□□□

CHAPTER 1

Unit I

Information Security Overview

Introduction

Q. 1 Explain the term Security and hence explain Information Security. (Ref. Introduction) (5 Marks)

What is security?

In general, security is "the quality or state of being secure" which simply means "to be free from danger". In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. A successful organization should have the following multiple layers of security in place to protect its operations :

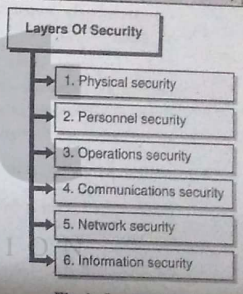

Fig. 1 : Layers of security

1. Physical security

To protect physical items, objects, or areas from unauthorized access and misuse.

2. Personnel security

To protect the individual or group of individuals who are authorized to access the organization and its operations.

3. Operations security

To protect the details of a particular operation or series of activities.

4. Communications security

To protect communications media, technology and content.

5. Network security

To protect networking components, connections and contents.

6. Information security

To protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness and technology.

Information security concepts

- Information security is simply the process of keeping information secure. Information is a valuable asset since the dawn of mankind.
- As access to computer stored data has increased, Information Security has become correspondingly important. In the past, most corporate assets were "hard" or physical.
- Today far more assets are computer-stored information such as customer lists, proprietary formulas, marketing and sales information and financial data. Some financial assets only exist as bits stored in various computers. Many businesses are solely based on information – the data IS the business.

Information security : A process

- Effective Information Security incorporates security products, technologies, policies and procedures.
- No collection of products alone can solve every Information Security issue faced by an organization. More than just a set of technologies and reliance on proven industry practices is required, although both are important.
- Products, such as firewalls, intrusion detection systems and vulnerability scanners alone are not sufficient to provide effective Information Security.
- Thus, Information Security is a process. An information systems' Security Policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure.
- Security Procedures document precisely how to accomplish a specific task. For example, a Policy may specify that antivirus software is updated on a daily basis and a Procedure will state exactly how this is to be done – a list of steps.

Security is everyone's responsibility

- Although some individuals may have "Security" in their title or may deal directly with security on a daily basis, security is everyone's responsibility.
- A chain is only as strong as its weakest link. A workplace may have an excellent security, but if a help desk worker readily gives out or resets lost passwords, or employees let others tailgate on their opening secure doors with their key card, security can be horribly compromised.
- Despite the robustness of a firewall, if a single user has hardware (e.g. a modem) or software (e.g. some file sharing software) that allows bypassing the firewall, a hacker may gain access with catastrophic results. There are examples where a single firewall misconfiguration of only a few minutes allowed a hacker to gain entrance with disastrous results.
- End user awareness is critical, as hackers often directly target them. Users should be familiar with Security Policies and should know where the most recent copies can be obtained. Users must know what is expected and required of them.
- Typically, this information should be imparted to users initially as part of the new hire process and refreshed as needed.

Information security involves a trade off between security and usability

- There is no such thing as a totally secure system – except perhaps one that is entirely unusable by anyone! Corporate Information Security's goal is to provide an appropriate level of security, based on the value of an organization's information and its business needs.
- The more secure a system is the more inconvenience legitimate users experience in accessing it.

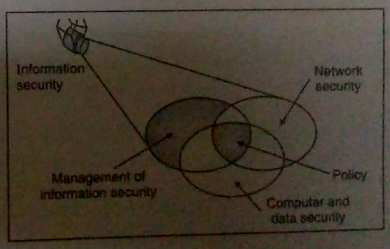

Fig. 2 : Component of Information Security

Syllabus Topic : The Importance of Information Protection

1.1 Information Security Overview

1.1.1 The Importance of Information Protection

Q. 1.1.1 Write short note on importance of information protection. (Ref. Sec. 1.1.1) **(5 Marks)**

- Information is an important asset. The more information you have at your command, the better you can adapt to the world around you. In business, information is often one of the most important assets a company possesses.
- Information differentiates companies and provides leverage that helps one company become more successful than another.
- Information can be classified into different categories. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity and its vulnerability to theft or misuse.
- Organizations typically choose to deploy more resources to control information that has higher sensitivity.
- The U.S. government, for example, uses a five-level classification system that progresses from unclassified information (which everyone can see) to Top Secret information (to which only the most trusted people have access).
- Organizations classify information in different ways in order to differently manage aspects of its handling, such as labelling (whether headers, footers and watermarks specify how it should be handled), distribution (who gets to see it), duplication (how copies are made and handled), release (how it is provided to outsiders), storage (where it is kept),encryption (if required), disposal (whether it is shredded or strongly wiped) and methods of transmission (such as e-mail, fax, print and mail).
- The specifics are spelled out in an organization's information classification and handling policy, which represents a very important component of an organization's overall security policy.
- Companies may have confidential information, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts and earnings announcements, that is intended for internal use on a need-to-know basis.
- Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a Non Disclosure Agreement (NDA) or equivalent obligation of confidentiality.
- Information intended for internal use only is usually meant to be seen by employees, contractors and service providers, but not by the general public.
- Examples include internal memos, correspondence, general e-mail and instant message discussions, company announcements, meeting requests and general presentation materials. This type of information is typically the least restricted because spending a lot of time and money on protecting it doesn't outweigh the value of the information or the risk of its disclosure.

Syllabus Topic : The Evolution of Information Security

1.1.2 The Evolution of Information Security

Q. 1.1.2 Write short note on Evolution of Information Security. (Ref. Sec. 1.1.2) **(5 Marks)**

- Individual computers were connected together in the early days of networking, only in academic and government environments. Thus, during that period of time, the networking technologies that were developed were specific to academic and government environments.
- Originally, the academic security model was "wide open" and the government security model was "closed and locked." The governments across the globe are mainly concerned with blocking access to computers, restricting internal access to confidential data and preventing interception of data.
- (For example, by shielding equipment to prevent electromagnetic radiation from being intercepted). This method of protecting assets provided a hard-to-penetrate perimeter.

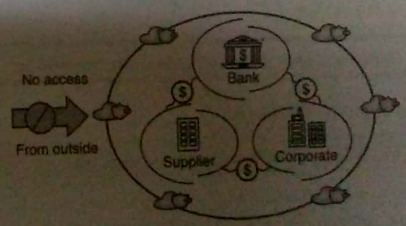

Fig. 1.1.1 : Protected Internal Resources

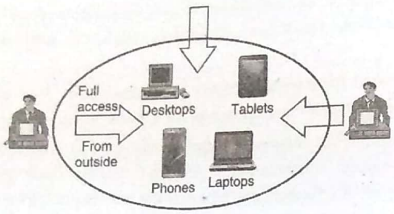

Fig. 1.1.2 : Open access model (unprotected internal resources)

- The two models are diametrically opposite and the government model blocks everything, while the academic model allows everything. There is plenty of room in between these two extremes. So, the practice of network security evolved.
- The concepts of intranets and extranets were developed to accommodate internal and external customers, respectively, with secured boundaries that resembled miniature versions of the firewall perimeter.
- Virtual Private Networks (VPNs) were developed to provide a secure channel (or tunnel) from one network to another. These approaches continued through the end of the 1990s to the early part of the 2000s.
- Modern security products are now designed to balance the needs of business on the Internet while protecting against today's sophisticated threats.
- Modern information security practices have evolved into a blended approach to managing access to information.
- Technology and information are blended into everyday life and they can no longer be kept in a locked box or left unprotected.

Syllabus Topic : Justifying Security Investment

1.1.3 Justifying Security Investment

Q. 1.1.3 What is security benefit? Explain with its benefits. (Ref. Sec. 1.1.3) **(5 Marks)**

- Every organization invests a lot of money on security aspect. This spending must be justified. That is perhaps the most challenging and debated topic in the field of information security.

- Initially there was FUD (Fear, Uncertainty and Doubt) amongst the people. Executives of companies were frightened to spend money in security as there was no prominent outcome visible.
- Return On Investment (ROI) was another concept that was used as an attempt to market security as an investment that "pays for itself". This was the standard approach to justifying information technology budgets, but it never translated well to security.
- There is really no good way to demonstrate a monetary mount gained by spending money on security. So, ROI was combined with Annualized Loss Expectancy (ALE), a risk measurement strategy that combines the frequency (or probability) of a loss with the cost of that loss, to produce a yearly expected monetary value.
- The "insurance analogy" was developed as an alternative to value-based security justifications. People and businesses spend money on insurance even though they may never have a claim to file.
- Likewise, businesses spend money on security because it's insurance against theft but it's hard to quantify.
- The business benefits of security are hard to express in terms of a simple monetary value. Good security practices allow the business to prosper. They help provide a solid foundation upon which the business can expand and grow.
- Robust information security practices not only reduce risks and costs, but also provide new opportunities for revenue. In the past, security was thought of only in the context of protection (blocking access, closing holes, segmenting and separating systems and networks and denying connections).
- Today that view has evolved to focus on enabling business on a global scale, using new methods of communication.
- Modern security practices provide information to those who need it without exposing it to those who should not have it. Good security practices allow companies to perform their operations in a more integrated manner, especially with their customers.
- By carefully controlling the level of access provided to each individual customer, a company can expand its customer base and the level of service it can provide to each individual customer, without compromising the safety and integrity of its business interests, its reputation and its customers' assets.
- Businesses thus land upto some basic benefits that they get out of all these measures that are applied. Some benefits of a strong security program are business agility, cost reduction and portability.

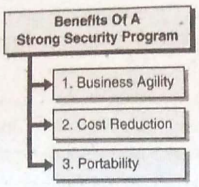

Fig. 1.1.3 : Benefits of a strong security program

➜ **1. Business agility**

- Every company in current scenario wants to open up its business operations to its customers, suppliers and business partners, in order to reach more people and facilitate the expansion of revenue opportunities.
- In business or in any aspects of life, knowledge is power. The higher knowledge improves business strategies. With high knowledge security of data is also an important aspect.
- Strong security provides insight into what is happening on the network and consequently in the enterprise.
- Weak security leaves many companies blind to the daily flow of information to and from their infrastructure. If a company's competitors have better control of their information, they have an advantage.
- Security allows information to be used more effectively in advancing the goals of organization because that organization can safely allow more outside groups of people to utilize the information when it is secure.
- The more access provided, the more people can be reached and that means a lot can be achieved from small effort. Automation of business processes, made **trustworthy** by appropriate security techniques, allows companies to focus on their core business.

➜ **2. Cost reduction**

- Modern security practices do reduce some costs, such as those resulting from loss of data or equipment. Data loss due to mishandling, misuse, or mistakes can be expensive.
- A ramp antivirus outbreak, a web site outage, or a Denial of Service (DoS) attack can result in service outages during which customers cannot make purchases and the company cannot trans act business.

- The consequences of a security compromise can be significant. A publicized security incident can severely damage the credibility of a company and thus its ability to acquire and retain customers.
- An increasing number of attacks are categorized as Advanced Persistent Threats (APTs).These attacks are designed to deploy malware into a network and remain undetected until triggered for some malicious purpose.
- Often, the goal of the attacks is theft of financial information or intellectual property. Loss of service or leakage of sensitive data can result in fines, increased fees and an overall decrease in corporate reputation and stock price.
- Strong security reduces loss of information and increases service availability and confidentiality.

➜ **3. Portability**

- Portability simply means that software and data can be used on multiple platforms or can be transferred within an organization, to a customer, or to a business partner.
- The consumption of information by the consumer has placed demands on companies to be able to provide meaningful and accurate information at a moment's notice.
- To meet the demands of today's businesses and consumers, architectures and networks need to be designed with security controls incorporated in as part of the development process.
- With sound security built in from the ground up, portability of data as a key benefit can be realized. Portability also enables business and creates value. For example, Apple's ability to both host music and allow personal music libraries to be synchronized to a tablet, mobile phone and MP3 player has greatly increased Apple's bottom line.
- Security for mobile platforms affords users the opportunity to take their music everywhere while protecting the interests of the business by preventing unauthorized downloading of copyrighted material.

Syllabus Topic : Security Methodology

1.1.4 Security Methodology

Q. 1.1.4 What are the basic aspects of security ? OR Explain security methodology. (Ref. Sec. 1.1.4) (5 Marks)

- Security is a paradigm, a philosophy and a way of thinking. A defender who overlooks vulnerability, risks the exploitation of that vulnerability.

- The best approach to security is to consider every asset in the context of its associated risk and its value and also to consider the relationships among all assets and risks.
- The field of **security** is concerned with protecting assets in general. **Information security** is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication. At its core, the practice of security is all about reducing risks to assets to acceptable levels by using a layered, comprehensive approach so that risk is still mitigated and controlled even when one control fails.
- The field of information security evolves constantly, but the foundations of good security practice have not changed throughout history.
- If there is intent to succeed in protecting one's own assets, then a significant consideration must be given to the lessons learned from successful security strategies, as well as those learned from poor ones. Three aspects of security can be applied to any situation which is considered as three D's of security which are Defense, Detection and Deterrence.
- **Defense** is often the first part of security that comes to mind. The desire to protect ourselves is instinctive and defense usually precedes any other protective efforts.
- Defensive measures reduce the likelihood of a successful compromise of valuable assets, thereby lowering risk and potentially saving the expense of incidents that otherwise might not be avoided. Conversely, the lack of defensive measures leaves valuable assets exposed inviting higher costs due to damage and loss.
- Defensive controls on the network can include access control devices such as **stateful firewalls, network access control,** spam and malware filtering, **web content filtering** and change control processes.
- These controls provide protection from software vulnerabilities, bugs, attack scripts, ethical and policy violations, accidental data damage and other such vulnerabilities. However, defense is only one part of a complete security strategy.
- Another aspect of security is **detection.** In order to react to a security incident, knowledge about it is important. Examples of detective controls include video surveillance cameras in local stores (or even on your house), motion sensors and house or car alarm systems that alert passers-by of an attempted violation of a security perimeter.
- Detective controls on the network include audit trails and log files, system and network intrusion detection and prevention systems and Security Information and Event Management (SIEM) alerts, reports and dashboards.

- A Security Operations Center (SOC) can be used to monitor these controls. Without adequate detection, a security breach may go unnoticed for hours, days, or even forever.
- **Deterrence** is another aspect of security. It is considered to be an effective method of reducing the frequency of security compromises and thereby the total loss due to security incidents.
- Many companies implement deterrent controls for their own employees, using threats of discipline and termination for violations of policy.
- These deterrent controls include communication programs to employees about acceptable usage and security policies, monitoring of web browsing behaviour, training programs to acquaint employees with acceptable usage of company computer systems and employee signatures on agreements indicating that they understand and will comply with security policies. With the use of deterrent controls such as these, attackers may decide not to cause damage.

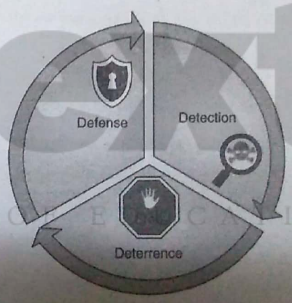

Fig. 1.1.4 : The Three Ds of security

- When only one or two of these aspects of security are applied to the network, it mainly results in exposures. Implementing defense and detection without deterrence will be vulnerable to internal attacks, such as misuse and accidents caused by employees who are not motivated to follow the correct procedures.
- A network that fails to employ detection faces exposure to all failures of the defensive and deterrent controls and management may never become aware of these failures, which means abuses may continue unchecked. Employing no defensive controls on a network exposes that network to any of the well-known threats of internal or external origin.

Syllabus Topic : How to Build a Security Program ?

1.1.5 How to Build a Security Program ?

Q. 1.1.5 What are the basic components required to build a security program and hence explain any three ? (Ref. Sec. 1.1.5) **(5 Marks)**

The overall approach to building a security program, should begin with describing what is needed and why and to proceed to define how it will be implemented along with when and using which particular methods. There are many components that go into the building of a security program :

- **Authority :** The security program must include the right level of responsibility and authorization to be effective.
- **Framework :** A security framework provides a defensible approach to building the program.
- **Assessment :** Assessing what needs to be protected, why and how leads to a strategy for improving the security posture.
- **Planning :** Planning produces priorities and timelines for security initiatives.
- **Action :** The actions of the security team produce the desired results based on the plans.
- **Maintenance :** The end stage of the parts of the security program that have reached maturity is to maintain them.

Authority

- A **security program charter** defines the purpose, scope and responsibilities of the security organization and gives formal authority for the program.
- Usually, the security organization is responsible for information protection, risk management, monitoring and response.

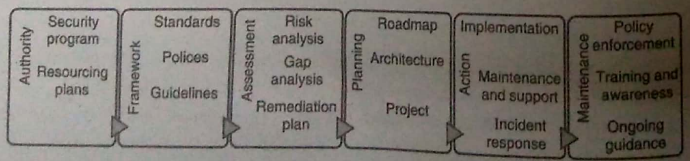

Fig. 1.1.5 : Security program components

- It might also be responsible for enforcement, such as reprimanding or even terminating employees or contract workers, but more commonly that authority is vested in the Human Resources department.
- Other responsibilities may include physical security, disaster-recovery and business-continuity planning, regulatory and internal compliance and auditing.

Framework

- The **security policy** provides a framework for the security effort. The policy describes what must be done to comply with the business requirements.
- **Policy** includes all aspects of technical implementations, as well as policies and procedures. Ideally, a security policy should be documented and published before any implementations begin.
- **Standards** are the appropriate place for product-specific configurations to be detailed. Standards are documented to provide continuity and consistency in the implementation and management of network resources.
- Standards change with each version of software and hardware, as features are added and functionality changes and they are different for each manufacturer. Because standards do change, they require periodic revision to reflect changes in the software and hardware to which they apply.
- **Guidelines helps users to handle the product efficiently.** Guidelines to use a software, computer systems and networks should be clearly documented for the sake of the people who use these technologies.
- Guidelines are driven to some extent by the technology, with details of how to apply the tools. They are also driven by the security policy, as they describe how to comply with the security policy.

Assessment

- A **risk analysis** provides a perspective on current risks to the organization's assets. This analysis is used to prioritize work efforts and budget allocation, so that the greater risks can receive a greater share of attention and resources.
- A risk analysis results in a well-defined set of risks that the organization is concerned about. These risks can be mitigated, transferred or accepted.
- A **gap analysis** compares the desired state of the security program with the actual current state and identifies the differences. Those differences, or gaps, form a collection of objectives to be acted on over the course of a remediation effort to improve the

organization's security posture to bring it in line with one or more standards, requirements, or strategies.

- **Remediation planning** takes into account the risks, gaps and other objectives of the security program and puts them together into a prioritized set of steps to move the security program from where it is today to where it needs to be at a future point.

Planning

- A **roadmap** is a plan of action for how to implement the security remediation plans. It describes when, where and what is planned.
- The roadmap is useful for managers who need the information to plan activities and to target specific implementation dates and the order of actions. It is also useful for implementers who will be responsible for putting everything together.
- The roadmap is a relatively high-level document that contains information about major activities and milestones coming up in the next defined period of time.
- The **security architecture** documents how security technologies are implemented, at a relatively high level. It is driven by the security policy and identifies what goes where. It does not include product specifications or specific configuration details, but it identifies how everything fits together.
- A good tool for architecture documents is a block diagram. A block diagram shows the various components of a security architecture at a relatively highlevel, which shows how the components work together.
- A block diagram does not show individual network devices, machines and peripherals, but it does show the primary building blocks of the architecture.
- Block diagrams describe how various components interact, but they don't necessarily specify who made those components, where to buy them, what commands to type in and so on.
- The **project plans** detail the activities of the individual contributors to the various security implementations. A good project plan starts with an analysis phase, where all of the affected parties discuss and review the requirements, scope and policy.
- This is followed by a design phase, in which the architecture is developed in detail and the implementation is tested in a lab environment. After the design has been made robust, an initial test is performed to expose bugs and problems.
- The next phase which is an implementation phase is mostly modular based. The main task is broken into small collections of tasks whenever possible.

- Each task is implemented separately either by different teams or one by one. Testing follows implementation, after which the design is revised to accommodate changes discovered during testing. Upon completion, the implementation team should meet to discuss the hits and misses of the overall project in order to prepare for the next phase.

Action

- **Procedures** describe how processes are performed by people on an ongoing basis to produce the desired outcomes of the security program in a repeatable, reliable fashion.
- Maintenance and support are part of maintaining the ongoing operations of the security program and its associated technologies, as part of a normal lifecycle of planning, updating, reviewing and improving.
- The actions that should be taken when a security event occurs are defined in the **incident response plan.**
- Advance planning for what to do when security incidents occur helps shorten the response time and provides repeatable, reliable and effective actions to limit the scope and damage of an incident.

Maintenance

- **Policy enforcement** is necessary to ensure that the intentions of management are carried out by the various people responsible for the behaviour and actions defined in the security policies. Often, this enforcement is a shared effort between security management, company management and Human Resources.
- **Security awareness programs** are used to educate employees, business partners and other stakeholders about what behaviours are expected of them, what actions they should take under various circumstances to comply with security policies and what consequences may ensue if they don't follow the rules.
- As an educational tool, an awareness program can also be great resources for helping people understand why they should want to follow the rules and how security benefits them. Motivation can be an effective approach.
- **Ongoing guidance** for business projects, daily operations and general walk-up questions is an important part of a security program.
- After all, business situations change every day and security should be considered in every situation. Someone should be available to advise the business on the best way to do things in a secure manner.

Syllabus Topic : The Impossible Job

1.1.6 The Impossible Job

Q. 1.1.6 Write short note on the impossible job. (Ref. Sec. 1.1.6) **(5 Marks)**

- A universal truth of security, regardless of the application, is that the job of the attacker is always easier than the job of the defender.
- The attacker needs only to find one weakness while the defender must try to cover all possible vulnerabilities.
- The attacker has no rules the attacker can follow unusual paths, abuse the trust of the system, or resort to destructive practices. The defender must try to keep their assets intact, minimize damage and keep costs down.

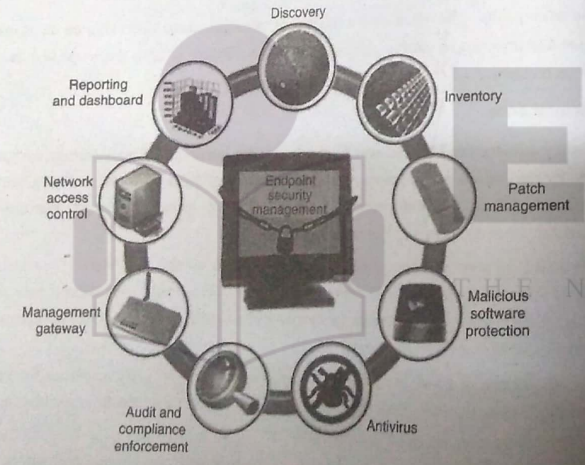

Fig. 1.1.6 : Secure system reduce chances of attack

- In fact, the defender has an impossible job if the goal is to have 100 percent protection against all conceivable attacks. That is why the primary goal of security cannot be to eliminate all threats.
- Management may need to be educated about this concept, because they may not realize that this is a tenet of the security profession.
- Every defender performs a risk assessment by choosing which threats to defend against, which to insure against and which to ignore. **Mitigation** is the process of defense, **transference** is the process of insurance and acceptance is deciding that the risk does not require any action.

Syllabus Topic : The Weakest Link

1.1.7 The Weakest Link

Q. 1.1.7 What are weakest links in security measures ? (Ref. Sec. 1.1.7) **(5 Marks)**

- A security infrastructure will drive an attacker to the weakest link. Usually an attacker goes from the easiest to the hardest level of security breach.
- The weakest link will attract the greatest number of attacks. Fig. 1.1.7 demonstrates this concept. All security controls should complement each other and each should be equally as strong as the others. This principle is called **equivalent security or transitive security.**

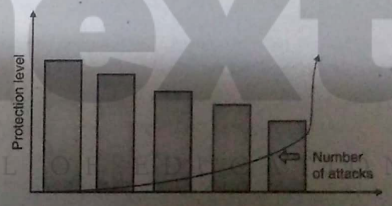

Fig. 1.1.7 : Attack vector focus on weakest link

- When deciding which security project should be of next priority, choose to shore up the weak points first.
- Because threats come from many sources and tend to focus on the weakest link, protecting a particular asset requires securing the asset as well as securing other resources that have access to that asset.
- For instance, consider the asset as a credit card which must be kept safe along with other resources responsible to make the card function properly such as network, database, etc.

- These resources may include nontechnical resources as well, so focusing only on electronic data can overlook important threat vectors.
- Securing the data means discovering its path throughout the system and protecting it at every point. Equivalent or transitive security controls on all the places where that asset may be attacked make the attacker's job harder by protecting against weak points the attacker can exploit.
- In a computer network, firewalls are often the strongest point of defense. They encounter their fair share of attacks, but most attackers know that properly configured firewalls are difficult to penetrate, so they will look for easier prey.
- This can take the form of DSL (Digital Subscribers Line) in labs or small offices that aren't firewalled, modems and other remote access systems, Private Branch Exchange (PBX), phone switches, etc.
- For any device that is to be protected, more attacks will occur via less protected paths and those attacks will typically be more often successful. These attacks may exploit vulnerabilities in Internet-facing systems, compromised internal systems, administrative channels, unsecured paths, or even trusted credentials.
- The most successful of those attacks will be the ones that take advantage of the weakest security.
- One objective of an effective security strategy is to force the attacker to spend so much time trying to get past the defenses that the attacker will simply give up and go elsewhere.
- Other strategies attempt to delay the intruder for a long enough time to take a reactive response, such as summoning authorities. Still others try to lure the attacker into spending too much time on a dead end.
- In any case, weak points in the security infrastructure should be avoided whenever possible.
- In situations where weak points are necessary due to business requirements, detective and deterrent security controls should focus on the areas where defensive weak-points exist. You can expect these weak points to attract attackers and you should plan accordingly.

Syllabus Topic : Strategy and Tactics

1.1.8 Strategy and Tactics

Q. 1.1.8 What are strategy and tactics ? (Ref. Sec. 1.1.8) **(5 Marks)**

- A **security strategy** is the definition of all the architecture and policy components that makeup a complete plan for defense, detection and deterrence.
- Security **tactics** are the day-to-day practices of the individuals and technologies assigned to the protection of assets.
- It can also be said that strategies are usually proactive and tactics are often reactive. Both are equally important and a successful security program needs to be both strategic and tactical in nature.
- Often there is an immediate need to secure a part of the network infrastructure and time is not on the side of the strategic planner. In these cases, a tactical solution can be put in place temporarily to allow appropriate time for planning a longer-term solution.
- If a company finds itself focusing only on strategy or only on tactics, it should review its priorities and consider adding additional staff to address the shortfall. Fig.1.1.8 demonstrates the interplay of strategy and tactics.
- Initially, at a given starting point in time, tactical effort may be high where strategy has not previously been employed. As time progresses and strategic planning is employed, tactical operations should begin to require less effort, because the strategy should simplify the operation and the business processes.
- Given enough time, strategic planning should encompass tactics, confining them to the point where most daily tactical operations take place in a well-planned strategic context and only unexpected fluctuations cause reactive efforts.

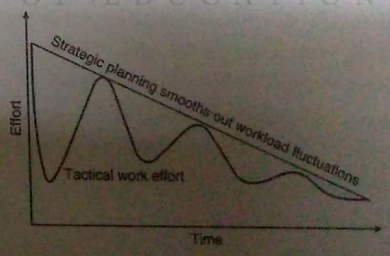

Fig. 1.1.8 : Strategy reduces tactical work effort over time

- In the ideal situation, strategy and tactics are at equilibrium. The strategic focus paves the way for quarter-to-quarter activities and the tactical operations follow the strategy set forth in the previous quarters.

- In this balanced system of planning and action, a framework has been set in advance by the strategists for the operational staff to follow, which greatly facilitates the jobs of the operational staff who must react to both expected and unplanned situations.

Syllabus Topic : Business Processes vs. Technical Controls

1.1.9 Business Processes vs. Technical Controls

Q. 1.1.9 Describe business process and technical control. (Ref. Sec. 1.1.9) **(5 Marks)**

- In security, there is no magic wand i.e. there is no single security device, product, or technology that provides complete protection against all threats.
- Some security products are marketed as "security-in-a-box" solutions that provide all the security a company needs.
- In reality, security threats and exposures are complex and constantly evolving.
- Security technologies need to be selected on the basis of business context, so they are targeted toward specifically identified risks with clear objectives.
- Organizations that place technical controls on their network without accompanying business processes have not recognized that computers are tools for accomplishing specific objectives and that tool should be considered within a business process in order to be effective.
- For example, just buying a firewall doesn't magically provide security and if technical controls get in the way of the business or slow down workflow, people will find ways to work around them, rendering them ineffective or useless.
- In the context of network security, business objectives, priorities and processes determine the choice of tools and the tools are used to facilitate the business processes.
- Fig. 1.1.9 illustrates this principle.
- Any security implementation is a snapshot that includes the current threat model, the protection requirements, the environment being protected and the state of the defensive technology at the time. As technology and the business environment evolve over time, the technical controls that are part of this snapshot will become less and less appropriate.

- Before selecting security products, the business processes must be identified so that security products can be chosen that fit appropriately into the business environment.
- The security practitioner must attempt to understand the underlying business processes and data flows in order to solve the security challenge.

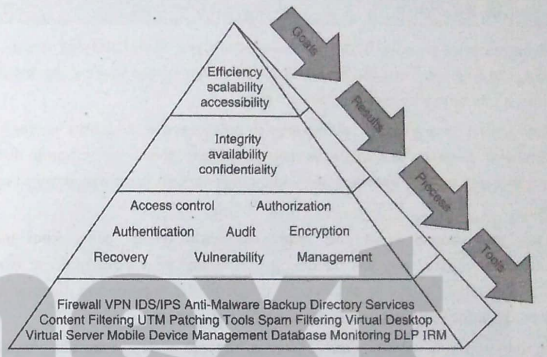

Fig. 1.1.9 : Business objectives, priorities and processes drive tool selection

1.2 Introduction to Risk

- The objective of a security program is to mitigate risks. Mitigating risks does not mean eliminating them; it means reducing them to an acceptable level.
- To make sure that the security controls are effectively controlling the risks in the environment, there is a need to anticipate what kinds of incidents may occur. There is also a need to identify what is to be protected and from whom. That's where risk analysis, threat definition and vulnerability analysis come into picture of security.
- Spending more money on security than on an asset rarely makes sense but at the same time, spending nothing at all to secure an asset makes no sense either.
- The goal is to find the optimal balance between the business risks associated with technologies and processes and the cost of security controls that address those risks.

Syllabus Topic : Threat Definition

1.2.1 Threat Definition

Q. 1.2.1 Define threat and hence explain threat vectors and threat source and target. (Ref. Sec. 1.2.1) **(5 Marks)**

- Evaluating threats is an important part of risk analysis. By identifying threats, security strategy can be given focus and thus reduces the chance of overlooking important areas of risk that might otherwise remain unprotected.
- Threats can take many forms and in order to be successful, a security strategy must be comprehensive enough to manage the most significant threats. Many people that haven't seen real-world security breaches don't know this so they focus exclusively on external threats.
- Security professionals know that many real-world threats come from inside the organization, which is why just building a wall around your trusted interior is not good enough. Regardless of the breakdown for the particular organization, there is a need to make sure that the security controls focus on the right threats.
- To avoid overlooking important threat sources, all types of threats must be considered and valued. This consideration should take into account the following aspects of threats :
  - Threat vectors
  - Threat sources and targets

1.2.1.1 Threat Vectors

Q. 1.2.2 Explain computer virus, worms and Trojan. (Ref. Sec. 1.2.1.1) **(5 Marks)**

- A **threat vector** is a term used to describe where a threat originates and the path it takes to reach a target.
- An example of a threat vector is an e-mail message sent from outside the organization to an inside employee, containing an irresistible subject line along with an executable attachment that happens to be a Trojan program, which will compromise the recipient's computer if opened.
- A good way to identify potential threat vectors is to create a table containing a list of threats you are concerned about, along with sources and targets.

- Choosing different combinations of sources, threats and targets produces interesting varieties of threat vectors, which helps with the process of brainstorming and enumeration.
- Many different analyses of threat vectors are routinely published. One reputable source for conducting and publishing the results of this type of survey is the Computer Security Institute (CSI), which identifies particular threat vectors and their frequency.
- It is important to understand threat vectors and consider them when designing security controls, to ensure that possible routes of attack for the various threats receive appropriate scrutiny.
- Understanding threat vectors is also important for explaining to others, such as management, how the protective mechanisms work and why they are important.
- Insider threat vectors take many forms. For example, Trojan programs and viruses compromise computers on the trusted internal network. Trojan programs are covertly installed pieces of software that perform functions with the privileges of authorized users, but unknown to those users.
- Common functions of Trojans include stealing data and passwords, providing remote access and/or monitoring to someone outside the trusted network, or performing specific functions such as spamming.
- When Trojans are installed on a trusted system, they run with the same credentials and privileges as the user whose account they exploit, so they constitute a form of insider threat.
- Viruses typically arrive in documents, executable files and e-mail. They may include Trojan components that allow direct outside access, or they may automatically send private information, such as IP addresses, personal information and system configurations, to a receiver on the Internet.
- These viruses usually capture and send password keystrokes as well. The insider threat is serious and needs to be taken into account in any security strategy. Building a perimeter defense around the organization's network is not enough.
- A risk analysis that includes consideration of all major threat vectors helps ensure that the security controls will be effective against the real risks to the organization.

1.2.1.2 Threat Sources and Targets

- A security practitioner needs to understand how attacks work so se to select the best counter measures for defense.

- The goal is to equip with the knowledge, principles and perspective needed to implement the right countermeasures for the environment.

Security controls can be logically grouped into several categories :

- **Preventative :** Block security threats before they can exploit vulnerability.
- **Detective :** Discover and provide notification of attacks or misuse when they happen.
- **Deterrent :** Discourage outsider attacks and insider policy violations.
- **Corrective :** Restore the integrity of data or another asset.
- **Recovery :** Restore the availability of a service.
- **Compensative :** In a layered security strategy, provide protection even when another control fails. Each category of security control may have a variety of implementations to protect against different threat vectors.
- **Physical :** Control that are physically present in the "real world".
- **Administrative :** Controls defined and enforced by management.
- **Logical/technical :** Technology controls performed by machines.
- **Operational :** Controls that are performed in person by people.
- **Virtual :** Control that are triggered dynamically when certain circumstances arise.

Syllabus Topic : Types of Attacks

1.2.2 Types of Attacks

Q. 1.2.3 List the types of attacks and hence explain any four. (Ref. Sec. 1.2.2) **(5 Marks)**

- Any computer that is accessible from the Internet will be attacked. It will constantly be probed by attackers and malicious programs intending to exploit vulnerabilities.
- Candidates for exploitation include any computer running a popular operating system or application for which the system administrator hasn't followed recommended hardening procedures.
- People sometimes criticize Microsoft for making insecure products and recommend using other, "safer" products. While Microsoft products include their fair share of vulnerabilities, you won't find any popular product from any manufacturer that hasn't been hacked.
- Every product that has ever claimed to be more securing than its competitors and has at least a moderate market share has been hacked.

- For example, Oracle Corporation launched an "Unbreakable" ad campaign in 2003 claiming Oracle's database software was impossible to compromise.
- The hacker community loves a good challenge and in short order three vulnerabilities were found. Java claimed to be much more secure than Microsoft's ActiveX mobile code security model, but time has shown us that Java has had dozens of compromises of its well-designed, but complex, security model.
- Open source fans have claimed for years that Linux is more secure than Microsoft Windows, but several studies don't back up that claim.
- Whatever system is popular and is used by a majority of people will be hacked. Changing from one popular OS to another may delay attackers for a brief while, but then exploits and hacks will appear.
- Hacking, worms and viruses existed long before Microsoft arrived in the computer world and they will be around long after Microsoft is gone. The truth is that any computer can be compromised and any computer can be extremely secure.
- The key is to make a habit of applying patches and taking appropriate security counter measures on a consistent basis.
- Attacks can take the form of automated, malicious, mobile code travelling along networks looking for exploit opportunities, or they can take the form of manual attempts by an attacker. An attacker may even use an automated program to find vulnerable hosts and then manually attack the victims.
- The most successful attacks, in terms of numbers of compromised computers, are always from completely automated programs. A single automated attack, exploiting a single system vulnerability, can compromise millions of computers in less than a minute.

1.2.2.1 Malicious Mobile Code

- There are three generally recognized variants of malicious mobile code : viruses, worms and Trojans. In addition, many malware programs have components that act like two or more of these types, which are called hybrid threats or mixed threats.
- The lifecycle of malicious mobile code might possibly comprise of phases such as Find, Exploit, Infect and Repeat.

a) Computer viruses

- A virus is a self-replicating program that uses other host files or code to replicate. Most viruses infect files so that every time the host file is executed, the virus is executed too.

- A virus infection is simply another way of saying the virus made a copy of itself (replicated) and placed its code in the host in such a way that it will always be executed when the host is executed.
- Viruses can infect program files, boot sectors, hard drive partition tables, data files, memory, macro routines and scripting files.

Anatomy of a virus

- The damage routine of a virus is called the **payload**. The vast majority of malicious program files do not carry a destructive payload beyond the requisite replication. This means they aren't intentionally designed by their creators to cause damage.
- However, their very nature requires that they modify other files and processes without appropriate authorization and most end up causing program crashes of one type or another. Error-checking routines aren't high on the priority list for most attackers.
- At the very least, a "harmless" virus takes up CPU cycles and storage space. The payload routine may be mischievous in nature, generating strange sounds, unusual graphics, or pop-up text messages. Payloads can be intentionally destructive, deleting files, corrupting data, copying confidential information, formatting hard drives and removing security settings. Some viruses are devious (long lasting and less direct).
- If the virus executes, does its damage and terminates until the next time it is executed, it is known as a **non resident virus**. These types of viruses are easier for novice malicious coders to write.
- If the virus stays in memory after it is executed, it is called a **memory-resident virus.** Memory-resident viruses insert themselves as part of the operating system or application and can manipulate any file that is executed, copied, moved, or listed.
- Memory-resident viruses are also able to manipulate the operating system in order to hide from administrators and inspection tools. These are called **stealth viruses.** Stealth can be accomplished in many ways.
- Memory-resident viruses have also been known to disinfect files on the fly, while they are being inspected by antivirus scanners and then re-infect the files after the scanner has given them a clean bill of health.
- If the virus overwrites the host code with its own code, effectively destroying much of the original contents, it is called an **overwriting virus.** If the virus inserts itself into the host code, moving the original code around so the host programming still remains and is executed after the virus code, the virus is called a **parasitic virus.**

- Viruses that copy themselves to the beginning of the file are called **pre-pending viruses** and viruses placing themselves at the end of a file are called **appending viruses.** Viruses appearing in the middle of a host file are labelled **mid-infecting viruses.**
- The modified host code is not always a file; it can be a disk boot sector or partition table, in which case the virus is called **a boot sector or partition table** virus, respectively.

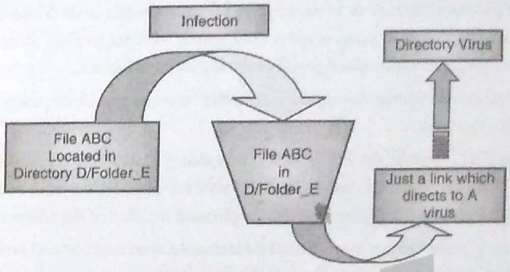

Fig. 1.2.1 : Example of overwriting virus

- There is one exception to the rule. Some boot sector viruses, like Tequila, are classified as **multipartite viruses,** because they can infect both boot sectors and program files.
- If activated in their executable file form, they will attempt to infect the hard drive and place infected boot code without having been transferred from an infected booted disk.
- Boot sector viruses (and partition table viruses) play tricks with the logical structure of the disk before the operating system has a chance to load and be in control.
- Boot sector viruses move the original operating system boot sector to a new location on the disk and partition table viruses manipulate the disk partition table in order to gain control first.
- Depending on how the virus accomplishes this and how well it is able to maintain the original boot information determines whether or not Windows can load afterward. Most boot sector virus damage routines run at the beginning of the virus's execution, before Windows is loaded. **Macro** viruses infect the data running on top of an application by using the program's macro or scripting language.

b) Computer worms

- A computer worm uses its own coding to replicate, although it may rely on the existence of other related code to do so. The key to a worm is that it does not directly modify other host code to replicate.

- A worm may travel the Internet trying one or more exploits to compromise a computer and if successful, it then writes itself to the computer and begins replicating again.

E-Mail worms

- E-mail worms are a curious intersection of social engineering and automation. They appear in people's inboxes as messages and file attachments from friends, strangers and companies. They pose as pornography, cute games, official patches from some reputed sources or unofficial applications found in the digital marketplace,
- After the malicious authors create the worm, they can use one of the many anonymous e-mail services to launch it.
- The worm first modifies the PC in such a way that it makes sure it is always loaded into memory when the machine starts. Then it looks for additional e-mail addresses to send itself to. It might use the registry to find the physical location of the address book file.
- In this way it grabs one or more e-mail addresses to send itself to and probably uses one of the found e-mail addresses to forge the sender address.

c) Trojans

- **Trojan horse programs**, or **Trojans**, work by posing as legitimate programs that are activated by an unsuspecting user.
- After execution, the Trojan may attempt to continue to pose as the other legitimate program (such as a screensaver) while doing its malicious actions in the background.
- Many people are infected by Trojans for months and years without realizing it. If the Trojan simply starts its malicious actions and doesn't pretend to be a legitimate program, it's called a **direct-action Trojan.**
- Direct-action Trojans don't spread well because the victims notice the compromise and are unlikely, or unable, to spread the program to other unsuspecting users.

Remote access trojans

- A powerful type of Trojan program called a **Remote Access Trojan (RAT)** is very popular in today's attacker circles. Once installed, a RAT becomes a **back door** into the compromised system and allows the remote attackers to do virtually anything they want to the compromised PC.
- RATs can delete and damage files, download data, manipulate the PC's input and output devices and record keystroke's screenshots. Keystroke and screen-capturing allows the attacker to track what the user is doing, including entry of passwords and other sensitive information.

- Unlike regular viruses and worms, the damage resulting from a RAT compromise can be felt long after the RAT is eradicated. RATs have even been known to record video and audio from the host computer's web camera and microphone. Imagine malware that is capable of recording every conversation made near the PC. Surely confidential business meetings have been recorded.
- RATs come with server and client programs. The client portion creates server executables that are meant to be run on unsuspecting users' PCs, while the server programs can be extensively customized.
- The server can be made to listen on a particular UDP or TCP port, use encryption, require connection passwords and be compiled with all sorts of additional functionality. The RAT server executable can be disguised as a game or combined with some other interesting program.
- Occasionally, RATs are used for detective work and spying. Commercial, legal RATs have been used by investigators to reverse-hack and track attackers. RATs are being used by scorned ex-spouses during divorces to spy and gather evidence on their former partners.
- Legitimate RATs are even being marketed as a way for mom and dad to monitor the kids' online activity from work and as a way for employers to monitor employees' computer use.

Zombie trojans and DDoS attacks

- **Zombie Trojans** infect a host and wait for their originating attacker's commands telling them to attack other hosts. The attacker installs a series of zombie Trojans, sometimes numbering in the thousands.
- With one predefined command, the attacker can cause all the zombies to begin to attack another remote system with a **Distributed Denial of Service (DDoS)** attack. DDoS attacks flood the intended victim computer with so much traffic, legitimate or malformed, that it becomes over utilized or locks up, denying legitimate connections.

1.2.2.2 Malicious HTML

- Pure HTML coding can be malicious when it breaks browser security zones or when it can access local system files. Malicious HTML has often been used to access files on local PCs, too.

- Specially crafted HTML links can download files from the user's workstation, retrieve passwords and delete data.HTML coding often includes script languages with more functionality and complex active content.
- Script languages, like JavaScript and VBScript, can easily access local resources without a problem and thus most e-mail worms are coded in VBScript.

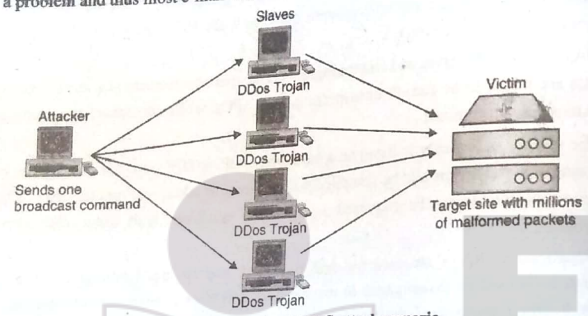

Fig. 1.2.2 : Example of DDoS attack scenario

- An increasing number of malicious exploits are being accomplished with malformed media files, the end users thinks that they are downloading a music or video file and hidden in the content is a buffer overflow or virus.
- Almost all of the most popular media types used on the Internet today have been exploited, including Flash, Real Audio and Windows Media Player files.

1.2.2.3 Advanced Persistent Threats (APTs)

Q. 1.2.4 Explain Advanced Persistent Threats (APTs). (Ref. Sec. 1.2.2.3) (5 Marks)

- The use of sophisticated malware for targeted cybercrime is known as **Advanced Persistent Threats (APTs).**
- Usually targeted at businesses and governments that have political adversaries, APTs are created and directed by hostile governments and organized criminals for financial or political gain.
- APTs are intentionally stealthy and difficult to find and remove and they may hide for months on an organization's network doing nothing, until they are called upon by their controllers.

- These attacks usually begin with a simple malware attack. This can be a targeted attack against a victim within the organization, such as an engineer or researcher with access to confidential material. The attacker may send an infected document, such as a PDF file, to the victim, along with a highly believable e-mail message to trick the victim into opening the file.
- Alternatively, the attacker may send a URL that point to a web server that executes malicious code on the victim's browser, even without the victim's intervention.
- This is known as a **drive-by download**. In some cases, the attacker may first compromise a legitimate web site the victim may run across during normal business research or poison DNS entries to send the victim to their compromised web site.
- In either case, the malicious code is run by the victim's web browser without requiring the user to respond. All of these targeted attacks are collectively known as **spear-phishing i.e.** targeting a specific individual or small group of people with a tailored attack intended to look like a legitimate inquiry, in order to trick the victim into running the malware. This is the first phase of an APT attack.
- Once the malware infects the victim's computer, usually silently and without the user's knowledge, it remotely triggers to download further malware. In this second phase of the attack, the malware reaches out to a **Command and Control Server (CnC Server)** to bring down **rootkits**, Trojans, RATs and other sophisticated malware completely compromising the victim's computer and usually without any indication that anything is wrong, when in full effect.
- A computer that has been compromised by an APT can never be fully cleaned, because the sophistication of the malware allows it to embed itself deeply into the computer's internal and the vulnerabilities it exploits may not be patched for a long time, if ever. Compromised systems should be completely rebuilt.

1.2.2.4 Physical and Network-Layer Attacks

Q. 1.2.5 Explain Physical, Network-Layer Attacks. (Ref. Sec. 1.2.2.4) (5 Marks)

- In today's world of interconnectedness, the least popular means of attack is direct physical access, but if an attacker can physically access a computer, its game over. They literally can do anything, including physically damage the computer, steal passwords, plant key stroke logging Trojans and steal data.
- Firstly, physical security is a necessity and secondly, it is often those we trust that break our security.

- Many attacker attacks are directed at the lower six layers of the Open Systems Interconnection (OSI) network protocol model.
- Network-layer attacks attempt to compromise network devices and protocol stacks. Network-layer attacks include packet-sniffing and protocol-anomaly exploits.

a) Packet sniffing

- Encryption is a technique used to prevent packet-sniffing (also known **as packet capturing or protocol analyzing)** attacks. **Sniffing** occurs when an unauthorized third party captures network packets destined for computers other than their own.
- Packet sniffing allows the attacker to look at transmitted content and may reveal passwords and confidential data.
- In order to use sniffing software, an attacker must have promiscuous network card and specialized packet driver software, must be connected to the network segment they want to sniff and must use sniffer software.
- By default, a Network Interface Card (NIC) in a computer will usually drop any traffic not destined for it. By putting the NIC in promiscuous mode, it will read any packet going by it on the network wire.
- Packet-sniffing attacks are more common in areas where many computer hosts share the same collision domain (such as a wireless segment or local LAN shared over an Ethernet hub) or over the Internet where the attacker might insert a sniffer in between source and destination traffic.
- Although many protocols encrypt traffic going across the network, many protocols send data unencrypted in their plaintext forms. Popular protocols like HTTP, FTP and Telnet are famous for leaking passwords and confidential information if sniffed.

b) Protocol-anomaly attacks

- Most network protocols were not created with security in mind. A rogue attacker can create malformed network packets that do not follow the intended format and purpose of the protocol with the result that the attacker is able to either compromise a remote host or network or compromise a confidential network data stream.
- Network-layer attacks are most often used to get past firewalls and to cause DoS attacks. DoS attacks are common against big e-commerce sites. Network-layer attacks usually require that the attacker create malformed traffic, which can be created by tools called **packet injectors or traffic generators.**

- Packet injectors are used by legitimate sources to test the throughput of network devices or to test the security defences of firewalls and IDSs.
- Attackers can even manually create the malformed traffic as a text file and then send it using a **traffic replay** tool. Network-layer attacks are not nearly as common as application-layer attacks.

1.2.2.5 Application-Layer Attacks

Q. 1.2.6 Explain Application-Layer Attacks. (Ref. Sec. 1.2.2.5) **(5 Marks)**

- Application-layer attacks include any exploit directed at the applications running on top (7^{th} layer) of the OSI protocol stack.
- Application-layer attacks include exploits directed at application programs, as well as against operating systems. Application-layer attacks include content attacks, buffer overflows and password-cracking attempts.

a) Content attacks

- After malicious mobile code, content and buffer overflow attacks are the most popular attacker method.
- The attacker learns which applications are running on a particular server and then sends content to exploit a known hole.
- Common content attacks include the following :
  - SQL injection attacks
  - Unauthorized access of network shares
  - File-system transversals
- In **SQL injection,** an attacker connects to a web site with a SQL server back-end database.
- The web site contains a customer input form asking for some sort of innocent information such as age. But instead of entering a numeric value, as the web site is expecting, the attacker enters a malformed command that is misinterpreted by the server and that leads to the remote execution of a privileged command.
- **Unauthorized access of network shares** results from a major flaw in Windows is that, by default, network shares are advertised for the world to see on NetBIOS ports 137 through 139 and port 445 (in newer Windows versions).

- On a Windows PC which is connected to the Internet without a firewall blocking access to those ports, it is likely that the PC's network shares a reviewable by the world.
- If the Windows system is unpatched or the shares have weak passwords or no passwords, then remote attackers will be able to access shares.
- Although exploiting open Windows shares is a common worm action, if attackers detect open NetBIOS ports, they will attempt to access the shares manually.
- **File-system transversal** attacks happen when an attacker is able to malformed an application input request in such a way that unauthorized access to a protected directory or command is allowed. Usually this is done by using encoded character schemes, numerous backslashes(\) and periods(.).

b) Buffer overflows

- **Buffer overflows** occur when a program expecting input does not do input validation. For example, suppose the program was expecting the user to type in a five-digit ZIP code, but instead the attacker replies with400 characters.
- The result makes the host program error out and quit, throwing excess data into the CPU. If the buffer overflow attacker can reliably predict where in memory his buffer overflow data is going, the buffer overflow can be used to completely compromise the host Otherwise, it just creates a DoS condition.

c) Password cracking

- Password crackers either try to guess passwords or they use brute-force tools. **Brute-force** tools attempt to guess a password by trying all the character combinations listed in an accompanying **dictionary.**
- The dictionary may start off blindly guessing passwords using a simple incremental algorithm or it may use passwords known to be common on the host. If the attacked system locks out accounts after a certain number of invalid login attempts, some password attackers will gain enough access to copy down the password database and then brute-force it offline.

1.2.2.6 Man-in-the-Middle (MITM) Attacks

Q. 1.2.7 Explain Man-in-the-Middle (MITM) Attacks (Ref. Sec. 1.2.2.6)

- Man-In-The-Middle (MITM) attacks are a valid and extremely successful threat vector. Exploitation often requires knowledge of multiple tools and physical access to the network or proximity to an access point. MITM attacks often take advantage of ARP poisoning at Layer 2 (of OSI model).
- An MITM attack can take a few different forms such as Media Access Control (MAC) flooding, ARP poisoning, DHCP (Dynamic Host Configuration Protocol) poisoning, DNS (Domain Name Server) poisoning and ICMP (Internet Control Message Protocol) poisoning which are very effective, as well as the use of a malicious wireless Access Point (AP).
- Fake APs have become a common threat vector, exploiting the manner in which clients automatically connect to known SSIDs.
- This enables an attacker to connect and intercept the victim's network traffic without the victim seeing any indication they are under attack.

a) Media Access Control (MAC) Flooding

- MAC flooding, technically known as MAC addresses flooding, is where an application injects a specially crafted layer two and layer three packets onto the network repeatedly.
- This causes the layer-two switch to fill up its buffers and crash. Since switch crash behavior is to fail/open, all ports are flooded with all frames, thus causing the Denial of Service (DoS).

b) Address Resolution Protocol (ARP) Poisoning

- ARP poisoning works by simply responding to Address Resolution Protocol (ARP) requests with the attacker's *MAC address*.
- The attacker tells the device that wishes to communicate with the victim's computer that the attacker knows how to reach the victim and then the attacker tells the network that the attacker's computer is the victim's computer and effectively masquerading as the victim's computer and responding on its behalf.
- The switch then updates its table of MAC addresses with the attacker's MAC address. The switch uses this to route traffic and now believes the attacker's system is the victim's system.
- This creates an MITM situation where the victim routes its traffic through the attacker and out through the gateway to whatever it needs to go. This attack simply exploits the correct functioning of the ARP protocol. The problem is when a rogue system actually responds to all ARP requests. The switch will continue to update its table with the incorrect information.

- An ARP poisoning attack can be executed so that it only updates the ARP table of the victim and not the gateway (one-way poison).
- Many organizations protect the network architecture, but put no such defenses in place for their host systems.
- An attacker can leverage this oversight to poison the host systems and still route victim traffic through the attacker's system. True defenses must protect the client systems as well as the networking devices routing traffic.

c) Dynamic Host Configuration Protocol (DHCP) Poisoning

- Another poisoning attack is DHCP poisoning. This attack allows an attacker to compromise victims with three simple steps : provide the pool of addresses to assign for the victims, provide the netmask for the victims and finally provide the DNSIP address.
- An attack takes only seconds to execute. Once a request for an IP address is heard on the line, the fake DHCP server will race against the true DHCP server to provide an address from its pool.
- Once accepted, the victim is connected and traffic will be passing through the attacker's system. Denial of service attack is used as a tool to repeat the renew process with different parameters. This causes the DHCP server to exhaust its pool of addresses, resulting in the denial of service.

d) Domain Name System (DNS) Spoofing Attack

- A DNS spoofing attack is just as easy to execute as a DHCP poisoning attack. All traffic from the victim is forwarded through the attacker's fake DNS service and redirected so that all requests for Internet or internal sites land at the attacker's site, from which the attacker can harvest credentials or possibly launch browser-based attacks.
- The fundamentals of this attack come from "namere solution order" and manipulating that process. DNS is designed so that every DNS query first goes to a DNS server, usually a local one on the network or provided by the ISP.
- That server will have been pre-configured with the IP addresses of the top-level (root) DNS servers on the Internet that are the authoritative "source of truth" for all IP addresses and hostnames.

- The root server that responds would respond with the address of a lower level DNS server. This process continues until the name and IP address is found, usually at least three levels down.
- But this rarely occurs in practice today. The Internet is millions of times larger than was considered when DNS was designed and the root DNS servers would be over whelmed by all the DNS requests that happen in reality.
- As a result, lower level DNS servers "cache" information storing it locally for faster response. This storage is kept for the length of time specified by the Time-To-Live (TTL) setting on each DNS server.
- It is these caches that can be poisoned with false information that sends requestors to the attacker's IP address. A complete mastery of DNS is needed to defend against these attacks because they target a common open port, TCP/UDP 53, which is very necessary in today's networks.

e) Internet Control Message Protocol (ICMP) Poisoning

- The final poisoning attack available is ICMP poisoning. One caveat for the attacker wishing to execute an ICMP attack is that they need to be able to see all traffic; if they are attached to a switch, this attack is not useful because this is a layer three attack, unless the attacker's computer is connected to a spanning port, which in turn would forward all traffic to the attacker's system so they could see it.
- Like the other poisoning options available, this can be set up and executed quickly.
- An attacker only has to provide the MAC address of the gateway and the IP address of the gateway. The attack tool will do the rest.

1.2.2.7 Wireless Attacks

- Three common wireless attacks are to use a fake Access Point (AP), to use a fake AP with a static Extended Service Set ID (ESSID) and to use a fake AP and an "evil twin".
- All can be set up and executed quickly. By setting up the fake AP, an attacker can gain full control over all TCP/IP connections passing through it.
- At that point, intercepting traffic and capturing or modifying it becomes trivial. With an SSID that is known to the unsuspecting victim, the fake AP cannot be distinguished from a real AP.
- An attacker can set up a fake AP with a static ESSID and channel designation. This attack helps to target specific victims whose devices look to connect with a specific ESSID.

- The attack begins by launching a fake AP along with a DHCP server to provide IP addresses to the victims. As connections are made, each victim will be assigned an IP address and traffic will be tunneled through the attacker's system.
- Another wireless attack option is to set up an "evil twin" AP. This differs from the static attack in that it responds to all beacons from potential victims even while the real AP is responding.
- It informs the victims that it is indeed the AP they are looking to connect with regardless of ESSID. Those victims who hear from the evil twin first will use its information instead of that from the real AP.
- The setup and execution is similar to the static attack, except the ESSID and channel designations are unnecessary. This attack listens and responds to all requests on all channels. This attack can be leveraged within an organization, but is most useful when a less targeted approach is required, in locations such as coffee shops, airports, trains, airplanes, hotels, or anywhere a mobile device is looking for a connection to its organization's network or other networks.
- Sometimes, setting up a malicious AP is not enough. If a potential victim is already connected to a wireless network, they are less likely to switch to the attacker's connection. In an effort to hasten a victim's connection, a DoS attack can be used to deauthenticate devices from their current access point. A "last man standing" approach is to deny service to all APs in the vicinity by using a DoS attack, leaving the attacker's malicious AP as the only one available to the potential victims.

  One of three things will happen during these attacks :
  - Nothing if the APs are properly defended.
  - The victim device will automatically connect to the malicious AP.
  - The victim device will manually connect to the malicious AP.
- Do these attacks sound difficult to perform? They're not. An all-in-one wireless attack tool is available that can do all these things automatically, without requiring any specialized knowledge of the underlying technology. In other words, with the right tool, an attacker doesn't even have to know how the attacks work.

Syllabus Topic : Risk Analysis

1.2.3 Risk Analysis

Q. 1.2.8 Explain risk analysis. (Ref. Sec. 1.2.3) (5 Marks)

- A risk analysis needs to be a part of every security effort. It should analyze and categorize the assets that need to be protected and the risks that need to be avoided and it should facilitate the identification and prioritization of protective elements.
- It can also provide a mean to measure the effectiveness of the overall security architecture, by tracking those risks and their associate dmitigation over time to observe trends.
- Risk analysis depends on factor such as the needs of the organization and the audience for the information.
- In a larger, well structured environment, a more detailed risk analysis may be needed.
- Military and high-risk environments may also merit a greater level of diligence and detail. Conversely, a small office environment may not require a deep analysis.
- In any case, there must be at least some definition of what the security program is intended to defend otherwise it may focus on the wrong priorities or overlook important assets(leaving them exposed) and threats (failing to defend against them).
- Simply put, the formal definition of *risk* is the probability of an undesired event (a threat) *exploiting* a *vulnerability* to cause an undesired result to an *asset*. Thus :

  Risk = Probability (Threat + Exploit of Vulnerability) × Cost of Asset Damage
- A quantitative approach to risk analysis will take into account actual values such as the estimated probability or likelihood of a problem occurring along with the actual cost of loss or compromise of the assets in question. One commonly used approach to assigning cost to risks is Annualized Loss Expectancy (ALE).

Annualized Loss Expectancy (ALE)	=	Single Loss Expectancy (SLE)	×	Annualized Rate of Occurrence (ARO)

  where : Single Loss Expectancy (SLE) is the cost of an undesired event and Annualized Rate of Occurrence (ARO) is the number of times that event is expected to occur in one year.
- A qualitative approach to risk analysis, which may suffice in smaller environments or those with limited resources, can be just as effective. You can identify your assets (for example, a web server, a database containing confidential information, workstation computers and a network).

- You can identify the threats to those assets (malware, hack attacks, bugs and glitches, power outages and so forth). And you can assign a severity level to help you prioritize your remediation.
- If the severity is high enough, you will probably want antivirus capability on the endpoints as well as on the network, a high-quality stateful firewall, a timely patching program that includes testing and Uninterruptable Power Supplies (UPSs).
- How much you spend on these things and which ones you work on first, depends on the severity you assign to each. Regardless of whether you take a quantitative or qualitative approach and how deeply you dive into the analysis, don't overlook the risk analysis process. It is an important part of the planning that needs to go into the development of an effective security program.

Syllabus Topic : Secure Design Principles

1.3 Secure Design Principle

Q. 1.3.1 Write short note on Secure Design Principle. (Ref. Sec. 1.3) **(5 Marks)**

- Network security implementation is based on some kind of model, whether clearly stated as such or assumed.
- For example, organizations that use firewalls as their primary means of defense rely on a perimeter security model, while organizations that rely on several different security mechanisms are practicing a layered defense model.
- Every security design includes certain assumptions about what is trusted and what is not trusted and who can go where.
- Starting out with clear definitions of what is fully trusted, what is partially trusted and what is untrusted, along with an understanding of which defense model is being used, can make a security infrastructure more effective and applicable to the environment it is meant to protect.

Syllabus Topic : The CIA Triad and Other Models

1.3.1 The CIA Triad and Other Models

Q. 1.3.2 Explain CIA triad model. (Ref. Sec. 1.3.1) **(5 Marks)**

- The CIA triad stands for Confidentiality, Integrity and Availability. This venerable, well-established conceptual model, though very data-centric, is often useful in helping people think about security in terms of the most important aspects of information protection.
- The CIA concept focuses on three aspects of information protection that are important.

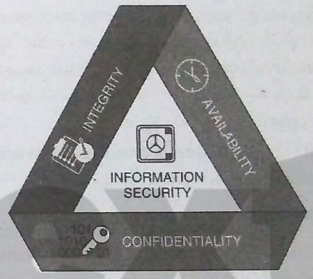

Fig. 1.3.1 : The CIA triad of security

Confidentiality

- **Confidentiality** refers to the restriction of access to data only to those who are authorized to use it. This simply means that a single set of data is accessible to one or more authorized people or systems and nobody else can see it.
- Confidentiality is distinguishable from **privacy** in the sense that "confidential" implies access to one set of data by many sources, while "private" usually means the data is accessible only to a single source.
- As an example, a pin code of Debit card is considered private because only one person should know it, while a bank account number is considered confidential because multiple persons may need to know the account to do some transaction.

Integrity

- Integrity, which is particularly relevant to data, refers to the assurance that the data has not been altered in an unauthorized way.

- Integrity controls are meant to ensure that a set of data can't be modified (or deleted entirely) by an unauthorized party. Part of the goal of integrity controls is to block the ability of unauthorized people to make changes to data and another part is to provide a means of restoring data back to a known good state (as in backups).

Availability

- Unlike confidentiality and integrity, which make the most sense in the context of the data contained within computer systems, availability refers to the "uptime" of computer-based services which gives the assurance that the service will be available when it's needed. Service availability is usually protected by implementing high-availability (or continuous-service) controls on computers, networks and storage.
- High-Availability (HA) pairs or clusters of computers, redundant network links and RAID disks are examples of mechanisms to protect availability.

Additional Concepts

- Alternatives to the CIA triad that include other aspects of security have been proposed by various thought leaders in the security profession.
- The U.S. Department of Defense defined "Five Pillars of Information Assurance", which include Authenticity and Non-Repudiation along with the CIA triad.
- The Organization for Economic Co-operation and Development (OECD) published guidelines that added Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management and Reassessment. Perhaps the most complete set is included in the U.S. National Institute of Standards and Technology Special Publication800-27, Revision A, which proposes a total of 33 principles for securing technology systems.
- There are many ways to categorize security principles and the CIA triad is the most simplistic of them all.
- In sum, the best-known attributes of security defined in the preceding models and others like them includes Confidentiality, Integrity, Availability, Accountability, Accuracy, Authenticity, Awareness, Completeness, Consistency, Control, Democracy, Ethics, Legality, Non-repudiation, Ownership, Physical Possession, Reassessment, Relevance, Response, Responsibility, Risk Assessment, Security Design and Implementation, Security Management, Timeliness, Utility.

Syllabus Topic : Defense Models

1.3.2 Defense Models

Q. 1.3.3 Explain lollipop model and onion model. (Ref. Sec. 1.3.2) (5 Marks)

- There are two basic approaches that can be taken to preserve the confidentiality, integrity, availability and authenticity of electronic and physical assets such as the data on the network :
  - Build a defensive perimeter around those assets and trust everyone who has access inside.
  - Use many different types and levels of security controls in a layered defense-in depth approach.
- A firewall alone provides only one layer of protection against threats originating from the Internet and it does not address internal security needs.
- With only one layer of protection, which is common on networks connected to the Internet, all a determined individual has to do is successfully attack that one system to gain full access to everything on the network.
- The lollipop and the onion concepts are used to visually depict the two most common approaches to security.

The lollipop model

- The most common form of defense, known as **perimeter security**, involves building a virtual (or physical) wall around objects of value.
- Perimeter security is like a lollipop with a hard, crunchy shell on the outside and a soft, chewy center on the inside. In network security, a firewall is like the perimeter that can't keep out all attackers.
- Yet the firewall is the most common choice for controlling outside access to the internal network, creating a virtual perimeter around the internal network (which is usually left wide open).
- This often creates a false sense of security because attackers can break through, exploit vulnerabilities or compromise the network from the inside.
- One of the limitations of perimeter security is that once an attacker breaches the perimeter defense the valuables inside are completely exposed.

- As with a lollipop, once the hard, crunchy exterior is cracked, the soft, chewy center is exposed. Hence the security is compromised so this cannot be considered as the best model of defense.
- Another limitation of the lollipop model is that it does not provide different levels of security.
- On a computer network, a firewall is limited in its abilities and it shouldn't be expected to be the only line of defense against intrusion.

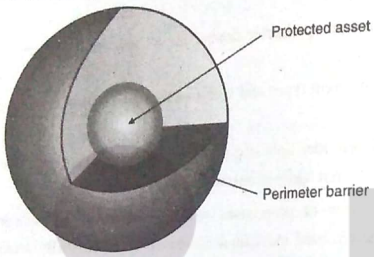

Fig. 1.3.2 : The Lollipop model of defence

The onion model

- A better approach is the **onion model** of security. It is a layered strategy, often referred to as **defense in depth.** This model addresses the contingency of a perimeter security breach occurring. It includes the strong wall of the lollipop but goes beyond the idea of a simple barrier.
- A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer.

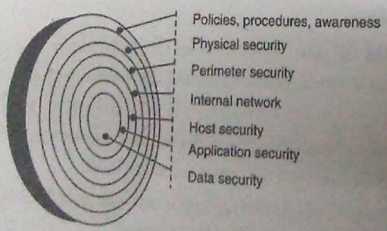

Fig. 1.3.3 : The Onion model of defence

- When an attacker gets past the firewall or when a trusted insider, like an employee or a contractor, abuses their privileges, the on ion model addresses these contingencies.
- A layered security architecture provides multiple levels of protect ion against internal and external threats.
- The more layers of controls that exist, the better the protection against a failure of anyone of those layers.
- The layered security approach can be applied at any level where security controls are placed not only to increase the amount of work required for an attacker to break down the defenses but also to reduce the risk of unintended failure of any single technology.
- System, network and application authentication controls can be layered. Network, system access controls and Encryption protocols can be layered (such as by encrypting first with PGP (Pretty Good Privacy) followed by encrypting with Blowfish or AES) can also be layered.
- Audit trails can be layered with the use of local system logs coupled with off-system network activity logs.

Syllabus Topic : Zones of Trust

1.3.3 Zones of Trust

Q. 1.3.4 Describe zone of trust. (Ref. Sec. 1.3.3) **(5 Marks)**

- Different areas of a network trust each other in different ways. Some communications are trusted completely and the services they rely on assume that the sender and recipient are on the same level, as if they were running on a single system.
- Some are trusted incompletely and they involve less trusted networks and systems, so communications should be filtered. Some networks (like the Internet or wireless hotspots) are untrusted.
- The security controls should carefully screen the interfaces between each of these networks.
- These definitions of trust levels of networks and computer systems are known as **zones of trust.**

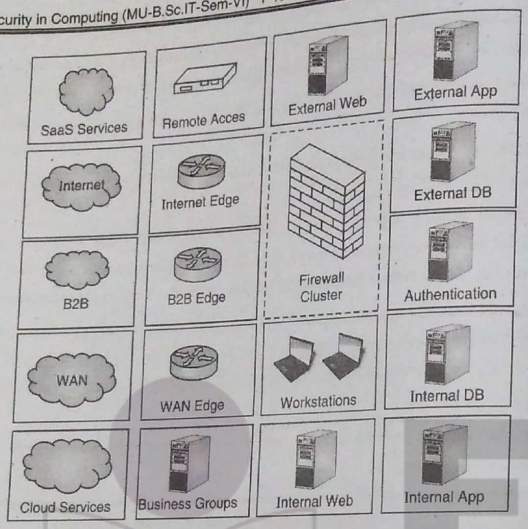

Fig. 1.3.4 : Zones of trust

- Once the risks and threats to the business is identified and it is known what functions are required for the business, those functions can be separated into zones of trust.
- Zones of trust are connected with one another and business requirements evolve and require communications between various disparate networks, systems and other entities on the networks.
- Separating the resources into zones of trust enables a user to vary the levels of security for these resources according to their individual security needs.
- The use of multiple zones allows access between a less and a more trusted zone to be controlled to protect a more trusted resource from attack by a less trusted one.
- Any zone could be subdivided into **policy pockets** of common security policies used to support additional classification categories without the infrastructure expense of establishing another zone.
- Firewalls, routers, virtual LANs (VLANs) and other network access control devices and technologies can be used to separate trust zones from each other. Access Control Lists (ACLs) and firewall rules can be used to control the intercommunication between these levels based on authorization rules defined in the security architecture.

- The importance of trust models is that they allow a broad, enterprise-wide view of networks, systems and data communications and they highlight the interactions among all of these components.
- Trust models can also distinguish boundaries between networks and systems and they can identify interactions that might otherwise be overlooked at the network level or system level.
- Trust can also be viewed from a transaction perspective. During a particular transaction, several systems may communicate through various zones of trust.
- In a transaction-level trust model, instead of systems being separated into different trust zones based on their locations on the network, systems can be separated into functional categories based on the types of transactions they process.
- Thus, security controls at the system and network levels should allow each of these systems to perform their authorized functions while preventing other systems not involved in the transaction from accessing these resources.
- Segmenting network data resources based on their access requirements is a good security practice. Segmentation allows greater refinement of access control based on the audience for each particular system and it helps confine the communications between systems to the services that have transactional trust relationships.
- Segmentation also confines the damage of a security compromise. In the event that a particular system is compromised, network segmentation with access control lists reduces the number and types of attacks that can be launched from the compromised system.
- A layered segmentation approach also provides a useful conceptual model for network and system administrators. Several groups of servers can be included in a layer, defined by the types of services they perform, the types of data they handle and the places they need to communicate to and from.

Syllabus Topic : Best Practices for Network Defense

1.3.4 Best Practices for Network Defense

Q. 1.3.5 List some best practices for network defense and hence explain four practices. (Ref. Sec. 1.3.4) (5 Marks)

There are many countermeasures that can be implemented to minimize the risk of a successful attack, such as securing the physical environment, hardening the operating systems, keeping patches updated, using an antivirus scanner, using a firewall software, securing network share permissions, using encryptions, securing applications, secure P2P services, make sure programmers program securely, backing up the system, creating a computer security defense plan and implementing ARP poisoning defenses.

1.3.4.1 Secure the Physical Environment

- A basic part of any computer security plan is the physical aspect.
- Depending on the working environment, PCs and laptops might need to be physically secured to their desks.
- There are several different kinds of lockdown devices, from thin lanyards of rubber-coated wire to hardened metal jackets custom-made to surround a PC.
- If anyone leaves their laptop on their desk overnight, it should be secured.
- There are also other steps that need to be taken on every PC in the environment such as password protect booting, password protect CMOS (Complementary Metal-Oxide Semiconductor) and Disable Booting from USB and CD.

Harden the Operating System

The **attack surface** of the operating system is reduced by removing unnecessary software, disabling unneeded services and locking down access :

1. Reduce the attack surface of systems by turning off unneeded services.
2. Install secure software.
3. Configure software settings securely.
4. Patch systems regularly and quickly.
5. Segment the network into zones of trust and place systems into those zones based on their communication needs and Internet exposure.
6. Strengthen authentication processes.
7. Limit the number (and privileges) of administrators.

1.3.4.2 Keeping Patches Updated

- An unpatched system is the best choice for any attacker. In most cases, the vulnerabilities use dare widely known and the affected vendors have already released patches for system administrators to apply.

- A solid patch management plan is essential for protecting any platform, regardless of operating system and regardless of whether or not it is connected directly to the Internet.
- Keeping any technology system up-to-date with the latest software is crucial, because vendors find and fix vulnerabilities overtime.

1.3.4.3 Using an Antivirus Scanner (with Real-Time Scanning)

- An antivirus (AV) scanner is very essential in current scenario. It should be deployed on the desktop, with forced, automatic updates and it should be enabled for real-time protection.
- By placing the antivirus solution on the desktop, it is ensured that no matter how the malware gets there, it will be blocked.
- The AV solution should be enabled for real-time protection so it scans every file as it comes into the system or enters the computer's memory, so it can prevent malware from executing.
- Sometimes, in the interest of performance, users will want to disable the real-time functionality.

1.3.4.4 Use Firewall Software

- As important as an AV scanner is, the firewall is equally important. Firewalls are able to collate separate events into one threat description (such as a port scan) and can identify the attack by name. Every PC should be protected by firewall software.
- Desktop firewall software (also known as host-based firewalls or personal firewall software) can protect a PC against internal and external threats and usually offer the added advantage of blocking unauthorized software applications (such as Trojans) from initiating outbound traffic. Many antivirus scanning organizations offer firewall combo packages.

1.3.4.5 Secure Network Share Permissions

- One of the most common ways an attacker or worm breaks into a system is through a network share (such as NetBIOS or SMB) with no password or a weak password.
- Folders and files accessed remotely over the network should have Discretionary ACLs (DACLs) applied using the principle of least privilege and should have complex passwords.

- By default, Windows assigns and most administrators allow, the 'Everyone' group to have Full Control or Read permissions throughout the operating system and on every newly created share. This is the opposite of the least privilege principle.
- To counteract this problem, at a minimum, 'Everyone' Full Control can be changed to Authenticated Users Full Control, wherever possible.
- Many Windows administrators believe that it is acceptable for all shares to have Everyone Full Control as the underlying NTFS (New Technology File System) permissions, which are usually less permissive, will result in the desired tighter effective permissions.

1.3.4.6 Use Encryption

- Most computer systems have many encryption opportunities which must be used. Linux and Unix administrators should be using SSH (Secured SHell) instead of Telnet or FTP (File Transfer Protocol) to manage their computers.
- The latter utilities work in plaintext over the network, whereas SSH is encrypted. If FTP is used, it must be used along with SSL (Secured Socket Layer) and digital certificates to encrypt traffic. In order for encrypted FTP to work, both the client and the server must support the same encryption mechanism.
- Encrypting File System (EFS) is one of the most exciting features in Windows. EFS encrypts and decrypts protected files and folders on the fly. Once turned on by a user, EFS will automatically generate public/private encryption key pairs for the user and the recovery agent.
- All the encrypting and decrypting is done invisibly in the background. If an unauthorized user tries to access an EFS-protected file, they will be denied access since EFS encrypts and decrypts on the fly, it won't prevent malware occurrences while the authorized user is logged on.
- However, EFS-protected folders and files will be protected when the authorized user is not logged on. This may prevent maliciousness in certain circumstances. Since EFS can help provide additional security, is virtually invisible to the end user and has a minimal performance hit, it is something to consider using for added protection.

1.3.4.7 Securing Applications and their Configuration

- Managing the applications and their security should be a top priority of any administrator. Applications can be managed by configuring application security, installing applications to nonstandard directories and ports, locking down applications, securing P2P services and making sure your application programmers code securely.

- Applications should be configured with the vendors' recommended security settings.

Securing E-Mail

- E-mail worms continue to be the number-one threat on computer systems. Most worms arrive as a file attachment or as an embedded script that the end user executes.
- Clearly, you can significantly decrease your network's exposure risk by securing e-mail. This can be done by disabling HTML content and blocking potentially malicious file attachments. Anything beyond plain text in an e-mail can be used maliciously against a computer. For that reason, it is important to restrict e-mails to plain text only or, if you must allow it, plain HTML coding only.
- You should disable scripting languages and active content, such as ActiveX controls, Java and VBScript objects. Often this is as simple as checking a checkbox in the e-mail client to force all incoming e-mail to be rendered in plain text. Some clients handle this more elegantly than others and HTML-only messages can be badly mangled during conversion or can appear blank.
- Outlook and Outlook Express allow e-mails with active content to be opened in the Restricted Internet zone, which disables content beyond plain HTML coding. This is the default setting in Microsoft's latest e-mail clients.
- Early clients opened e-mail in the much more permissive Internet security zone. If you can block active content from executing, then all you have to worry about is end users clicking malicious HTML links or opening file attachments.
- It is difficult to block users from clicking malicious HTML links if they already have Internet access. In Windows environments, you can use Group Policy, Internet Explorer Administration Kit (IEAK), or some other type of proxy server filter to only allow end users to visit preapproved sites, but beyond that you have to rely on end-user education.

1.3.4.8 Blocking Dangerous File Types

- Blocking dangerous file attachments is the best way to prevent exploits. Considering today's preferred method of e-mailing viruses and worms the biggest question is "What constitutes a dangerous file type?"
- The truth is that almost any file type can be used maliciously, so the better question is "What are the popularly used malicious file types?" Even that list isn't small. Table 1.3.1 shows the Windows file types that are commonly blocked in organizations that are concerned about the various popular attacks that use these file types as vectors. These are in order of their prevalence in e-mail server block lists.

Table 1.3.1 : Commonly Blocked File Extensions

File Extension	Description	Threat
.scr	Windows screen saver file	Can contain worms and Trojans
.bat	DOS batch file	Can contain malicious commands
.pif	Program information file	Can run malicious programs
.com	DOS application	Can be a malicious program
.exe	Windows application	Can be a malicious program
.vbs	Visual Basic script	Can contain malicious code
.cmd	Command script	Can be used to script malicious batch files
.shs	Shell scrap object	Can mask rogue programs
.vbe	Visual Basic file	Can contain malicious code
.hta	**HTML.** application	Frequently used by worms and Trojans
.reg	Windows registry settings file	Modifies Windows registry, can change security settings.
.jse	JavaScript encoded file	Can contain malicious code
.wsf	Windows Script file	Can execute malicious code
.sct	Windows Script components file	Can execute malicious code
.wsh	Windows Script Host file	Can execute malicious code
.chm	Microsoft Compiled **HTML.** Help file	Can exploit browser vulnerabilities
.js	JavaScript file	Can contain malicious code
.jnk	Shortcut link	Can be used to automate malicious actions
.cpt	Windows Control Panel file	Can be used to automate malicious actions
.htp	Microsoft Help file	Can be used in multiple exploits

File Extension	Description	Threat
.wsc	Windows Shell command file	Can execute malicious code
.shb	Shell scrap object	Can execute malicious code
.vb	Visual Basic file	Can contain malicious code
.msi	Windows Installer package	Can install malicious programs
.msp	Windows Installer Patch file	Can contain malicious code
bas	Programs written in the BASIC programming language	Can be malicious code
.crt	Digital certificate	Can be used in exploits to trust malicious code
.ins	Microsoft Internet communication settings	Can change security settings
.isp	Microsoft Internet Service Provider settings	Can change security settings
.msc	Microsoft Management Console settings	Can change security settings
.mst	Windows Installer transform file	Can install malicious code
.ade	Microsoft Access file	Can contain malicious code
.adp	Microsoft Access file	Can contain malicious code
.mdb	Microsoft Access file	Can contain malicious code
.inf	Installation package	Can install malicious code

- As large as Table 1.3.1 is, many readers can probably add other file extensions to the list from their own experience. Only you can judge what file extensions have an acceptable cost/benefit ratio and should be allowed into your network.
- However, allowing every file extension into your network is asking for a security exploit. For example, Visual Basic script (.vbs) files are one of the most common malicious file types for e-mail worms and viruses.

- Although people rarely send each other .vbs files for legitimate reasons, worms and viruses do it all the time. It only makes sense to block .vbs files from automatically entering your network.
- Dangerous file extensions can be blocked at the Internet gateway device, e-mail server, or e-mail client. A plethora of commercial and open source programs exist to block file attachments at the gateway and e-mail server level. In addition, most antivirus vendors offer an e-mail server antivirus solution.

Install applications to nonstandard directories and ports

- Many malware programs depend on the fact that most people install programs to default directories and on default ports. The risk of exploitation can be minimized by installing programs into nonstandard directories and by using nonstandard ports. Many Unix and Linux exploits rely on the existence of the /etc directory.
- By simply changing the installation folder to something other than /etc, you've significantly reduced the risk of malicious attacks being successful.
- Similarly, instead of installing Microsoft Office to ***C:\Program Files\Microsoft Office***, consider customizing the program during installation to be placed in ***C:\Program Files\MSOffice***. Consider installing Windows into a different folder than the default of ***C:\Windows***.
- Any change from the default setting, even one character, is enough to defeat many automated attack tools. If your application opens and uses a TCP/IP port, see if you can make it communicate on a port other than the default.
- For instance, if you have an extranet web site, consider telling your customers to connect to some other port besides port 80 by using the following syntax in their browser : **http://www.domainname.com:X**
- Where, *X* is the new port number. For example, ***http://www.mydomain.com:801***
- Many web exploits only check for web servers on port 80, so this change would guard against that attack.

1.3.4.9 Secure P2P Services

- Peer-to-peer (P2P) applications, like Instant Messaging (IM) and music sharing, are likely to remain strong attack targets in the future. P2P applications have very limited security and are often installed in the corporate environment without the administrator's authorization.

- They are designed to access files on the end user's computer, which makes the job of stealing those files much easier. Consequently, P2Papplications are seen more as a nuisance than a legitimate service that needs to be secured and managed. However, there are some steps that can be taken to manage P2P applications and minimize their security consequences.
- Firstly, if P2P isn't authorized in the corporate environment, eradicate it. Secondly, ensure that the firewall is configured to explicitly stop P2P traffic as it often uses port 80 as a proxy port and it can be difficult to block P2P traffic by port number alone.
- Possible solution to this is that if the P2P clients connect to servers with a particular IP address or in a particular domain, block the destination at the firewall. Lastly, if the end users insist on using P2P and it is authorized by management, insist on a more secure P2P application, if possible.

1.3.4.10 Make Sure Programmers Program Securely

- SQL injection and buffer-overflow attacks can only be defeated by programmers using secure coding practices.
- Stopping buffer-over flow attacks requires input validation. Several free and commercial tools are available to test the applications for the presence of these attacks and to offer remediation suggestions.
- The IIS Lockdown Tool should be executed on any system running IIS. It works by using templates specifically designed for different web server roles (such as OWA server, public web server and so on).
- The security templates turn off unnecessary features, remove unneeded files and install URL Scan, which filters out many common, malicious URL attacks. If the installation negatively affects the IIS server, it can easily be uninstalled and the original settings restored.

1.3.4.11 Back Up the System

- With the notable exception of stolen confidential information, the most common symptom of damage from malware is modified, corrupted, or deleted files. Worms and viruses often delete files, format hard drives, or intentionally corrupt data.
- Even malware that does nothing intentionally wrong to a system's files is maliciously modifying a system just by being present. Security experts cannot always repair the damage and put the system back to the way it was prior to the exploit. This means it's important to keep regular, tested backups of your system.

- The backup should include all your data files at a minimum and a complete system backup ensures a quicker recovery in the event of a catastrophic exploit event.
- The one caveat to this last piece of advice is to remember that the exploit or hidden malware that damaged your system in the first place could have contaminated your backups and may need to be dealt with prior to putting the system back into production.

1.3.4.12 Implement ARP Poisoning Defenses

Q. 1.3.6 What are the possible ARP poisoning techniques? (Ref. Sec. 1.3.4.12) (5 Marks)

- ARP poisoning attacks are one of the most common and effective threats against network infrastructures (especially wireless networks). They are a form of Man-In-The-Middle (MITM) attack that allows an attacker to intercept and modify network traffic, invisibly.
- Thus, these attacks merit their own special counter measures. There are a few ways an organization can defend against an ARP poisoning attack.
- Defenses include implementing static ARP tables, configuring port rate limiting, or using DHCP snooping with Dynamic ARP Inspection (DAI). The most effective defense is a combination of the latter two methods.

a) Implement static ARP tables

- From a console, if the command arp – a is executed, it will display the ARP table for the system. A quick review of the output shows the IP address and the MAC address associated with the IP address(device).
- This is how the system knows how to route traffic. One of the devices listed is the gateway address. This is the address for the switch where traffic will pass, if the device wants to send information to a device that doesn't exist in its ARP table. A simple ARP request is sent to ask for the information.
- The information is then added to the ARP table of the device. The switch follows the same steps to build its ARP table. This is known as dynamic updating and is used for most devices in an organization.
- A static ARP table implies that instead of using the basic ARP request/reply method, the tables are managed by the organization, essentially hard coded. This helps to prevent an ARP poisoning attack because the main avenue of the attack is cut off.
- The issue with static ARP is the amount of overhead required to keep static ARP tables up to date. Static ARP requires making a manual entry in all other devices in order to properly route traffic through the network.

b) Configure Port Rate Limiting (PRL)

- Another possible solution for defense is port rate limiting (PRL). In this scenario, the amount of traffic passing over a port during a given length of time is monitored. If the configured threshold is tripped, the port closes itself until either it is enabled manually or a specified length of time passes (usually 15 minutes).
- In order to establish an effective threshold, an organization will need to monitor the amount of traffic for a "normal" system over the course of a few weeks. By monitoring traffic correctly, a proper threshold can be set.
- Considering an MITM attack with ARP poisoning works, PRL is a fairly effective defense. ARP poisoning works by moving the traffic of the victim system(s) through the attacker's device.
- If an attack is executed on a port with PRL, the amount of traffic is enough to trip the threshold and thus shut off the port.
- If the port is unusable to an attacker, you have essentially cut off their ability to perform ARP poisoning from that port. It is essentially a "fail closed" scenario for the organization.
- If enabling the port requires manual intervention, this could help alert the organization of something suspicious, especially if it happens on several ports within a short timeframe.
- PRL requires the attacker to do more research within the organization to set a proper threshold.
- A motivated attacker will learn from this experience and perhaps perform a more targeted attack in hopes of circumventing this defense.

c) Use DHCP snooping and dynamic ARP inspection

- The most effective defense against ARP poisoning is to use DHCP snooping with Dynamic ARP Inspection (DAI).
- The basis of this defense is that it drops all ARP reply requests not contained within its table. As with PRL, this defense requires the organization to do some research on its environment before full implementation is executed.
- The organization needs to run DHCP snooping for two to three weeks in order to build a proper table of IP addresses and MAC addresses.
- After it has built that table, it can implement DAI. Once implemented, DAI provides a solid defense against ARP poisoning attacks.

- In this scenario, when the attacker's system tells the switch via ARP reply that his system's MAC address is the victim's MAC address, the switch compares this information with its table and drops the traffic if it doesn't match, thereby cutting off the avenue in which the attacker communicates.

Summary

- This chapter covered the principles that information security practitioners need to know in order to secure technology infrastructures. The CIA triad is perhaps the most well-known model to guide security implementations, with its focus on confidentiality, integrity and availability of data.
- However, there are several other models that focus on other aspects of information security that are also important. Those additional aspects should be taken into consideration when designing a security program.
- Whether you're talking about a network, a single computer, or any environment from any other branch of security, an onion is always better than a lollipop.
- The onion represents a layered security strategy, whereas the lollipop represents a single defense.
- A defense-in depth strategy is better because it requires attackers to break through many different countermeasures. These security layers can be combined and allocated into different areas of a network, known as zones of trust, based on the criticality, risks and exposure of sources located in those zones.
- Attacks can come from automated malicious code or from manual assaults by attackers. There are many countermeasures you can implement on computers to minimize the risk of a successful attack, including securing the physical environment to stop direct attacks by attackers who gain physical control of a device, hardening the operating system to reduce the attack surface, keeping patches updated so that vendor-supplied security fixes are applied, using an antivirus scanner to detect and block malware, using firewall software to control who can get in to a computer and what programs can communicate out, securing network shares to stop worms and attackers from spreading malware, using encryption to preserve the confidentiality of data and securing applications using their built-in security options.
- Reliable backups are also important, so that systems can always be returned to a known good state. Security settings should be automated whenever possible and should be part of a computer security defense plan.

- Finally, ARP poisoning was covered because it's a significant threat in today's networks. Even if all computers are locked down according to best practices, ARP poisoning can be used to take over those computers' network sessions by a Man in the Middle, who would then control all communications.
- Defenses against ARP poisoning include manual configuration of ARP tables, port rate limiting and dynamic ARP inspection.
- Security implementations that solve specific business problems and produce results that are consistent with clearly identified business requirements produce tangible business benefits by reducing costs and creating new revenue opportunities.
- Companies that provide access into their network under control allow employees and customers to work together more effectively, enabling the business.
- Security both prevents unwanted costs and allows greater business flexibility. Thus security creates revenue growth at the same time as controlling losses.
- Security can be thought of in the context of the three Ds : defense, detection and deterrence of which each is equally important. Defense reduces misuse and accidents, detection provides visibility into good and bad activities and deterrence discourages unwanted behaviour.
- A security program that employs all three Ds provides strong protection and therefore better business agility. Strategies are used to manage proactive security efforts and tactics are used to manage reactive security efforts. Together, well designed security strategy and tactics result in an effective, business-driven security program.
- This chapter covered threat definition and risk assessment, which are necessary to focus the security program on the areas that are most important and relevant to the environment you are trying to protect.
- The threat definition process should take into account the various threat vectors that represent the greatest potential harm to your organization's assets. There are many threat sources and targets that need to be considered as part of this process.
- Attacks are one type of threat that can take the form of malicious mobile code, Advanced Persistent Threats and manual attacks.
- Once the threats are identified, risks should be analyzed based on those threats. Each risk is a combination of the threats, exploitation of vulnerabilities and the resulting cost of damage. Based on this analysis, the proper defensive, detective and deterrent controls can then be applied using a layered security strategy (based on the onion model with over lapping and compensative controls) to the most effective results.

1.4 Exam Pack (Review Questions)

Q. 1 Explain the term Security and hence explain Information Security. (Refer Introduction) **(5 Marks)**

☞ **Syllabus Topic : The Importance of Information Protection**

Q. 2 Write short note on importance of information protection. (Refer Section 1.1.1) **(5 Marks)**

☞ **Syllabus Topic : The Evolution of Information Security**

Q. 3 Write short note on Evolution of Information Security. (Refer Section 1.1.2) **(5 Marks)**

☞ **Syllabus Topic : Justifying Security Investment**

Q. 4 What is security benefit? Explain with its benefits. (Refer Section 1.1.3) **(5 Marks)**

☞ **Syllabus Topic : Security Methodology**

Q. 5 What are the basic aspects of security ? OR Explain security methodology. (Refer Section 1.1.4) **(5 Marks)**

☞ **Syllabus Topic : How to Build a Security Program ?**

Q. 6 What are the basic components required to build a security program and hence explain any three ? (Refer Section 1.1.5) **(5 Marks)**

☞ **Syllabus Topic : The Impossible Job**

Q. 7 Write short note on the impossible job. (Refer Section 1.1.6) **(5 Marks)**

☞ **Syllabus Topic : The Weakest Link**

Q. 8 What are weakest links in security measures ? (Refer Section 1.1.7) **(5 Marks)**

☞ **Syllabus Topic : Strategy and Tactics**

Q. 9 What are strategy and tactics ? (Refer Section 1.1.8) **(5 Marks)**

☞ **Syllabus Topic : Business Processes vs. Technical Controls**

Q. 10 Describe business process and technical control. (Refer Section 1.1.9) **(5 Marks)**

☞ **Syllabus Topic : Threat Definition**

Q. 11 Define threat and hence explain threat vectors and threat source and target. (Refer Section 1.2.1) **(5 Marks)**

Q. 12 Explain computer virus, worms and Trojan. (Refer Section 1.2.1.1) **(5 Marks)**

☞ **Syllabus Topic : Types of Attacks**

Q. 13 List the types of attacks and hence explain any four. (Refer Section 1.2.2) **(5 Marks)**

Q. 14 Explain Advanced Persistent Threats (APTs). (Refer Section 1.2.2.3) **(5 Marks)**

Q. 15 Explain Physical, Network-Layer Attacks. (Refer Section 1.2.2.4) **(5 Marks)**

Q. 16 Explain Application-Layer Attacks. (Refer Section 1.2.2.5) **(5 Marks)**

Q. 17 Explain Man-in-the-Middle (MITM) Attacks.(Refer Section 1.2.2.6) **(5 Marks)**

☞ **Syllabus Topic : Risk Analysis**

Q. 18 Explain risk analysis. (Refer Section 1.2.3) **(5 Marks)**

☞ **Syllabus Topic : Secure Design Principles**

Q. 19 Write short note on Secure Design Principle. (Refer Section 1.3) **(5 Marks)**

☞ **Syllabus Topic : The CIA Triad and Other Models**

Q. 20 Explain CIA triad model. (Refer Section 1.3.1) **(5 Marks)**

☞ **Syllabus Topic : Defense Models**

Q. 21 Explain lollipop model and onion model. (Refer Section 1.3.2) **(5 Marks)**

☞ **Syllabus Topic : Zones of Trust**

Q. 22 Describe zone of trust. (Refer Section 1.3.3) **(5 Marks)**

☞ **Syllabus Topic : Best Practices for Network Defense**

Q. 23 List some best practices for network defense and hence explain four practices. (Refer Section 1.3.4) **(5 Marks)**

Q. 24 What are the possible ARP poisoning techniques? (Refer Section 1.3.4.12) **(5 Marks)**

Chapter Ends...

❑❑❑