UNIT 4

Information Security Metrics

Q. 1. What are measurement and metrics?

Ans. Measurement is defined as the process of assigning symbols, usually numbers, to represent an attribute of the entity. Measurements provide a one - time view of specific measurable parameters and are represented by numbers, weight or binary statement.

A metric is defined as a standard of measurement using quantitative, statistical and mathematical analysis. Metrics are produced by taking measurement over time and comparing two or more measurement with pre defined baselines.

Q. 2. What is Infosec metrics? Give the classification of security metrics. Also define Infosec metrics management.

Ans. An Infosec (information security) metric is the application of quantitative, statistical and mathematical analyses to measuring infosec functional trends and workload. A well-defined and implemented metrics can report how well policies, process and control are functioning and whether or not desired performance outcomes are being achieved.

Infosec Metrics Management - Infosec metrics management is the managing of information security program through the use of metrics. It can be used where managerial tasks must be supported for such purposes as supporting the Information system position on budget matters.

The primary process to collect metrics is as follows:

1. Identify each infosec function.
2. Determining what drives that function, for example - labor, (no of people or hour used) policies, procedures, systems, etc.
3. Establish a metrics collection process.

Q. 3. Give model and classification of Security Metrics.

Ans. Conceptually, security metrics model consist of three components:-

1. The object being measured.
2. The security objectives, that is the 'measuring rod' that the object is being measured against.
3. The method of measurement.

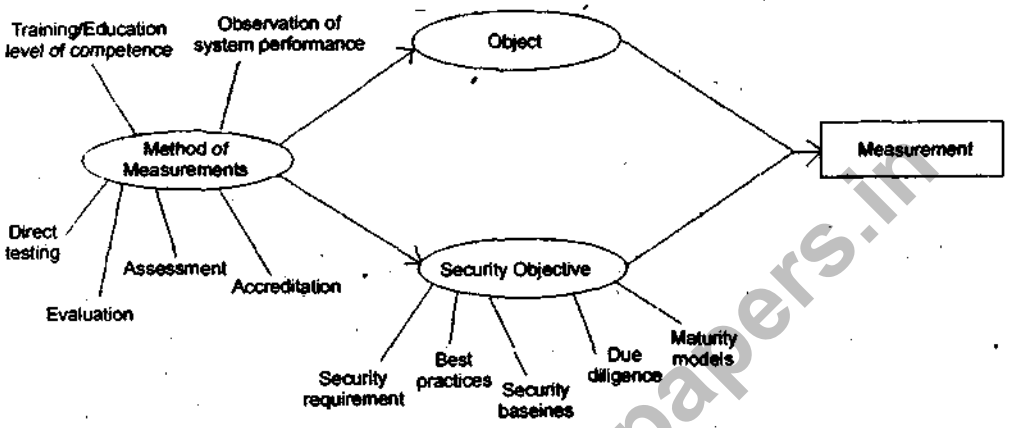
The security objectives are divided into

1. Security requirements such as specifications, standards and control objectives and Common criteria.
2. Best practices.
3. Security baselines.
4. Due diligence, that is, security management based on experience.
5. Maturity models such as infosec assurance capability maturity model (IA-CMM).

Methods of measurement include the following:

1. Direct testing (such as penetration testing)
2. Evaluation

3. Assessment (such as risk/vulnerability assessment)
4. Training /education/level of competence.
5. Observation of system performance such as intrusion detection systems (IDS).



Different types of metrics for security that organizations can focus on can be listed as follows.

1. **Business impact:**
   - Business value gained/lost.
   - Acceptable loss estimate.
2. **Program results:**
   - Timeline of security service delivery
   - Operational results.
3. **Process implementation:-**
   - Level of implementation
   - Implementation totality

Q. 4. Why security metrics are important?

Ans. Security metrics are important because security managers are increasingly turning to security metrics scorecards, hoping to produce business cases for spend and to drive accountability outward to business units. Security metrics - based scorecard present a number of benefits:

1. Identify key risks within the organization
2. Targeting remediation/mitigation action
3. Measuring internal compliance with organizational policy
4. Discovering internal process breakdown
5. Taking advantage of security - related sunk costs

Metrics suitable for business unit scorecards, meet the following criteria:

1. They contain information necessary to support business unit.
2. Business unit behavior directly influences them.
3. All business units contribute data to them.

Q. 5. What are the benefits of using security metrics?

Ans. The benefits of using security metrics are as follows:-

1. Organization can improve accountability for security by deploying ITS metrics.
2. ITS can be created to measure each aspect of the organization's security. For example- result of risk assessment, penetration testing etc.
3. Using the result of metrics analysis, program managers and system owners can isolate the problem.

4. Organization can get the best value from the available resources.
5. ITS metrics can be used as an input into the security audit that organization may want to run with applicable standards such as (ISO)-27001.

Q. 6. What is the need of information security and law?

or

Why the need of information security and law are rising?

Ans. The needs of information security and infosec laws are rising because the first and foremost requirement is to keep data and information system secure. These requirements may stem from public laws (statuettes & regulations) or private arrangement made via contracts.

In its second aspects, infosec law addresses 'liability' that arises from security branches (loop holes) defects in security products or services.

Third and most relevant for today's paradigm, infosec law covers secure electronic commerce (e-commerce), secure e-commerce answers questions such as:

1. How do parties form contacts online?
2. Does the law treat online contracts in the same way as paper contracts under the traditional law?
3. What must a person or business do to authenticate himself, herself or itself to another party online?
4. What must be done to tie an individual or business to an online transaction and hold that party accountable for it?

Q. 7. State the following laws:

1. **IPR law**
2. **Copyright law**
3. **Patent law**

Ans. (i) IPR laws: IPR stands for intellectual property right, which can be defined as rights acquired over a property created with the intellectual effort of an individual.

The property is intangible in nature. IPR is divided into 7 main branches under the TRIP (Trade related aspects of IPR) agreement. These branches are

1. Patents
2. Copyright
3. Trade marks
4. Geographical indication
5. Layout design for IC
6. Design registration
7. Confidential information

(ii) Patent law: Patent law protects the 'device or process' for carrying out an idea; the two critical requirements are - 'the device or process' works in a new and inventive way and that is capable of industrial application. The economic justification for patent law is to encourage inventors, by creating an artificial monopoly for the exploitation of the inventions. Generally patents need to be registered with a central authority.

The patent owners have the exclusive right to make use, or sell the inventions.

(iii) Copyright law: Copyright is a legal concept that gives the creator of original work exclusive rights to it, usually for a limited period of time. In its most general form, it is literally 'the right to copy', but also gives the copyright holder the right to be credited for the work.

In short it gives exclusive right to copy, adopt, distribute and perform that material. However, unlike patent law, the right is not 'exclusive'; therefore, copyright in a work can exist with two different people if it can be proved that each version of the work was developed independently.

There are four main forms of remedies in the event that copyright infringements take place:

1. An injunction to stop the production of further copies.
2. A demand that all copies are surrendered to the copyright owner.
3. Damages for losses suffered by the copyright owner.
4. An account of profits made by the infringer.

Q. 8. Describe legal issues in data mining security.

Ans. Data mining is called knowledge discovery in data bases (KDD), is the process of automatically searching large volumes of data for patterns using tools such as classification, association rule mining, clustering etc.

Example: Hospital Management system, Student Management system etc.

An analysis of laws shows that there are in fact, few legal constraints on government access to commercial data bases. The privacy does not apply to private-sector databases, laws on specific categories on commercial data entities intelligence agencies to access the data.

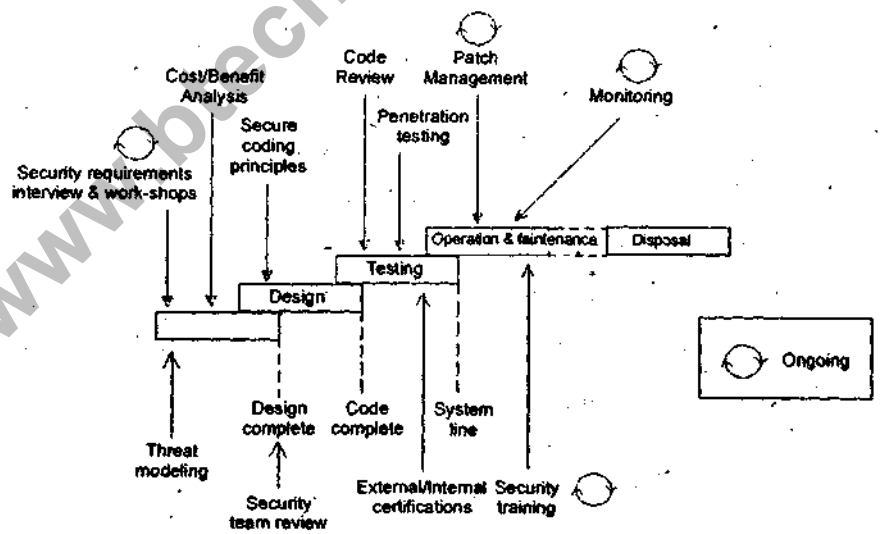
The privacy Act 1974 prevents federal Govt. agencies from disclosing records to any person or to another agency.

Q. 9. Explain the concept of building security into software/system development lifecycle.

or

How do you build security in the early stages of software development lifecycle?

Ans. It is important to appreciate the attention to application system's security starts right from the requirements definition stage. Secure system development lifecycle is depicted below.



1. Software requirement specification communicates the software's required performance and features to the entire team. Example-Clearly starting the level of authentication for each interface [Web, command level and application program interface [API] will prevent developers from making their own assumptions about the level of trust required for the application environment.

2. The next step is classifying the data-By reviewing the data that will be collected or handled by the application and assigning a classification based on their value to the organization's sensitivity and legal requirements, you can ensure security right up front.
3. The development and coding stage is, where the requirements, architecture and design come together, is critical. Developers need to understand application security threats, and must be aware of common coding errors, such as buffer overflows, injection flaws and invalidated inputs that can lead to security vulnerabilities.

Q. 10. Why are computer ethics important? Also discuss some ethical issues related to computer.

Ans. Ethics is a branch of philosophy that deals with what is considered to be right or wrong. As information in cyber space can be accessed globally, with the help of 'computer ethics', There is a need to examine what is right and wrong for computer/internet users. Also, ethics is a set of moral principles that regulate the use of computers. The term computer ethics was first coined by Walter Maner in mid 1970's.

Computers ethics has two parts:

1. The analysis of the nature and social impact of computer technology.
2. The corresponding formulation and jurisdiction of policies for ethical use of such technology.

There are 10 commandments of computer ethics created by Computer Ethics Institute (CEI).

1. You shall not use a computer to harm others.
2. You shall not interfere with other people's computer work.
3. You shall not snoop around other people's computer file.
4. You shall not use a computer to steal.
5. You shall not use a computer to bear false witness.
6. You shall not copy or use proprietary software for which you have not paid (i.e. pirated software)
7. You shall not use other people's computer resources without authorization.
8. You shall not appropriate other people's intellectual output.
9. You shall think about the social consequences of the program you are writing or the system you are designing.
10. You shall always use a computer in ways that insure consideration and respect for your fellow humans.

Q. 11. Explain:

I. Date privacy issues

II. Software privacy issue

Ans. Date privacy issue - Data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information is collected and stored in digital form. Improper or nonexistent disclosure can be the root cause for private issues. Data privacy issue can arise in response to information from a wide range of sources such as:

- Health Care records
- Financial Institutions and transactions
- Residence and geographic records
- Organizational records
- Ethnicity

The challenge in data privacy is to share data while protecting personally identifiable information.

Software privacy issue: Software has the ability to store vast amount of information about individuals. Software can be designed to recognize faces, monitor, e-mail, analyze consumer spending habits, track web surfing and record other pattern and activities. Information tracking software has raised much privacy concern.

Consumer privacy concern: Consumer can have their purchasing habit closely tracked. Web surfing habits are also tracked by corporations to prevent piracy.

Business monitoring employers: Businesses use software to read their employee's email and in some cases employ staff to employee email. Additional, certain words used in emails will activate software's that notifies third parties of email containing those words.

Government software and privacy rights: Law makers have expressed concern over government softwares that allow military, intelligence and law enforcement agencies to recognize pattern indicative of terrorism or criminal activity in personal data and web surfing.

Hackers: They are the people who specialize in unauthorized access of private information stored in computers. Hackers cab share information and techniques that allow them to violate an individual or organization's privacy and security. Hackers are a big concern to law enforcement and the private sector.

Q. 12. Explain Cyber crime. Also, discuss some types of cyber crime.

or

What is Cyber crime? Explain some of its types.

Ans. "Cyber Crime" can be said to be an act of omission, committed on the internet, whether directly or indirectly, which is prohibited by any law for which punishment is provided. In simple language we can say that the unlawful activity (crime) done in which computer/ internet has played any role, is known as Cyber Crime.

Cyber crime can be classified as, Old crimes, committed on or through the new medium of the internet. For example fraud, defamation, harassment, pornography, threats etc.

Types of threats related to cyber crime include: -

1. **Spreading Computer Viruses:** Segments of code that is able to perform malicious acts. Viruses disrupt the normal working of a program, software or a computer.
2. **E-mail Spoofing:** Using someone else's e-mail ID to send e-mails. However, the e-mail in reality has not been sent from that ID which it tends to be coming from. The e-mail Id has only been spoofed. i.e. Fake e-mails.
3. **Hacking:** Out of all Cyber crimes, Hacking is amongst the biggest threats to internet and e-commerce. Hacking refers to breaking into computer systems without permission and stealing important or valuable information.
4. **DoS Attack:** Denial of Service (DoS) attack is used to attack the target system/server with large no. of requests, which it cannot handle and ultimately crashes. It means sending large number of requests to a system generally higher to the capacity which it can handle.
5. **E-mail Bombing :** Sending large number of e-mails to a particular ID/person. i.e. bombing his/her inbox with hundreds or thousands of e-mails together. It sometimes results in crashing the inbox.