidentiality Traffic Flow Confidentiality Connection Integrity with Recovery Connection Integrity without Recovery Selective Field Connection Integrity Connectionless Integrity Selective Field Connectionless Integrity Non-repudiation with Proof of Origin Non-repudiation with Proof of Delivery	Encipherment Access Control Digital Signature Data integrity Traffic Padding Notarization

1.5 Operational Model of Network Security (Network Security Model)

SPPU - March 19(In Sem.)

Q. Explain Operational Security Model for Networks Security. **(March 19, 5 Marks)**

Definition : *Network Security Model (NSM) is a seven-layer model that divides the task of securing a network infrastructure into seven manageable sections.*

It is similar to the seven OSI layers. The model is generic and can apply to all security implementation and devices. NSM provides a unified way of securing networks. It is easier to pinpoint issues at the respective NSM layers and address the gaps, if any.

Table 1.5.1 lists the NSM layers and how they align with the OSI layers. It is important to understand that like the OSI layers, each NSM layer builds on top of the previous layer.

– If any layer is compromised, the layers above it are disrupted as well. For example, if there is an attack at NSM layer 2, it would disrupt layers above it (3, 4, 5, 6 and 7). Let's learn about each of the NSM layers.

Table 1.5.1

Network Security Model (NSM)	OSI Model (inverted)
Physical	Physical
VLAN	Data Link
ACL	Network
Software	Transport
User	Session
Administrative	Presentation
IT Department	Application

1. **NSM Layer 1 : Physical :** It works at the physical layer. It ensures to safeguard the physical aspects of network. For example, physical access to the routers, switches or any other is networking equipment. There could be several physical forms of physical security such as security alarms, security guards and CCTV.
2. **NSM Layer 2 : VLAN :** VLAN stands for Virtual Local Area Network. At this layer, the network is segmented (partitioned) into smaller network chunks to safeguard them individually and to also manage them effectively. It ensures that only authorized devices connect to the provided networks. You could create VLANs department wise, region wise or in any other suitable grouping mechanism based on your site requirements.
3. **NSM Layer 3 : ACL :** ACL stands for Access Control List. ACLs are created to allow or deny access based on the network layer from the OSI layer. For example, certain IP ranges (say finance department) might be restricted for access by other devices on the network. ACLs can be created on routers, firewalls and switches and can effectively control the network access as designed and intended.
4. **NSM Layer 4 : Software :** The software layer is focused on keeping the device software up to date with the latest upgrades and patches in order to mitigate any known software vulnerabilities. At this layer, the patches are installed to ensure that the software running on the device cannot be exploited. For example, you install security patches on your operating system or update applications on your phone to ensure that you are running the secure version of the software and it does not have any known exploits.
5. **NSM Layer 5 : User :** This layer deals with the user access and management. The user layer focuses on the user's training and knowledge about security on the network. The user should understand the basic concepts of network security and should be capable of applying security related judgement. For example, users should be aware of which software to run on the system and which not.
6. **NSM Layer 6 : Administrative :** The administrative layer focuses on the training of administrative users. It works very similar to the user layer but focuses primarily on the administrative staff. It provides guidance to the layers below it to adequately protect the network. For example, it can dictate which software is allowed for user consumption.
7. **NSM Layer 7 : IT Department :** The IT department layer deals directly with the maintenance of all layers and making sure that the entire network works correctly from NSM model. It has several professionals in the team that know to architect and operate a secure network.

1.6 Security Threats and Vulnerabilities

- From our previous discussion on Debit Card and PIN, you now understand what security threat and vulnerabilities mean. Threats can exploit your assets and vulnerabilities are situations that could possibly lead to such an exploit.
- Let us review some of the security threats and vulnerabilities commonly found in the context of information security.

1.6.1 Security Threats

- There are several security threats to an information system. Some of them are briefed as shown in Fig. 1.6.1.

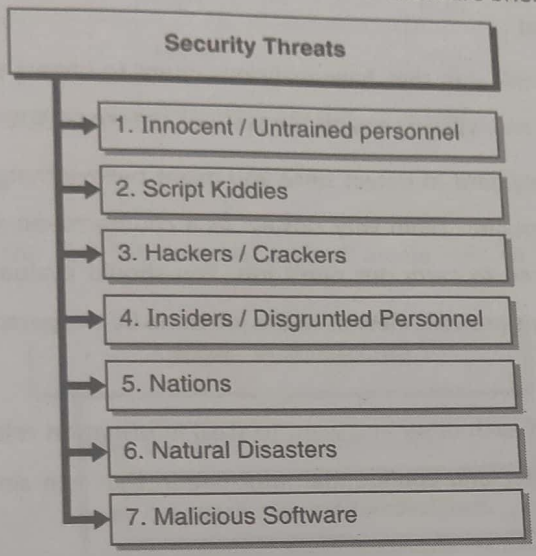

Fig. 1.6.1 : Security Threats

1. Innocent / Untrained personnel

- These could be your employees, household members or any person who does not understand intricate complexities of security. These people believe the information presented to them and often are soft targets of several frauds.
- These can get easily convinced and can be pushed to do harm to your organisation (say by sharing critical details) or to any other critical asset. As a countermeasure, you should provide security training time to time and enforce the idea that security is everyone's responsibility.

2. Script Kiddies

- These are just exploiting the systems for fun. They have a lot of free time and can go around the internet to find systems that have weak controls. Once a system is found, they can play games, watch movies, download other software or just send some random messages on the screen.
- These do not have sophisticated skills to exploit weaknesses themselves and usually depend on attack tools or software. As a countermeasure, test your website and software against general attack tools and ensure that any weaker controls are sufficiently addressed.

3. **Hackers / Crackers**
   - These are people who have sophisticated computer security skills. They have a deep understanding of how various protocols, services, operating systems, drivers, network equipment etc. work and can thus launch sophisticated attacks on such information systems.
   - They usually hide their presence and activities to ensure that they are unnoticed and can exploit the systems for a long time without getting detected. As a countermeasure, invest in penetration testing of your website and software and ensure that all the security findings are adequately addressed.
4. **Insiders / Disgruntled personnel**
   - These people are on your side, but they have malicious intent to impact your systems. They might have grudge on you or the organisation and typically exploit the systems to take revenge.
   - Insider threats are extremely hard to detect since you might believe that their actions are part of their job and may not suspect them or monitor them very closely. As a countermeasure, use access control to provide least possible permissions required to carry out one's job. You should evaluate the permissions time to time and ensure that those permissions are still relevant to the job done by the person.
5. **Nations**
   - Many a times, nations spy on each other and want to steal information related to country defence, forces, arms, and other intellectual property and confidential information that can severely damage the reputation of the country or its economics.
   - These attacks are highly sophisticated but have huge impact on nations. For example, you might have heard of Russian involvement in the US elections. As a countermeasure, nations typically protect the sensitive information by limiting information sharing only amongst the high-ranking officials. They deploy top notch security solutions, processes and continuously monitor their operations to detect any unauthorised activities.
6. **Natural disasters**
   - Natural disasters such as flood, earthquake, lightning, etc. can severely damage the information systems (remember availability as one of the tenets of security?) and could impact information availability.
   - As a countermeasure, you invest in backup, business continuity processes and disaster recovery solutions that can quickly bring back the systems and information to avoid large impact on your business.
7. ***Malicious software***
   - These are software programs written with malicious intent. The purpose of these programs is to harm the information systems or extract useful information in an unauthorised manner.
   - As a countermeasure, you install such software detection tools. These tools could be anti-virus, anti-malware anti-spyware, intrusion detection system, intrusion prevention system, etc. We would explore this in depth in the subsequent section.

1.6.1(A) Comparison between Security Threats

Sr. No.	Threat	Skills required	Impact	Detection Possibility
1.	Innocent / Untrained personnel	None	Low - High	Low
2.	Script Kiddies	Medium	Low - High	High
3.	Hackers / Crackers	High	High	Low
4.	Insiders	Low	High	Low
5.	Nations	High	High	Low
6.	Natural disasters	None	High	Low
7.	Malicious software	Medium	High	High

1.6.2 Security Vulnerabilities

As you recall, vulnerability is the lack of controls around assets. Let us see some of the common security vulnerabilities.

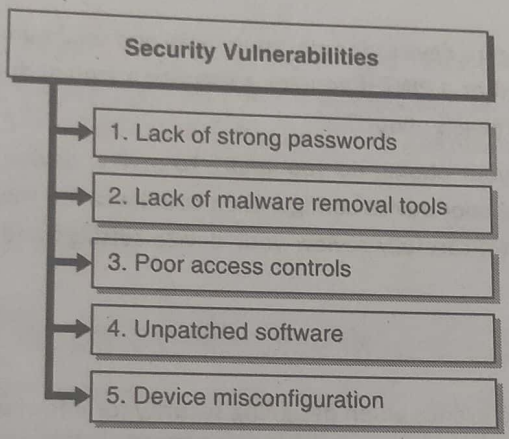

Fig. 1.6.2

1. Lack of strong passwords

- Passwords are everywhere. For quick and easy recall, you tend to choose simple passwords such as your name, date of birth, school name, etc. People, who know you, are generally aware of this information as well and can try to use this information as your password.
- Additionally, if you tend to choose simple English words as your passwords, someone can do a dictionary-based attack (more on that later) and can find out your password.
- As a countermeasure, always choose a complex password that is the combination of uppercase letters, lowercase letters, digits and special characters. Change your passwords regularly and do not use old passwords.

2. Lack of malware removal tools

- There are several malwares that can be installed on your device as you browse through various websites on the internet.

- If you do not have a good malware removal tool, overtime, your device might be compromised and impacted. As a countermeasure, install a reputed malware removal tool and update its definitions time to time.

3. **Poor access controls**

Do you allow everyone to be an administrator on your system? Can anyone access anything? If your answers are yes, you probably have not thought through the "Least Privilege" principle yet. You should only grant enough permission as required by the job at hand. No more and no less. Understand the different permissions required and assign them accordingly.

4. **Unpatched software**

- Vendors release security patches (software bundles that fix something in the software installed previously) time to time to fix security vulnerabilities found.
- If you do not install these patches, your system could be prone to exploit because the required security fix to stop the exploit is not installed.
- As a countermeasure, install software updates as released by the vendor specially the ones that carry security fixes.

5. **Device misconfiguration**

- Quite a few times, we configure devices for maximum ease and minimum security. For example, have you locked your phone with a password or a PIN? If you get a security warning, do you click ok even without reading and understanding what the warning is about ?
- When installing an app on your phone, do you ignore to review device permissions that the app would have? Such ignorant behaviour and poor device configuration could weaken the controls that the vendor has put out of factory. As a countermeasure, carefully review your device settings and ensure that they are tuned to provide adequate security.

1.6.3 STRIDE Model

STRIDE model is often cited as a reference when designing security for information systems.

Attack Category	Security Property that is attacked
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of service	Availability
Elevation of Privilege	Authorisation

1. ***Spoofing :*** When someone tries to steal your identity, it is called spoofing. Spoofing is also called as impersonating someone or something. For example, if I try to login to your Facebook account using your email address and password guesses, I am trying to spoof or impersonate your identity. Spoofing can also be used for fake news, fake websites, fake or malicious files or anything else that could be mistaken for being real. The target of spoofing attacks is to crack authenticity (of person, file, website, news or anything real).

2. **Tampering :** When someone tries to do an unauthorised modification to something, it is called tampering. You would have heard of cricketers tampering with the ball to suit their requirements. It is a punishable offense. Similarly, in information systems, if you try to tamper with say files, emails, or any other information in an unauthorised way, it is called tampering. Basically, you are trying to attack the integrity of the object by making such alterations.
3. **Repudiation :** In this, you are trying to falsely claim that you didn't carry out a particular action. For example, you didn't send an email or didn't visit a website. Remember your childhood days when you broke something and you try to escape the punishment saying that you didn't actually break it and then your parents finding proofs that it was indeed you who broke it. That's precisely what non-repudiation is. In repudiation attacks, you are trying to destroy evidences that someone can use to falsify your denial claims.
4. **Information disclosure :** This pertains to unauthorised revealing of any confidential information. In these attacks, the attacker wishes to know the confidential information and tries to crack controls around it to get hold of such confidential information.
5. **Denial of service :** In this type of attacks, the purpose of attack is to make the information system or its services unstable or unavailable to perform its assigned activities. For example, if you can succeed to bring Flipkart website temporarily down, it might mean severe loss of business for Flipkart and the customers may go to a different website for placing their urgent orders.
6. **Elevation of privileges :** In this category of attack, the attacker tries to get elevated (higher) privileges (permissions / authority) over resources. For example, if you are only a user on a system and you try to attack the system to become an administrator on the system, it is called an elevation of privileges attack.

1.7 Security Attacks

SPPU - March 19(In Sem.)

Q. How Information Security attacks are classified? Give example for each. **(March 19, 5 Marks)**

At a high level, there are two broad categories of security attacks carried over the network – active attacks and passive attacks.

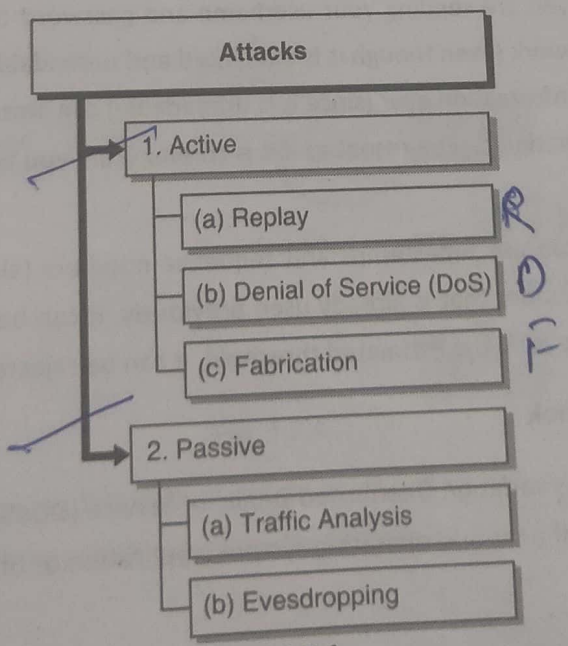

Fig. 1.7.1

1.7.1 Active Attacks

- An active attack is defined as,

Definition : An attack where the attacker actively participates in the in the communication or the attack mechanism and disrupts the systems by sending several manipulated inputs.

- In a nutshell, the attacker intercepts (captures) the communication channel, and manipulates the communication going over it. Another variation of the active attack is when the attacker continuously disrupts the ability of the system to process the information correctly. Let us expand on some of the examples of active attacks.

1. Replay Attack

- This is like replaying a song. The attacker captures the real and specific communication packets, stores them with herself, and then sends it at a later point in time as though she is sending the information for the first time like authentic information.

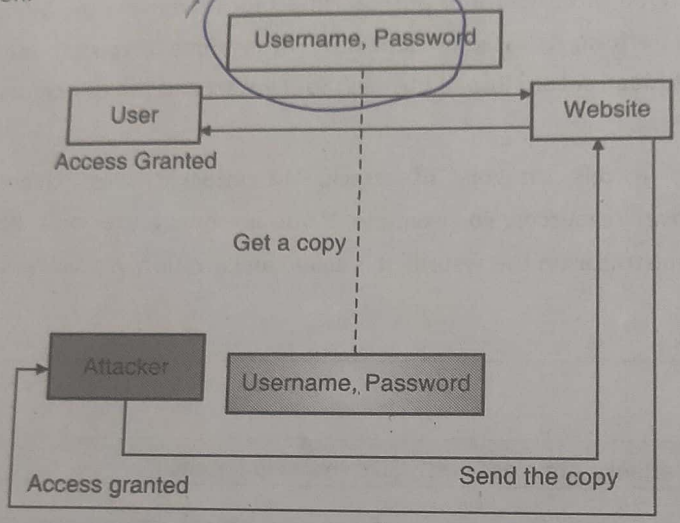

Fig. 1.7.2

- **For example :** Suppose you are sending your username and password to Facebook. Someone can capture that information over the network (even though it is encrypted and unreadable) and without even knowing the actual content of the captured information ever (since it is unreadable) can store it with herself. At a later point in time, the same captured information can be resent as if it is coming from you and the attacker might get access to your Facebook account.

- **Countermeasures :** You can use timestamps and sequence numbers (also called as session ID). If the message comes with a sequence number that is already used previously, it can be rejected. Similarly, if a message comes with a timestamp that is beyond the estimated threshold, it can be rejected.

2. Denial of Service (DoS) Attack

- Denial of Service (DoS) or its variation Distributed Denial of Service (DDoS) refers to a category of attacks that can be aimed at various layers of network, operating system, application or other parts of information systems.

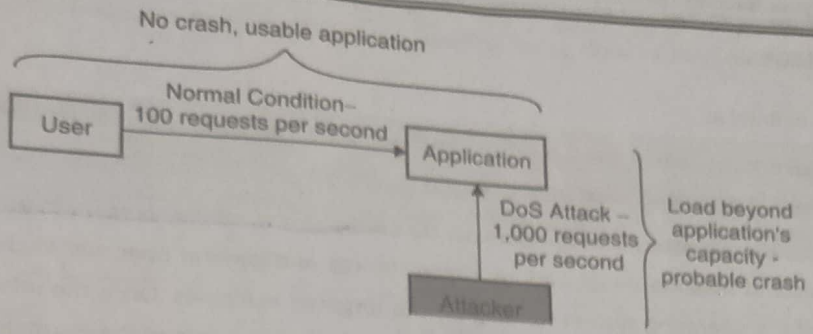

Fig. 1.7.3

- In this type of attack, the attacker overloads the system beyond its capacity such that the system or controls around it fail.
- Once the system fails, it is no more available for performing its assigned activities. For example, an application might be capable of processing a maximum of 100 requests per second. Attacker would typically send over 1,000 requests per second such that the application fails to cope up with it and crashes. The sole motivation behind DoS attacks is to bring down the availability of the system.
- **Countermeasures :** Some of the countermeasures to protect from DoS are firewall, application limit, whitelisting networks, etc. Firewall can be used to drop network connections that come from a particular location or based on other networking parameters (a list of allowed IP addresses, etc.). Application limits can protect application from crashing when the rate of requests goes beyond a set limit.

3. Fabrication Attack

- Fabrication attack is again a broad category of active attacks where the attacker deliberately modifies messages, parameters, properties etc. of information system components and tries to alter the behaviour of the system often bypassing security controls. SQL injection, masquerade and email spoofing are some of the examples of fabrication attacks.

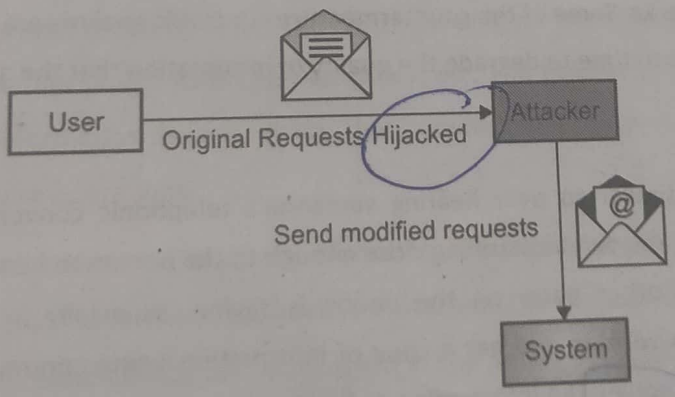

Fig. 1.7.4

- Some of the counter measures to fabrication attacks are hashing, redundancy checks, and input and output validation. You will learn about these techniques in other chapters.

1.7.2 Passive Attacks

- A passive attack is defined as,

> ***Definition :*** *An attack where the attacker does not alter the behaviour of the information system and silently performs her malicious activities.*

- Unlike active attacks, passive attacks are predominantly used to learn information such as number of systems, how the system operates and behaves under various circumstances and general operational characteristics such as the name and version of the operating system running on the targeted machines. Once the information is gathered, the attacker launches complex and more impactful attacks. Let us expand on some of the examples of passive attacks.

1. Traffic Analysis

- In traffic analysis, the network traffic and its patterns are watched out over a period of time to infer important information and guess possible activities. For example, following is some information that can be possibly guessed just by knowing the traffic volume and patterns.
  - Long communication – can denote some emergency
  - Short communications – can denote planning, checking, and negotiation
  - No communication – can indicate a lack of activity
  - Time of communication – can indicate who works when

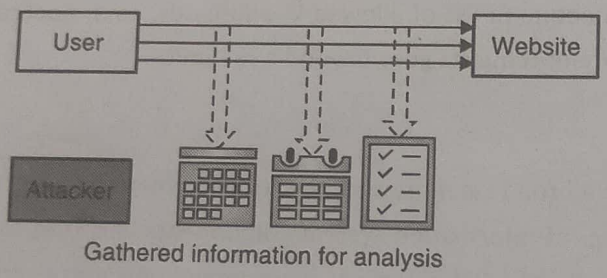

Fig. 1.7.5

- Such an information gathering exercise can give you a decent amount of information about your target to launch more sophisticated attacks. Some of the countermeasures to traffic analysis are to randomize the communication or send fake traffic time to time to degrade the quality of information that the attacker can gather for analysis.

2. Eavesdropping

- Eavesdropping is very similar to over hearing someone's telephonic conversation taking advantage of your proximity to the person. You can be standing close enough to the person to hear what she is speaking over phone or also hear what the other party on the phone is saying, especially in calm areas. Similarly, in digital communication, you can wiretap and get a copy of information being communicated and spy on it. Spying on such communication by tapping the information as it is being sent or received is called eavesdropping.

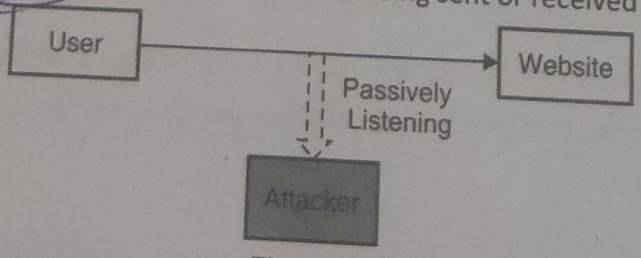

Fig. 1.7.6

- Some of the countermeasures to eavesdropping is sending noise time to time or using random channels of communication.

1.7.3 Comparison between Active and Passive Attacks

Sr. No.	Comparison Attribute	Active Attack	Passive Attack
1.	Complexity	High	Low
2.	Impact	High	Low
3.	Detection Possibility	High	Low
4.	Prevention Possibility	High	Low
5.	Duration of attack	Short	Long
6.	System Behaviour	Modified	Unaffected
7.	Original Information	Modified	Unaffected
8.	Purpose	Harm the ecosystem	Learn about the ecosystem

1.8 Security Policy

✍ ***Definition :*** *Information Security Policies or just Security Policies are aggregate of directives, regulations, rules, and practices that prescribe how an organisation manages, protects, and distributes information.*

- Policies, in general, define a broad set of rules that governs all aspects of how an organisation would operate. Like any political government, the organisation defines several policies covering the broad continuum of organisation management and operations.
- Here the term policy is used widely meaning various things depending on the context. For example, there could be authentication policy, authorisation policy, loan approval policy, etc. The policies that you are learning about in this section majorly refer to the Information Security Policy that is defined organisation wide to ensure protection for relevant business data and secure operations.
- Computer systems, data, applications and staff are crucial to the organisation's mission and objectives. Senior management needs to ensure that these all are adequately protected. The management needs to unify how these are handled, operated and protected and cannot just leave them at the personal understanding, experience and skills of various people or technology. The policies are defined at the top executive level and are pushed down to the various departments and individuals for adhering to those policies.

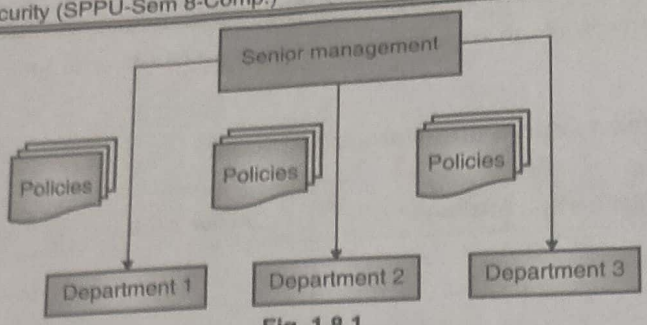

Fig. 1.8.1

1.8.1 Characteristics of Policies

Policies typically have the following characteristics.

1. They are driven by the organisation's mission and objectives.
2. They are clearly expressed and avoid ambiguity.
3. They consider all the department and the functions within the organisation.
4. They adhere to local and global laws and regulations that an organisation is subjected to.
5. They are forward and future looking and are not very frequently updated.
6. They define the roles and responsibilities for implementing them.
7. They are version controlled and protected from any unauthorised disclosure or modification.
8. They are periodically reviewed to ensure their relevance.
9. They are repeatedly communicated to all the stakeholders (employees, departments, contractors, etc.).
10. They are periodically audited and reported for compliance and non-compliance.

1.8.2 Types of Policies

SPPU - March 19(In Sem.)

Q. What are different security policies? Explain. **(March 19, 5 Marks)**

– There are majorly three types of policies.

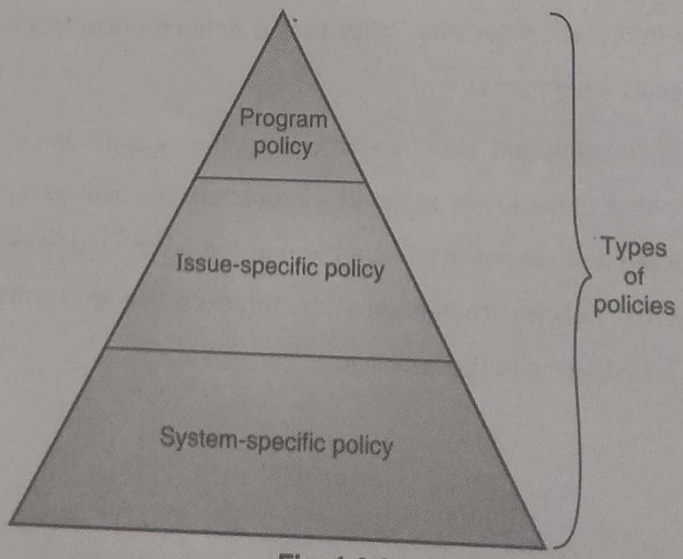

Fig. 1.8.2

- The types of policies also form a hierarchy where Program Policy is at the top and strategically defined.

1. Program policy

Definition : Program Policy is used to create the organisation's overall security program.

- This is also called as organisation policy. The program policy sets the strategic direction of the organisation and clearly defines the following components.

1. **Purpose :** The policy includes the purpose and goals of the program. It must highlight various security related requirements such as confidentiality, integrity and availability that must be met. It should define the high-level goals that must be achieved by the program. For example, if the organisation is a bank, then the integrity of data may be highlighted as the topmost goal whereas if the organisation is into e-commerce, then the availability of the e-commerce portal might be the top-most goal.
2. **Scope :** The program policy must also clearly define the scope to which it applies. The scope could be, for example, facilities, hardware, software, customer data or individuals. The policy might differ based on the scope or not everything could be within the scope of the policy. For example, the policy might apply differently to employees than contractors or suppliers. The policy should also consider various laws and regulations that the organisation must adhere to. For example, the organisation might be processing payment card data. It then should consider that how it would protect the card holder data and show compliance with the PCI DSS regulation when audited.
3. **Responsibilities :** The policy must clearly define the roles and responsibilities of various individuals or departments that would implement and enforce the policy.
4. **Compliance :** The policy must also address that how the organisation would achieve compliance (meet the policy requirements) and how it would handle non-compliance (not meeting the policy requirements). Generally, someone is assigned to oversee the implementation of policy requirements and monitor compliance. The policy also defines a provision for penalties or actions to be taken in case of non-compliance.

- Here is a sample program policy.

Sample Information Security Program

Program Objectives

- The objectives of this Information Security Program ("Program") are as follows:
  - Ensure the security and confidentiality of the Dealership's customer information.
  - Protect against any anticipated threats or hazards to the security and/or integrity of the Dealership's customer information.
  - Protect against unauthorised access to or use of the Dealership's customer information that could result in substantial harm or inconvenience to any customer.
- For purposes of the Program, "customer information" means any information about a customer of the Dealership, or information the Dealership receives about the customer of another financial institution that can be directly or indirectly attributed to the customer. This Program, in and of itself, does not create a contract between the Dealership and any person or entity.

2. Issue-specific policy

✍ ***Definition :*** *Issue-Specific Policy details out the security practices explicitly for a particular issue or function as relevant to the organisation.*

- This is also called as functional policy. The objective of defining an issue-specific policy is to go into slightly more details specific to particular issue and outline the various practices that the organisation would follow for that area. It is more detailed and requires regular revision to ensure its relevance.
- For example, the organisation can define issue-specific policies for the following areas.
  - Acceptable Use Policy for Organisation Assets
  - Access Control Policy
  - Data Retention Policy
  - Business Continuity Policy
  - Password Management Policy
  - Email Policy
  - Remote Use Policy
  - Social Media Policy
- Here is an example policy for Acceptable Use of Organisation's Assets.

Acceptable Use Policy

4.1 General Use and Ownership

4.1.1 Acme Inc's proprietary information stored on electronic and computing devices whether owned or leased by Acme Inc, the employee or a third party, remains the sole property of Acme Inc. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Acme Inc's proprietary information.

4.1.3 You may access, use or share Acme Inc's proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorised individuals within Acme Inc may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.

4.1.6 Acme Inc reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from an Acme Inc email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Acme Inc, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Acme Inc authorised to engage in any activity that is illegal under local, state, federal or international law while utilizing Acme Inc owned resources.

- Similar to Program Policy, Issue-Specific policy also has several components.

1. **Issue statement :** The issue, for which the policy is being drafted, must be clearly defined. It is also recommended to include any goals relevant to the issue for which the policy is being defined. For example, the organisation might define the issue "Use of Organisation's internet service for non-business purpose" as "To ensure the fair use of internet services within the organisation, the use of organisation's internet services is deemed to be legitimate only for the business purposes as defined in the job description of the employee".
2. **Statements of organisation's position :** The statement should define the organisation's stand against the issue. For example, it could be the following for the non-business use of internet issue. "Any use beyond the business purpose is subject to audit, questioning and disciplinary action".
3. **Applicability :** The issue-specific policy should also define the scope and circumstances in which the policy applies. For example, it could apply to all full-time and part-time employees, contractors and suppliers.
4. **Roles and responsibilities :** The policy should also define the roles and responsibilities of individuals who would implement and enforce the policy and also whom the policy applies to. For example, the responsibility of the employee could be to not browse any social media sites at work.

5. **Compliance :** The policy must also define how the compliance would be checked for the policy and what are the consequences for non-compliance. For example, the policy could state that the software installed on the employee's laptop would monitor the sites that the employee browses and the list of sites would be reported to the security team as well as the supervisor of the employee for audit purpose. If it is deemed that the non-business sites were visited, it could mean further disciplinary actions as stringent as the employee's layoff.
6. **Point of contact :** The policy may optionally include the point of contact to reach out to if any clarification for the policy is needed. The point of contact provides the consultation and discussion opportunity for the policy to ensure that the policy is clear enough to be understood and followed.

3. System-specific policy

Definition : System-Specific Policy is the most granular form of policy that provides information and direction for particular systems.

- For example, there could be a system-specific policy on which algorithms are approved for encrypting data. There could be another system-specific policy on how the systems should be patched. System-specific policy is mostly oriented and based on technology.
- However, there could be other policies that must be required to be enforced as well to achieve the overall security objectives and goals.
- Here is an example policy for encryption.

Encryption Policy

Purpose

- The purpose of this policy is to provide Acme Inc's guidance on the use of encryption to protect information resources that contain, process, or transmit confidential and firm-sensitive information. Additionally, this policy provides direction to ensure that State and Federal regulations are followed.

Scope

- This policy applies to all Acme Inc's employees and affiliates, including contractors. It addresses encryption policy and controls for confidential firm data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management. This policy should be/is compatible with but does not supersede or guarantee compliance with all State and federal encryption standards.

Policy

- Based on the data protection risk assessment described above, Acme Inc uses AES for encrypting confidential and other firm sensitive data, unless documented through the exception process as described below. Symmetric cryptosystem key lengths must be at least 80 bits for confidential data and 64 bits for other sensitive information identified by the firm. Asymmetric crypto-system keys must be of a length that yields equivalent strength, (e.g., approximate equivalencies of 64 bit symmetric = 512 bit asymmetric; 80 bit = 1024 bit; 112 bit = 2048 bit; 128 bit = 3072 bit).

- All encryption mechanisms implemented to comply with this policy support a minimum of, but not limited to AES 128-bit encryption.
- The use of proprietary encryption algorithms is not allowed for any purpose. Acme Inc's key length requirements will be reviewed annually and upgraded as technology allows.

1.8.3 Policy Implementation

- As you understand, a policy is broadly written and aligned with the organisation's mission and objectives. It may not be very specific to detail out every aspect of implementation such as commands to be executed on the system or things to be precisely checked.
- Hence, the organisation also develops standards, guidelines and procedures that help in implementing the policies. Such standards, guidelines and procedures could be documented and distributed as a manual or handbook or could be web hosted internally for quick reference.

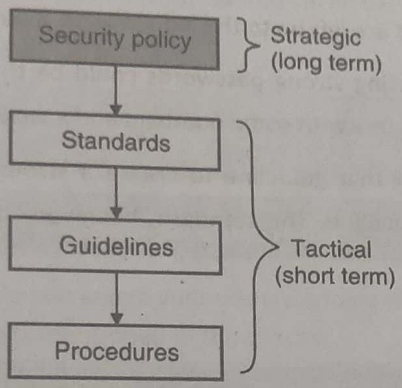

Fig. 1.8.3

1. Standards

Definition : Standard is a documented or published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the mentioned specifications.

- Do not confuse these standards with other local or global standards such as ISO, ANSI, etc.
- Standards referred here are organisation specific that unify the approach of handing technologies, hardware, software, people, parameters and procedures organisation-wide to minimise disruption or variations. Such standards are mandatory to be followed within the organisation.
- Standards define the organisation-wide requirements that would meet the policy needs. They are mechanisms that are approved to be used within the organisation.
- There could be several standards that an organisation can define. Following are a few examples of standards.
  1. Which brand of laptop and what configuration will the employees use? For example, all employees must use DELL manufactured laptop with 4 GB RAM and 100 GB hard disk running Intel Core 7 with 14-inch HD screen.

2. Which anti-virus software would be used on all the systems owned by the organisation? For example, all system must run McAfee version 7 anti-viruses and should update virus policy definition every day.
3. Which OS will the employees use and what would be its configuration? For example, all employees must use Windows 10 image hardened by the organisation and installed by the IT department.
4. How should employees form their passwords? For example, all employees must use strong passwords containing at least 1 digit, 1 uppercase letter, 1 lowercase letter, 1 special character and should be at least 14 characters long.

- The objective of defining standards is to unify the effort required for maintaining the security of various systems. Imagine if it was free for any employee to choose whatever hardware or software they use within the organisation. How could organisation ensure that all such varied systems are secure?

2. Guidelines

✍ *Definition : Guidelines are general recommendations that may be optionally followed to achieve a requirement enforced by a standard or a policy.*

- Guidelines are not mandatory and are left up to the individual to follow it or not. It is just a useful piece of advice.
- For example, a guideline for creating strong passwords could be that "Take the first letter of every word in a sentence and replace a few characters with some numbers and special characters."
- The user may not actually follow that guideline to create a strong password and a strong password can be created without following the guideline. The standard, however, for strong passwords must be enforced and followed.

3. Procedures

✍ *Definition : Procedures are detailed step-by-step tasks that should be performed to meet certain objective, task or goal.*

- The users can follow the step-by-step method and carry out the desired task. Procedures detail the actual steps that could be carried out on the systems to complete a task or meet the objective.
- For example, here is a sample procedure for adding a new employee in the organisation's database.
  1. Get details of the new employee in the enrolment form version 2.1 from the HR department.
  2. Verify that all the details mentioned in the enrolment form match the submitted documents.
  3. Log on to the active directory as administrator and fill the details present in the enrolment form.
  4. Send the details to a colleague for review.
  5. Notify the employee's supervisor and the HR department once the employee addition is successful.
  6. Send out the details on the employee's email and send the steps to change the pre-set password.
- Procedures are the lowest level of documentation in the organisation and are the closest to the actual systems and users. Because of such a strong tie up between the procedures and systems, procedures might require frequent changes based on the system and the requirements as they evolve.

4. Baselines

✍ *Definition : Baseline is the accepted set of controls that are considered to be effective enough to meet the policy requirements.*

- Baseline is taken as the reference point beyond which the systems are considered adequately protected. For example, hardening the system against an industry-accepted security benchmark could be considered to meet the baseline for system's security.

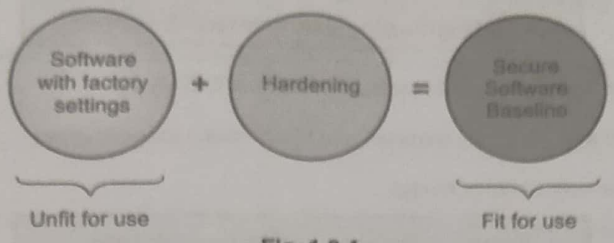

Fig. 1.8.4

- Software with the factory default settings may not be best configured for providing adequate security. The hardening process ensures that the software is configured to meet the security baseline beyond which the software can be securely used. Baseline is the minimum level of protection that is considered effective and adequate. Anything above the baseline mark is considered "even better".

Difference between Security and Privacy

Note: Please refer this topic in chapter 6. It is rightly placed in that chapter along with the other privacy related topics for your easy and comprehensive understanding.

Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

Elements of Information Security

Q. 1 Explain the terms Assets, Controls, Threats, Vulnerabilities, Risk and Exposure with examples. **[8 Marks]**

Q. 2 Draw a block diagram depicting the relation between Assets, Controls, Threats, Vulnerabilities, Risk and Exposure. **[6 Marks]**

Q. 3 With many security controls, you can reduce the risk to zero. Comment. **[4 Marks]**

Q. 4 Describe the three pillars of security with examples. **[8 Marks]**

Q. 5 Describe the three goals of security with examples. **[8 Marks]**

Q. 6 Write a short note on confidentiality. **[4 Marks]**

Q. 7 Write a short note on integrity. **[4 Marks]**

Q. 8 Write a short note on availability. **[4 Marks]**

Q. 9 Explain the terms Identification, Authentication, Authorisation, Accountability and Non-repudiation with example. **[8 Marks]**

Q. 10 Draw a block diagram depicting the relation between Identification, Authentication, Authorisation and Accountability. **[6 Marks]**

Basic Terminologies in Network Security

Q. 11 Draw a chart for various Security Services provided at various OSI layers. **[6 Marks]**

Q. 12 What is OSI Model? List a few Security Services and Mechanisms for each layer. **[8 Marks]**

Q. 13 Write a short note on Network Security Model. **[6 Marks]**

Security Threats and Vulnerabilities

Q. 14 Describe any three security threats of your choice. **[6 Marks]**

Q. 15 Take any five security threats of your choice and compare them. **[6 Marks]**

Q. 16 Write a short note on script kiddies. **[4 Marks]**

Q. 17 Explain any three security vulnerabilities of your choice. **[6 Marks]**

Q. 18 What is the vulnerability from unpatched software? **[4 Marks]**

Security Attacks

Q. 19 Classify security attacks and briefly explains each attack. **[8 Marks]**

Q. 20 Describe Replay Attack with a block diagram. **[8 Marks]**

Q. 21 Describe Denial of Service (DoS) Attack with a block diagram. **[8 Marks]**

Q. 22 Describe Fabrication Attack with a block diagram. **[4 Marks]**

Q. 23 Write a short note on traffic analysis. **[6 Marks]**

Q. 24 Write a short note on eavesdropping. **[6 Marks]**

Q. 25 Compare Active and Passive attacks. **[8 Marks]**

Security Policy

Q. 26 List the various characteristics of Policies. **[6 Marks]**

Q. 27 What is a program policy? Describe its structural components. **[6 Marks]**

Q. 28 What is an issue-specific policy? Describe its structural components. **[6 Marks]**

Q. 29 Write a short note on System-Specific Policy. **[4 Marks]**

Q. 30 Explain the terms Standards, Guidelines, Procedures and Baselines with suitable examples. **[8 Marks]**

Q. 31 Joe comes to John for some help. John says that he is busy in defining security baseline and requests him to come later on. What could be the purpose behind John's work? How does it help the organization ? **[4 Marks]**

❑❑❑