LECTURE 7

Objective:

Formal methods help in more precisely determine the requirements, and analyze the information system. This is done in order to prevent or at least identify the security incidents.

Steps:

Step 1 : System Specification

This step includes the abstraction and modeling for a system with a well-defined syntactic and semantic structure.

Step 2: Requirement specification

This step includes security modeling by using models like BLP model in order to represent the security requirements unambiguously.

Step 3: Validation:

This step includes validating the system formally as per the requirements specified in step 2. This can be done by:

Model Checking by searching the satisfiability of the given characteristics of the system in the possible models

Theorem proving (by inference of given system characteristics using syntactical inference rules in theory proving)

Modeling:

- Modeling involves capturing the essential system characteristics and ignoring the irrelevant details and making the abstract representations of system using mathematical entities and concepts.
- Model can be used for mathematical reasoning to prove system properties or predict new behavior
- There are 2 types of models: Continuous and discrete

Advantages of using formal specification:

- Clarifies the system requirements and design
- Clearly mentions the implicit assumptions
- Identifies undocumented or unexpected assumptions
- Expose defects
- Identify exceptions
- Evaluate test coverage

Generating the formal specifications:

- The non-mathematical description of a system such as diagrams, tables, natural language needs to be translated to a formal specification language
- The specification is a concise and precise description of high-level behavior and properties of a system
- Well defined language semantics are needed in order to do the formal deduction of the specification.

Types of formal specification:

Model oriented:

These are based on a model of the system behavior in terms of mathematical objects like sets, sequences, etc.

Examples: Statecharts, SCR(SCR (Software Cost Reduction), VDM (Vienna Development Method), Petri nets, automate theoretic models

Property oriented:

These are based on a set of properties which are sufficient to describe the system behavior in terms of axioms, rules, etc.

Examples: Algebraic semantics, temporal logic

Role of Formal Method in System Design and Engineering

The use of Formal methods in System Design and Engineering is motivated by the expectation that performing appropriate mathematical analysis can contribute to the reliability and robustness of an information system design.

Formal specification of an information system may be used as a guide while the system is being developed

- If the formal specification is in **operational semantics,** the observed behavior of the system can be compared with the behavior of the specification.
- If the formal specification is in axiomatic semantics, the pre-conditions and post-conditions of the specification may become assertions in the executable code

Bell-LaPadula (BLP) Model

BLP Model is used to enforce access control in information systems. It is built on the concepts of a state machine with allowable states in a computer system.

BLP Model defines 2 MAC rules and 1 DAC rule with 3 security properties:

- **Simple Security property –** a subject (e.g. User) at a given security level may not read an object (e.g. file) at a higher security level (no read-up)
- *** Property (Star Property)** - subject at a given security level must not write to any object at a lower security level (no write-down)
- subject at a given security level must not write to any object at a lower security level (no write-down)

Limitations of Formal Methods:

- The developer working on formal methods requires sound mathematical knowledge
- It is possible that we need to use different formal specifications methods to represent different aspects of design.
- Formal methods are useful for consistency checks, but it cannot guarantee the completeness of specification.

LECTURE 10
Authentication:

- Authentication is validation of a user's identity .
- Four general ways for authentication:
  - What an entity has (badge, ID card)
  - What an entity knows (passwords, secret information)
  - Who an entity is (fingerprints, retinal characteristics)
  - Where an entity is (in front of a particular terminal)

- Passwords: A password is information associated with an entity that confirms the entity's identity .
- Password storage: ■ Store in file ■ Store in encrypted file ■ Store with one-way hashes
- Password Attacks:
  - Types of Password Attacks:[Paraphrase this section]
    1. Phishing:
       Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device. We highlight several examples on the OneLogin blog.
- Countermeasures:

  Check who sent the email
  Double check with the source
  Check in with your IT team

2. Man-in-the-Middle Attack:

   Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords. If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle. Similarly, in 2017, Equifax removed its apps from the App Store and Google Play store because they were passing sensitive data over insecure channels where hackers could have stolen customer information.
- Countermeasures:

  Enable encryption on your router.
  Use strong credentials and two-factor authentication.
  Use a VPN

3. Brute Force Attack:

   If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.
- Counters:

-Use a complex password. The difference between an all-lowercase, all-alphabetic, six-digit password and a mixed case, mixed-character, ten-digit password is enormous. As your password's complexity increases, the chance of a successful brute force attack decreases.

-Enable and configure remote access.

-Require multi-factor authentication. If multi-factor authentication (MFA) is enabled on your account, a potential hacker can only send a request to your second factor for access to your account.

4. Dictionary Attack:

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

- Counters:

-Never use a dictionary word as a password.

-Lock accounts after too many password failures.

-Consider investing in a password manager. Password managers automatically generate complex passwords that help prevent dictionary attacks.

5. Credential Stuffing:

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

- Counters:

-Monitor your accounts.

-Regularly change your passwords. The longer one password goes unchanged, the more likely it is that a hacker will find a way to crack it.

-Use a password manager. Like a dictionary attack, many credential stuffing attacks can be avoided by having a strong and secure password.

1. Keyloggers:

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

- Counters:

-Check your physical hardware. If someone has access to your workstation, they can install a hardware keylogger to collect information about your keystrokes.

-Run a virus scan. Use a reputable antivirus software to scan your computer on a regular basis. Antivirus companies keep their records of the most common malware keyloggers and will flag them as dangerous.

- Countermeasures for those attacks: Mentioned in the above section…

- One-time passwords: Password that can be used exactly once
  - Generation mechanisms:
    1. Time-synchronization: Using a synchronized time between client and server. Example: Let tx be the current synchronized time, f(tx)=px The passwords in the order of use are p1 , p2 … px …
    2. Challenge-response: Using a challenge from server. Example: Let ci be the current challenge from server, f(ci) = pi. The passwords in the order of use are p1 , p2 …, pi , … pn
    3. Hash chain: Using a chain of hash functions . Example: h is the hash function, p is the OTP and an initial seeds h(s)=p1 , h(p1)=p2 , …, h(pn-1)=pn The passwords in the order of use are pn , pn-1 , …, p2 , p1

- Biometric Authentication:■ Fingerprints ■ Voices: speaker verification or recognition ■ Eyes: irises ■ Faces: image, or specific features ■ Keystroke dynamics: keystroke intervals, pressure, duration of stroke, where key is struck ■ Combinations of the above
  - Effectiveness of biometrics:
    - False reject rate: Rate at which supplicants (authentic users) are denied from accessing authorized areas due to a failure detected by biometric device (**Type I error**).
    - False accept rate: Rate at which supplicants who are not legitimate users are allowed access to systems or data due to failure detected by biometric device (**Type II error**).
    - Crossover error rate (CER): Level at which the number of false rejections equals the number of false acceptances, (equal error rate). This is the most common and important overall measure of the accuracy of biometric systems.
  - Usefulness of a biometric depends on the acceptability and effectiveness of the biometric.

- Access Control List:
  - A variant of the access control matrix, Store each column with the object it represents.
  - ACL(file 1) = {(user 1, RWO), (user 2, R)}
  - ACL(file 2) = {(user 1, R), (user 2, RO)}
  - ACL(file 3) = {(user 1, RWXO), (user 2, R)}
  - ACL(file 4) = {(user 1, W), (user 2, RWXO)}
- Capabilities:
  - Another variant of the access control matrix
  - Store each row with the subject it represents
  - CAP(user 1) = {(file 1, RWO), (file 2, R), (file 3, RWXO), (file 4, W)}

    - CAP(user 2) = {(file 1, R), (file 2, RO), (file 3, R), (file 4, RWXO)}
- ACL vs Capabilities: Two questions ■ Given an object, which subjects can access it, and how? ■ Given a subject, which objects can it access, and how?
- Access Control Models: [Paraphrase this section]

    Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization—that is, information systems, restricted areas such as computer rooms, and the entire physical location. Access control is achieved through a combination of policies, programs, and technologies. To understand access controls, you must first understand they are focused on the permissions or privileges that a subject (user or system) has on an object (resource), including if a subject may access an object and how the subject may use that object

- Types of Access Control:
    - Discretionary Access Control (DAC): Restricting access to objects based on identity of subjects and/or groups to which they belong

        Controls that are implemented at the discretion or option of the data user. provide the ability to share resources in a peer-to-peer configuration that allows users to control and possibly provide access to information or resources at their disposal. The users can allow general, unrestricted access, or they can allow specific people or groups of people to access these resources. For example, a user might have a hard drive that contains information to be shared with office coworkers. This user can elect to allow access to specific coworkers by providing access by name in the share control function.

- Mandatory Access Control (MAC): Restrict access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity
    - An access control approach whereby the organization specifies use of resources based on the assignment of data classification schemes to resources and clearance levels to users. MAC is an example of an LBAC approach
    - Mandatory access controls offer users and data owners little or no control over access to information resources. MACs are often associated with a data classification scheme in which each collection of information is rated with a sensitivity level. This type of control is sometimes called lattice-based access control.

- Role based access control (RBAC): To facilitate the security management in multi-user , multi-application systems
    - An example of a nondiscretionary control where privileges are tied to the role a user performs in an organization, and are inherited when a user is assigned to that role. Roles are considered more persistent than tasks. RBAC is an example of an LDAC. subject attribute See attribute.
    - Minimum requirements: ■ Associate roles with each individual. ■ Each role defines a specific set of operations that the individual acting in that role may

perform. ■ An individual needs to be authenticated, chooses a role assigned to the individual, and accesses information according to operations needed for the role.

- RBAC0 : the base model indicating that it is the minimum requirement for RBAC
- RBAC1 : include RBAC0 and support of role hierarchy ■ Inheritance among roles ■ Inheritance of permission from junior to senior roles
- RBAC2 : include RBAC0 and support of constraints ■ Enforces high-level organizational policies, such as mutually exclusive roles
- RBAC3 : combine RBAC1 and RBAC2

○ Situation-aware access control model: incorporates situation-awareness into RBAC

Situational awareness or **situation awareness** (SA) is the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status

From <https://en.wikipedia.org/wiki/Situation_awareness>

Situation awareness has been recognized as a critical, yet often elusive, foundation for successful decision-making across a broad range of situations, many of which involve the protection of human life and property, including law enforcement, aviation, air traffic control, ship navigation,[4] health care,[5] emergency response, military command and control operations, transmission system operators, self defense,[6] and offshore oil and nuclear power plant management.[7] Lacking or inadequate situation awareness has been identified as one of the primary factors in accidents attributed to human error.

From <https://en.wikipedia.org/wiki/Situation_awareness>

■ Example: only when the user with the role of a teacher in the Smart Classroom during the class time, the user can create a group discussion

LECTURE 11
Administrative Security Controls:

- Logging : Recording of events and statistics to provide information about system use and performance
- Auditing : Analysis of log records to present information about the system in a clear and understandable manner

  Accountability, also known as **auditability**, ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Accountability is most often accomplished by means of system logs, database journals, and the auditing of these records.
- What happened?
- When did it happen?
- Who did it?
- What went wrong?
- Who had access to key information?

- Auditing systems have 3 components:
  1. Logger: collects data
  2. Analyzer: analyzes the collected data
  3. Notifier: reports the results of analysis

- **Logger**: ■ The type and quantity of information decided by system or program configuration parameters ■ Information may be recorded in binary or human-readable form or transmitted directly to an analysis system
- Auditable events: ■Login ■Logoff ■Operating system changes ■User-invoked operating system commands ■User-invoked applications ■Read of data ■Creation of objects ■Network events , etc.

- **Analyzer**: ■ Input from logger and analyzes it. ■ Results of analysis may lead to changes in the data being recorded, or detection of some events or problems, or both.
  - Example: Used by an intrusion detection system

- **Notifier:** ■ Informs the analyst and other entities of the results of the audit. ■ Actions may be taken in response to these results.
  - Example: When a user's failed login attempts 3 times, the audit system will invoke the notifier, which will report the problem to administrator and disable the account.

- Audit Team:
  - Federal or State Regulators - Certified accountants, CISA from Dept. of Justice, etc.
  - Corporate Internal Auditors - Certificated accountants, CISA.
  - Corporate Security Staff - Security managers, CISSP, CISM.
  - IT Staff and needed expertise varies

- [Paraphrase following definitions CISA, CISM, CISSP, ISACA]

- **CISA** - Certified Information Systems Auditor

  Certified Information Systems Auditor (CISA) refers to a designation issued by the Information Systems Audit and Control Association (ISACA). The designation is the global standard for professionals who have a career in information systems, in particular, auditing, control, and security. CISA holders demonstrate to employers that they have the knowledge, technical skills, and proficiency to meet the dynamic challenges facing modern organizations.

From <https://www.investopedia.com/terms/c/certified-information-systems-auditor.asp>

- **CISM** - Certified Information Systems Manager
  - The CISM credential is geared toward experienced information security managers and others who may have similar management responsibilities. The CISM can assure executive management that a candidate has the required background knowledge needed for effective security management and consulting. This exam is offered annually. The CISM examination covers the following practice domains described in the ISACA 2014 Exam Candidate Information Guide: 1. Information Security Governance (24 percent): Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly. 2. Information Risk Management and Compliance (33 percent): Manage information risk to an acceptable level to meet the business and compliance requirements of the organization. 3. Information Security Program Development and Management (25 percent): Establish and manage the information security program in alignment with the information security strategy. 4. Information Security Incident Management (18 percent): Plan, establish, and manage the capability to detect, investigate, respond to, and recover from information security incidents to minimize business impact.

- **CISSP** – Certified Information Systems Security Professional
  - The CISSP certification is considered the most prestigious for security managers and CISOs. It recognizes mastery of an internationally identified Common Body of Knowledge (CBK) in information security. To sit for the CISSP exam, the candidate must have at least five years of direct, full-time experience as a security professional working in at least two of the 10 domains of information security knowledge, or four years of direct security work experience in two or more domains. The candidate must also have a fouryear college degree. The CISSP exam consists of 250 multiple-choice questions and must be completed within six hours.
  - It tests candidates on their knowledge of the following 10 domains:

    ● Access control ● Business continuity and disaster recovery planning ● Cryptography ● Information security governance and risk management ● Legal issues, regulations, investigations, and compliance ● Operations security ● Physical (environmental) security ● Security architecture and design ● Software development security ● Telecommunications and network security

- **ISACA** (Information Systems Audit and Control Association)
    - ISACA is an international professional association focused on IT (information technology) governance. On its IRS filings, it is known as the Information Systems Audit and Control Association, although ISACA now goes by its acronym only. ISACA currently offers 8 certification program as well as other micro-certificates

From <https://en.wikipedia.org/wiki/ISACA>

- Certifications offered by ISACA:
    - Certified Information Systems Auditor (CISA,1978)[18]
    - Certified Information Security Manager (CISM, 2002)[18]
    - Certified in the Governance of Enterprise IT (CGEIT, 2007)[18]
    - Certified in Risk and Information Systems Control (CRISC, 2010)[18]
    - Cybersecurity Practitioner Certification (CSX-P, 2015)[19]
    - Certified Data Privacy Solutions Engineer (CDPSE, 2020)[20]
    - Information Technology Certified Associate (ITCA, 2021)[21][22]
    - Certified in Emerging Technology (CET, 2021)

- **<u>Audit Process:</u>**
    1. Planning Phase

        ■ Entry Meeting ■ Define Scope ■ Learn Controls ■ Historical Incidents ■ Past Audits

        ■ Site Survey ■ Review Current IA Policies ■ Questionnaires ■ Define Objectives ■ Develop Audit Plan / Checklist
2. Testing Phase

    ■ Evaluate Audit Plan:

    ■What data will be collected? ■How/when the data will be collected? ■Site employees' involvement? ■Other relevant questions?

    ■ Data Collection:

    ■ Based on scope/objectives

    ■ Types of Data:

    ■ Activities involving physical security ■ Interview staff ■ Vulnerability assessments ■ Access control assessments
3. Reporting Phase

    ■ Exit Meeting - Short Report:

    ■ Immediate problems ■ Question & answer for site managers ■ Preliminary findings ■ Does NOT give in-depth information

    ■ Long Report - After Going Through Data:

    ■ Objectives/scope ■ How data was collected ■ Summary of problems ■ In-depth description of problems ■ Glossary of terms ■ References

    ■ Any computer misuse or abuse should be reported, and law enforcement may be involved if needed. x`

LECTURE 12

IA Policy:

High level statements of goals of procedures for information assurance:

1. Define what actions are required, and which are permitted
2. Not guidelines
3. Top level policies are often determined by management with significant input from IT personnel and represent corporate goals and principles
4. Important to distribute policies to those responsible for following the policies and/or implement the policy enforcement.

What is Policy and enforcement mechanism:

1. Every IA policy statement should have an enforcement mechanism
   - Critical to make employees aware of policies affecting their actions, and their violations may result in reprimand, suspension, or dismissal
   - The fact that individual employees have been made aware of should be documented. Example, an employee signs a statement that the employee has attended a training session.

What is a Security Policy?

1. A security policy sets the context in which we can define a secure system.

What is secure under a policy may not be secure under a different policy

Properties / Special Features of IA Policy:

1. IA policies indicating the organization is aware of proper operations against:
   a) Disregard for public laws, such as institutional violation of copyright laws, and violation of privacy laws
   b) Negligence
   c) Failure to use measures commonly found in other "like" organizations
   d) Failure to exercise due diligence by computer professionals (computer malpractice)
   e) Failure to enforce policies

Steps for defining IA Policy:

- Step 1: Secure strong management support
- Step 2: Gather key data
  - Relevant policies
  - Relevant statutes
  - Research on what other organizations are doing
- Step 3: Define framework
  - Determine overall goal of policy statement
  - List areas to be covered
  - Start with basic essentials and add additional areas as required

- Step 4: Structure effective review, approval, implementation, and enforcement procedures
  - Determine who need to coordinate and get them involved early
  - Know who are going to approve the policy and ensure they understand why the organization needs the proposed IA policy
  - Cross reference with HR policies Establishing IA Policies (cont.)
- Step 5: Perform risk assessment/analysis or audit.
- Step 6: Make sure each policy is written in same style as existing policies

Policy Areas:

1. Confidentiality Policies
   a. Prevent unauthorized disclosure of information
   b. Identify those states in which information leaks to those not authorized to receive it
   c. Must handle dynamic changes of authorization, and hence it includes a temporal element

2. Integrity Policies
   a. Identify authorized ways in which information may be altered and entities authorized to alter it.
   b. Describe conditions and manner in which data can be altered

3. Administrative Security Policies
   a. Typically exist before a system development process
   b. Usually focus on responsibilities of all members within IA team, and have legal implications.
   c. Access Control Policies
   d. Decide who can access what information under what conditions
   e. Authorize a group of users to perform a set of actions on a set of resources
   f. Ensure "separation of duty" and "least privilege

4. Audit Trails and Logging Policies
   a. Define rules on how the system behavior will be recorded
   b. Audit trails are usually continuous record about routine activities
   c. Logs are usually event-oriented record
   d. Essential when something bad happened since these records will help staff know who/what caused the problem

5. Documentation Policies
   a. Define rules about
   b. What kinds of information should be documented?
   c. Who can modify the documents?
   d. Under what situations can some of the documents be disclosed? and to whom?
   e. Important to ensure privacy and integrity of the system

6. Evidence Collection and Preservation
    a. Define rules about computer incident investigation:
    b. What information should be collected and how to collect it?
    c. How to store collected information to best present it later in a court?
    d. Computer forensics always conflict with personal privacy and the policies should clearly draw the line

7. Information Security Policies
    a. Set forth mechanisms by which information stored on organization's information systems and utilized by organization's employees is secured and protected
    b. State rights and obligations of organization to manage, protect, secure, and control various information that could be accessed through organization's information system

8. Information Security Policies (cont.)
    1. Help maintain data integrity and accuracy, and provide authorized individuals timely and reliable access to needed data. Also ensure that unauthorized individuals are denied access to computing resources or other means to retrieve, modify or transfer information
    2. Ensure organization to meet its record-keeping and reporting obligations as required by laws and to comply with various statutes and policies protecting rights and privacy of individuals

9. Personnel Security Policies
    a. Define rules to do background checking and screening before hiring
    b. Make agreement with employees before they start working
    c. Reduce risks of human errors, theft, fraud or misuse of facilities
    d. Ensure that users are aware of information security threats and concerns, and are equipped to support oganization's security policies in their normal work

<IA POLICY EXAMPLE - PREPARE IT FROM INTERNET - FOR YOURSELF>

LECTURE 13

1. What is Threat?

A threat is a potential occurrence that can have an undesirable effect on the system assets or resources

2. What is Vulnerability?

A vulnerability is a weakness that makes a threat to possibly occur

3. What is Risk?

a. A risk is a potential negative event that may affect the successful operations of a system
b. A risk is not necessarily an ongoing problem

4. **Common threat Examples**:

1. Human errors or failures
2. Compromises to intellectual property
3. Trespass
4. Information extortion
5. Sabotage or vandalism
6. Theft
7. Software attacks
8. Forces of nature
9. Deviations in quality of services
10. Hardware failures or errors
11. Software failures or errors
12. Technological obsolescence

5. Categories of Vulnerabilities:

1. Probabilistic vulnerabilities
   - Caused by hardware failures, human actions, and information problems in the operational environment
2. Algorithmic vulnerabilities
   - Caused by design and implementation errors introduced during system development, including both software and hardware

6.. Cost Benefit Analysis:

a. Infeasible or sometimes impossible to implement an extremely secure system
b. Helps identify risks which will most likely occur, and cause severe damages if occur
c. Acceptable risks: Some risks are always there (residual risk), but they are highly unlikely become problems, or they can easily be contained and solved if becoming problems.
d. Needed to allocate limited resources to most needed area

7.. Risk Analysis:

A process to systematically identify assets, threats, and (potential) vulnerabilities in a system, and to address:

a. Which threats present danger to your assets?
b. Which threats represent the most danger to organizations ‘sensitive information?
c. How much would it cost to recover from attack?
d. Which threat requires greatest resources to prevent?

Risk Rating = V*L*(1-P+U)
where
a. V: The value of the information asset
b. L: The likelihood of the occurrence of a vulnerability
c. P: The percentage of the risk mitigated by current controls
d. U: The uncertainty of current knowledge of the vulnerability

8.. Risk Analysis Example:

Information asset A has one vulnerability

i. The value of A is 50
ii. The likelihood of the vulnerability is 0.1
iii. Has no control (not addressed in risk management)
iv. Assumptions and data are estimated 90% accurate

Information asset B has two vulnerabilities

a. The value of B is 100
b. The likelihood of vulnerabilities #2 and #3 are 0.5 and 0.1
c. Current control addresses 50% of the risk of vulnerability and 0% of the risk of vulnerability.
d. Assumptions and data are estimated 80% accurate

9.. Controls:

Countermeasures for vulnerabilities

Deterrent controls discourage violation and reduce likelihood of deliberate attacks

a. Sanctions built into organizational policies, and punishments imposed by legislation.
b. Preventive controls stop attempts to exploit vulnerabilities
    i. Segregation of duties, proper authorization, adequate documents, proper record keeping, physical controls

c. Detective controls discover attacks and trigger preventive or corrective controls
    i. Firewall logs, inventory counts, input edit checks, checksums, message digests, intrusion detection

d. Corrective controls reduce the effect of an attack
    i. Virus quarantine, firewall rule reconfiguration

e. Recovery controls restore lost computer resources or capabilities from security violations

   i. Business continuity planning, disaster recovery plans, backup

10.. Risk Management:

1. Preventing risks from becoming problems

How to deal with risks identified in risk analysis?

a. Old philosophy: risk avoidance
   i. Do whatever you can to avoid risks
b. Current philosophy: risk management
   - Understand risks
   - Deal with them in cost-effective manner
c. Choices for each risk:

   1. Risk acceptance: tolerate those risks with low impact or rare occurrence: Risk acceptance can be established after the organization has done the following:
      d. Determine the level of each identified risk
      e. Assess the probability of each type of potential attacks
      f. Estimate potential damage from each type of attack
      g. Perform cost-benefit analysis on reducing each type of risks
      h. Evaluate controls using appropriate type
      i. Decide that the particular function, service, information, or asset did not justify the cost for protection

   2. Risk reduction (risk mitigation)
      Mitigation: Attempting to reduce impact caused by exploitation of vulnerability through planning and preparation

      a. Incident Response Plan: Actions and organization takes during incidents (attacks)
      b. Disaster Recovery Plan: Preparation for recovery if a disaster occurs; strategies to limit losses before and during disaster; stepwise instructions to regain normalcy
      c. Business Continuity Plan: Steps to ensure continuation of overall business when the scale of a disaster exceeds the Disaster Recovery Plan's ability to restore operations

   3. Risk transfer (to another entity): let others handle the risk

d. Typically use a combination of acceptance, reduction, and transfer for different risk

11.. Risk Management Strategies:

1. When a vulnerability exists: Implement security controls to reduce likelihood of a vulnerability being exploited
2. When a vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent occurrence.
3. When attacker's cost is less than his potential gain: Apply protection techniques to increase attack's cost.
4. When potential loss is substantial: Apply design principles, architectural designs, and technical and nontechnical protections to limit extent of attack, thereby reducing potential loss

12.. Risk Management Process:

1. Step 1: System characterization
   a. Input: hardware, software, system interfaces, system mission, people, data information
   b. Output: system boundary, system functions, system and data criticality and sensitivity
2. Step 2: Threat identification
   a. Input: attack history, data from intelligence agencies or mass media
   b. Output: threat statement
3. Step 3: Vulnerability identification
   a. Input: prior risk assessment reports, audit comments, security requirements, security test results
   b. Output: list of potential vulnerabilities
4. Step 4: Control analysis
   a. Input: current controls, planned controls
   b. Output: evaluation results of current and planned controls

5. Step 5: Likelihood determination
   a. Input: threat-source motivation, threat capacity, nature of vulnerability, current controls
   b. Output: likelihood rating
6. Step 6: Impact analysis
   a. Input: mission impact analysis, asset criticality assessment, data criticality and sensitivity
   b. Output: impact rating

7. Step 7: Risk determination
   a. Input: likelihood of threat exploitation, magnitude of impact, adequacy of planned or current controls
   b. Output: risks and associated risk levels

8. Step 8: Control recommendations and improvements
   a. Output: recommended controls and improvements

9. Step 9: Results documentation
    a. Output: A set of documents, including risk identification, assessment, cost effective evaluation, suggested control list.

A well-documented risk management process at one phase, which is also the starting point for the analysis at the next phase

10. Step 10: System monitoring:
    a. System and environment changed: Hardware expanded or upgraded, software updates, mission goal changed, etc.
    b. Performance: How many possible attacks have been prevented by controls; any failures or unwanted outcome, etc.

Restart the whole process from Step 1 again:

a. Periodically as part of system maintenance procedure
b. When system configuration is changed, it may generate some new risks not covered during the last risk management process
c. When some controls fail to prevent the risk from turning into attacks

LECTURE 14

IA certification:
Comprehensive eval of security features.
IA accreditation:
DAA approved IT systems with a particular security mode at an acceptable level of risk

Two Key players
DAA, CA

1. DAA Designated approving authority - takes responsibility for operating a system or network with any risk involved
2. CA Certification authority - Issues certificate for a particular design and implementation

C & A process - Certification and accreditation process that addresses the security threats and vulnerabilities

Phase 1: Definition:

- Defines the mission, system funcs, requirements, info category, and classification
- Prepare system arch desc
- Identifies the C & A roles and responsibilities
- Drafts the C & A document SSAA (system security authorisation and agreement)

Phase 2: Verification:

- Life cycle management, security req validation procedures, vulnerability eval

Phase 3: Validation:

- Security test and eval, penetration testing, compliance eval, system management, contingency plan, site accreditation, risk management, certification report for accreditation, declaration of accreditation generation, exception handling

Phase 4: Post Accreditation:

- Review config and security management of the system
- The changes of the system should be approved by DAA and CA.
- Find out whether the changed system will still follow the organisation's mission and arch
- If the changes are approved, the SSAA doc will be invalidated and the process will repeat again or else it will continue
- Risk management review - acceptable level of risk must be maintained.
- Compliance validation for any config changes to the system
- Maintain documentation, Monitor compliance

LECTURE 15

Why need IA management?

1. Many managers overlook IA since it is not directly related to their revenue. Need IA management for that.
2. The IA management staff will persuade the senior managers that, even though IA has a price tag, it has return in the form of saving cost for the damages due to info lost or misused.
3. Outsourcing can be used but it has more threats and vulnerabilities.

IA Management Personnel

- **Information Systems Security Officer (ISSO)** –

    1. Responsible to Designated approving authority.
    2. Ensures that security of an information system is implemented properly and throughout its entire life cycle

- **Operation Security (OPSEC) Manager**

    1. Responsible to Information Systems security officer
    2. Prevents sensitive information from being available to potential adversaries

- **System Manager**

    1. Responsible for proper operations and management of classified and unclassified Automated Information System (AIS).
    2. Supervises system staff in implementing AIS security policies, provides advice, and supports to ISSO on AIS security issues.

- **Program or Functional Manager –**

    1. Determines which users have verified needs to access their applications, along with the system managers
    2. Responsible for informing ISSO of any security incidents related to the application or the users of the application.

- **Communication Security (COMSEC) Custodian –**

    1. Responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account.

- **Telecommunications Officer –**

    1. Responsible for receipt, transfer, accounting, safeguarding telecommunication processes in organization

Security Review and Testing

Conducted throughout system life cycle.
Common Processes:

1. Review security policies, documents, patches and updates,
2. Develop security matrix summarizing threats and protected assets
3. Review audit capability and use
4. Run analysis tools
5. Correlate all information
6. Develop reports
7. Make recommendations to correct problems

IDENTFYING WEAKNESS IN SYSTEM

- VULNERABILITY SCANNING –
  1. Scan for unused ports, unauthorized software
- DISCOVERY SCANNING –
  1. Inventory and classification of information on OS and available ports,
  2. Identification of running applications to determine device function.
- Workstation Scanning –
  1. Make sure standard software configuration is current with latest security patches
  2. Locate unauthorized software
- Server Scanning –
  1. Make sure that software stored on server is updated with latest security patches
  2. Locate uncontrolled or unauthorized software
- Port Scanning –
  1. Scan various active ports used for communication (TCP/UDP)
  2. Stealth scans: also called spoofed scans
- Vulnerability Testing –
  1. False positives and false negative
  2. Heavy traffic

3. System crash
4. Unregistered port numbers

Methods to Promote Awareness –

1. **Periodic awareness sessions** to orient new employees and refresh senior employees which are direct, simple, and clear
2. Live/interactive presentations thorough lectures and videos.
3. Publishing/distributing posters, company newsletters
4. Incentives: awards and recognitions for security- related achievement
5. Reminders

Training –

Training often held in specific classroom or through one-on-one training

InfoSec Examples –

1. *Security-related job training* for operators and specific users
2. *Awareness training* for specific departments or personnel groups with security-sensitive positions
3. ***Technical security training*** for IT support personnel and system administrators
4. ***Advanced InfoSec training*** for security practitioners and auditors
5. ***Security training*** for senior managers, functional managers

Evaluation for Functionality and Assurance

1. A process in which the ***evidence for assurance*** is gathered and analyzed against requirements for functionality and assurance.
2. Can result in a measure of ***trust of an information system.*** A system is trusted if it has been shown to ***meet users' security requirements under specific conditions***
3. Trust is based on ***assurance evidence***
4. An evaluation methodology to determine whether the ***security requirements*** of an information system are satisfied based on assurance evidence.
5. A ***measure*** of the evaluation result (called a level of trust) indicating how ***trustworthy*** the product or system is

Different Types of Criteria –

1. Trusted Computer Based System Evaluation Criteria (TCSEC) –
   1. Developed in 1983-1999 by DoD Also known as the ***Orange Book***
   2. Emphasis on ***confidentiality***, especially protection of government classified information
   3. Limitations:
      1. Focus on security needs of U.S. government and military
      2. ***Not address integrity, availability and others requirements critical to business applications***

2. Information Technology Security Evaluation Criteria (ITSEC) –
   1. Developed in 1991-2001 by European Union
   2. ITSEC emphasizes ***integrity and availability***
   3. **Impact**:
      1. Can be used to evaluate any kinds of products or systems
   4. **Limitations**
      1. Considered technically weak compared to TCSEC
      2. Not used in Canada and US

3. Federal Criteria (FC) –
   1. Developed by NIST and NSA
   2. FC never completed (the last draft version was released in 1992), and supplanted by ***Common Criteria*** in 1998
   3. Many ideas of FC were adopted by the Common Criteria.
   4. The concept of ***protection profile (PP)***, which is an abstract specification of the security aspects of an IT product
   5. The concept of ***profile registry***, which is a collection of FC-approved protection profiles available to public for general use

4. Common Criteria (CC) -
   1. Developed by Canada, France, Germany, Netherlands, United Kingdom and United States, starting 1998
   2. An ***international standard***, also known as ***ISO 15408***
   3. Combines best features of TCSEC, ITSEC and FC
   4. Provides a common language and structure to express both security functional requirements and security assurance requirements
   5. Protection profile used in CC may not be as strong as TCSEC

LECTURE 16

Outsourcing: Delegating business processes/services to third party providers
Examples:

1. Cloud Computing
2. Software dev
3. other hardware services
4. COTS(Commercial off the self) items

Benefits of Outsourcing

1. Reduce cost
2. Reduce time
3. Expertise and skilled services milte hai
4. Concentration more on business

IA Challenges in Outsourcing

1. Risk analysis and mitigation of risk is difficult
2. No control over the outsourced material
3. The security policies might create a difference of opinion b/w client and provider
4. Risk to property
5. Outsource providers may not follow clients standards and laws
6. The providers may not document all the activities in proper format

COTS based system

- Companies, orgs, govt use COTS to build systems
  - eg: commercial dbms and web server to build a website
- Benefits of COTS
  - Reduce development cost and time
  - Proven to work
  - Technical support from vendors
- Risks for COTS
  - Difficult to verify security of these items
  - this software is more attractive for attackers
  - more info on security vulnerabilities is available
  - more to gain by attacking COTS products
  - vendors have very limited liability
  - very generic components
  - DoD agencies involved DISA, JITC

- Mitigating risks/reducing risks for COTS
  - identify all the components that will be used
  - understand the business goals
  - identify the sensitive info that is in the system
  - security mechanisms that will be required to protect the sensitive info
  - the connection b/w COTS and the customised comps are to be understood

- Access of COTS products should be controlled
- Security related problems and their fixes should be asked to the vendor
- History of security related problems and how frequently vendor fixes these problems factor towards the components to be used in COTS items
- Engage with user, security community and experts and look for certification

Open-Source software (OSS)

software that is freely available to public for redistribution, modification and examination

Examples of OSS

- Apache HTTP server
- GNOME
- GNU compiler collection
- KDE
- Mozilla
- Firefox
- Ruby
- Hyperledger
- Ethereum
- MySQL
- Open office.org
- PHP

Characteristics of OSS dev

- Collaborative dev
- Sharing ideas, tech, expertise
- peer reviews
- Better quality and higher reliability
- Low dev cost
- users help fix bugs - recognised as co developers
- Early releases, frequent integration
- multiple versions with diff features
- Beta versions with risks and vulnerabilities but with more features
- Stable versions with fewer features but less bugs
- Modular structure

Open-Source Definition:

- Free Redistribution
    - License will not interfere from distributing the software as a component to another software
    - No royalty fees is required
- Source Code
    - The source code must be included and distribution must be allowed in compiled and source code format
    - If the source code is not distributed, it should be available with a decent cost associated to it.

    - Source code must be in a human readable format
- Derived works
    - Can use derived works in the source code and it is allowed under the same license
- Integrity of Source code
    - if the source code has patch files attached during distribution, then a modified version of source code cannot be distributed under the license
    - Distribution of software built from modified source code should be allowed
    - Derived works may have to have a different name or version number
- No discrimination against persons, groups, fields of endeavor
- The license should also be transferred to the people to whom the program was distributed without them executing additional licenses
- License must not be specific to a product
- License must not restrict other software that came with the distributed software
- License must be technology neutral

Freeware and Shareware

- Freeware is free software
- Shareware is software without payment but for limited time and functionality
- Developers have copyrights
- Proprietary software
- License restricts modification and redistribution unlike OSS

Major OSS Companies

- Red hat
- Untangle
- Wordpress
- OpenBravo
- JasperSoft
- Canonical
- SugarCRM
- Digium
- MySQL
- Mozilla Foundation
- Apache software

Security of OSS

- OSS is less secure than proprietary software
    - Difficult to control quality
    - No responsibility for developer
    - Source code available to attackers
    - No reviews are guaranteed since it is public
    - Malicious developer can implant malicious functions in OSS
    - Attacker may inject virus, worm, malicious code
    - Poor documentation, since no entity control
    - System testing is ignored
- OSS is more secure than proprietary software

- More reliable since thousands of users are testing the OSS and fixing vulnerabilities
- More knowledge on security issues due to open communication
- User can check whether a feature is secure or not by checking the source code
- Proprietary software is expected to be secure but if the vulnerabilities are also kept a secret, they will not go away
- Proprietary software’s security is set by the vendors and cannot change unlike OSS where the user can make it more secure by adding more levels of features
- OSS is not influenced by commercial pressure that often degrades the quality of the code

<u>Lecture 17:</u>

Major New Computing Paradigms

- Service-oriented computing
  - Abstraction of functional units as software services with discoverable and interoperable interfaces, which can be described using common standards, such as WSDL

Cloud Computing:

- Derived from service computing and resource virtualization technologies (including Internet)
- Massively scalable computing capabilities provided 'as a service' to multiple customers simultaneously.
- IT resources across the Internet are dynamically configured and virtualized
- IT as an on-demand service
- Private, public and hybrid cloud systems

Major Characteristics of Cloud Computing:

- Resource pooling
- Heterogeneity
- Broad network access
- Agility
- Usability
- On-demand service
- Usage accounting
- Automation

Mobile Cloud Computing

- Emerging and considered as a cloud computing infrastructure, where data and processing occur outside mobile Devices
  - enabling new types of applications involving use of mobile devices, including handset centric features and network related features, such as GPS and/or cell-based location information.

Concerns of Mobile Cloud & Cloud users:

- Most cloud users are concerned with leakage of their sensitive data in the cloud because their data is processed and stored on machines owned and operated by various service providers, not controlled by users.
- Due to the severe limitation of resources available in mobile devices and characteristics of mobile cloud computing, security for mobile cloud computing are more severe.

Challenges: IA in Cloud Computing

- How to protect confidentiality and privacy of users' sensitive data from service providers?

  Possible Answers:

  - Enforcing communication via secure channels.
  - Performing strong identity verification to ensure devices are not compromised.
  - Limiting the use of third-party software and browsing to unsafe websites.

- Encrypting data on the device to protect against device compromise and theft.

- How to protect integrity of users' data within cloud?

  Possible answers:
  - Perform Risk-Based Validation.
  - Select Appropriate System and Service Providers.
  - Audit your Audit Trails.
  - Change Control.
- How to ensure that service providers will comply with security policies?

  Source: :https://www.globalknowledge.com/ca-en/resources/resource-library/articles/8-ways-to-get-employees-to-follow-it-security-policies/
- How to ensure the availability and reliability of each third-party service?
- How to support QoS adaptation in dynamic situation of the cloud?

  From: https://en.wikipedia.org/wiki/Quality_of_service

  Quality of service (**QoS**) is the description or measurement of the overall performance of a service, such as a telephony or computer network, or a cloud computing service, particularly the performance seen by the users of the network. To quantitatively measure quality of service, several related aspects of the network service are often considered, such as packet loss, bit rate, throughput, transmission delay, availability, jitter, etc.
- How to improve authentication and authorization of mobile devices in mobile cloud?
  - Use two-factor authentication
- How to improve network security, including mobile networks?

  From: https://www.sunnyvalley.io/docs/network-security-tutorials/what-are-ways-to-improve-network-security
  - Keep an Eye on Software Vulnerabilities
  - Be Careful Responding to Emails
  - Use VLAN
  - Encrypt the Entire Network
- How to avoid threat of malwares in cloud computing, especially in mobile cloud?

  Possible Answers:
  - Educate your employees. ...
  - Secure a data backup plan. ...
  - Who has access to the data? ...
  - Encryption is key. ...
  - Take passwords seriously. ...
  - Test, test, test. ...
  - Establish thorough cloud governance policies
- Protection of confidentiality and privacy of users' sensitive data from service providers
- Protection of integrity of cloud

Current State of Art: IA in Cloud Computing

- Assurance that service providers will comply with security policies
- Assurance of availability and reliability of third-party services
- Support for QoS adaptation in cloud

Lecture 18:

What is Social Computing ?

Social computing is a collection of technologies supporting collaborative and interactive online social communications and related activities among users through online social networks.

What is Social Network?

A social network is a social structure among social actors, such as individuals, groups, or organizations, which indicates specific types of social relationships or interdependencies in which the actors are connected.

Characteristics of Online Social Structure:

- User-created
- Interactive
- Community-driven
- Relationship-driven
- Heavily involving human factors

IA Issues on Online Social network:

- Easy targets of cyber attacks
- Security and privacy issues
- User management
- Data management
- Privacy management
- Virus / worms / malicious scripts
- Social engineering:

  Source: Internet (Paraphrase required)

  Social engineering is **the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information**. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

User management:

Difficult for following reasons:

- Social networks involve unpredictable
- sets of participants, including malicious
- users (hackers, private information collectors, phishers, or terrorists)
- Users' memberships, roles and privileges are dynamically changed
- A user may have multiple identities for different social networks or communities
- Establishing trustworthiness among users in a social network is difficult

What need to be done?

- Proper digital identity management
- Watch for anonymous access
- Trust management
- Efficient user authentication and authorization
- Proper access control for dynamic user privileges

- Detection of malicious behaviors

Data Management:
Difficult for following reasons:

- User-supplied data may violate laws or regulations
    - Violent/sexual contents, copyright-protected contents
- Quality of user-supplied data is difficult to control
    - Anyone can publish his/her contents on social networks
    - Rumors / gossips / incitements / false information
- Ownership of data is difficult to manage
    - Contents can be downloaded and republished on other social networks without owner's consent.
- Integrity of data is difficult to protect
    - Contents can be downloaded and easily modified without owner's consent.

How to improve ?

- Efficient filtering for contents against laws or regulations
- Efficient data quality control
    - A common way to control data quality in social networks is to use a reputation system. A user's reputation is scored by other users' feedbacks on the content he/she published. (e.g., seller rating system of eBay)
- Proper protection for copyrights and intellectual properties (e.g., digital watermarking)
- Proper protection for data integrity (e.g., digital signature)

Privacy Management:

- Two types of user-supplied content
    - Intentional content: Contents that users are willing to publish (e.g. blog posts, comments, reviews, ratings, links, RSS subscriptions, podcasts, and video).
    - Unintentional content: Byproducts of the intentional contents or the actions of users (e.g. metadata of

      intentional content, clickstreams, purchase history, search history, and other artifacts of behaviors).
- Privacy violation can occur on both intentional contents and unintentional contents

How to improve ?

- User-centric privacy management
    - User has control over
        - Who can access my content
        - How my personal information is collected
        - What kinds of unintentional content will be generated
- Fundamental principles for privacy protection
    - Notify users regarding collection, use and disclosure of personally identifiable information (PII)
    - Provide users the choice to opt out or opt in regarding disclosure of PII to third parties
    - Provide users the security to protect PII from unauthorized access
    - Enforce applicable privacy policies, laws and regulations

Viruses, Worms and Malicious Scripts

Online social networks are easy target of viruses, worms or malicious scripts

- Malicious users can easily publish contents containing viruses, worms or malicious scripts (e.g. cross-site scripting) which can quickly propagate through the social networks.

What need to be done?

- Sanitizing/validating user-supplied data
- Intrusion detection

Please paraphrase the below answers. DO NOT use it directly.

Virus:

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments.

Types: WannaCry, Stuxnet

How to protect:

- Antivirus software
- Antispyware software
- Firewalls
- Be careful what you click

Worms:

A computer worm is a subset of the Trojan horse malware that can propagate or self-replicate from one computer to another without human activation after breaching a system. Typically, a worm spreads across a network through your Internet or LAN (Local Area Network) connection.

The computer worm does not usually infect computer files, but rather infects another computer on the network. This is done by the worm replicating itself.

Example: Morris worm, Nimda, ILOVEYOU/Love Bug/Love Letter worm, etc

How to protect:

- Update software regularly
- Don’t click on pop-up ads while you’re browsing
- Be cautious when opening email attachments or links
- Firewall

Trojan Horse:

Trojan Horse is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

Example: Rakhni Trojan, Tiny Banker, Zeus or Zbot, etc

How to protect:

A Trojan horse virus can often remain on a device for months without the user knowing their computer has been infected. However, telltale signs of the presence of a Trojan include computer settings suddenly changing, a loss in computer performance, or unusual activity taking place. The best way to recognize a Trojan is to search a device using a Trojan scanner or malware-removal software.

LECTURE 19
Malware and Defense

Malware:
Malware is a file or code, typically delivered over a network, that infects, explores, steals, or conducts virtually any behavior an attacker wants. It is a piece of software injected in an information system to cause harm to the system or other systems or to subvert the ways using systems other than those intended by their owners.

Problems because of Malware:

1. Gain unauthorized access to an information system.
2. Steal sensitive data from an information system.
3. Disable security measures of an information system.
4. Damage an information system functionally and non functionally.
5. Compromise data and system integrity.

Characteristics of Malware:

1. Multi-functional and modular:
   The malware now are more modular and designed in such a manner that they disrupt multiple functionalities of a system. This is done so as to cause maximum damage.
2. Difficult to detect
   Malware started using multiple forms of hiding, in order to make it more difficult for the anti-malware programs to detect them. They use techniques like polymorphism to become undetectable.
3. Easy to obtain
   They are widely available over internet, and it is even possible to customize a malware so as to target a particular feature in system.
4. User-friendly
   Their deployment interface is easy and can be easily deployed by merging with an image text message etc. They get merged with the system so well that they become difficult to detect.
5. Enable broader cyber attack
   Malware can sometimes act as trigger and once infected a system, it can affect all the systems that are connected over the same network and cause maximum harm.
6. Affect various devices and computers
   Malware has the capability to connect to multiple systems over the local network and infect other systems as well.
7. Profitable
   Some organizations might use the malwares for their advantage like they may infect user systems to detect and analyze the day-to-day activities of the users.
8. Self-propagating and self-replicating
   As the malwares can infect systems over local internet they possess the capability to replicate and propagate at a faster rate.

Types of Malware:

Virus, Worms, trojan Horses, Trap doors, Logic Bombs etc.

1. Trap Doors (Back Doors):
   A trap door is kind of a secret entry point into a program that allows anyone to gain access to any system without going through the usual security access procedures. Trap Doors are quite difficult to detect and also in order to find them the programmers or the developers have to go through the components of the system. Programmers use Trap door legally to debug and test programs. Trap doors turn to threats when any dishonest programmers gain illegal access. Program development and software update activities should be the first focus of security measures. The operating system that controls the trap doors is difficult to implement.

2. Logic Bombs:
   A logic bomb is a set of instructions in a program carrying a malicious payload that can attack an operating system, program, or network. It only goes off after certain conditions are met to perform some destructive or security-compromising activity. A simple example of these conditions is a specific date or time.

3. Trojan Horse:
   A standalone malicious program that may give full control of an infected PC to another PC is called a Trojan horse. This is actually a code segment that tries to misuse its own environment. They somehow look attractive but on the other hand, they are really harmful and they actually serve as virus carriers. It may make copies of them, harm the host computer systems, or steal information. The Trojan horse will actually do damage once installed or run on your computer but at first, a glance will appear to be useful software. Trojans are designed as they can cause serious damage by deleting files and destroying information on your system. Trojans allow confidential or personal information to be compromised by the system creating a backdoor on your computer that gives unauthorized users access to your system. Unlike, Trojans do not self-replicate or reproduce by infecting other files nor do they self-replicate which means Trojan horse viruses differ from other computer viruses and do not spread themselves.

4. Virus:
   A computer virus is a type of malware that attaches to another program (like a document), which can replicate and spread after a person first runs it on their system. For instance, you could receive an email with a malicious attachment, open the file unknowingly, and then the computer virus runs on your computer. Viruses are harmful and can destroy data, slow down system resources, and log keystrokes. May exist on your computer, but it cannot infect your computer unless you run or open the malicious program. A virus cannot be spread without human action, such as running an infected program, to keep it going. A computer virus works in much the same way:
   i. A computer virus requires a host program.
   ii. A computer virus requires user action to transmit from one system to another.
   iii. A computer virus attaches bits of its own malicious code to other files or replaces files outright with copies of itself.

5. Worms:

Worms are a type of malware similar to viruses. Like viruses, worms are self-replicating. The big difference is that worms can spread across systems on their own, whereas viruses need some sort of action from a user in order to initiate the infection. The biggest danger is its capability to replicate itself on your system, rather than your computer sending out a single worm, it could send out thousands of copies of itself, creating a huge devastating effect. Example: ILOVEYOU: Came in an email with "I LOVE YOU" in subject and contained an attachment that, when opened, would result in the message being re-sent to everyone in the recipient's Microsoft Outlook address book, and the loss of every JPEG, MP3, and other files on recipient's hard disk. Reached 45 million users in a day.

6. Botnet:
   Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word’s “robot” and “network.” Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution. Botnets use your devices to scam other people or cause disruptions — all without your consent. A botnet usually consists of tens of thousands of compromised computers

Attacks using Malware:

- Distributed Denial of Service (DDoS)
- Compromising access control mechanism
- Compromising integrity of system
- Stealing online identity
- Spreading spam emails

Malware Propagation/Spread Mechanisms:

- Email attachments containing malicious code can be opened, and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, further compromising a network.
- File servers, such as those based on common Internet file system (SMB/CIFS) and network file system (NFS), can enable malware to spread quickly as users access and download infected files.
- File-sharing software can allow malware to replicate itself onto removable media and then on to computer systems and networks.
- Peer to peer (P2P) file sharing can introduce malware by sharing files as seemingly harmless as music or pictures.
- Remotely exploitable vulnerabilities can enable a hacker to access systems regardless of geographic location with little or no need for involvement by a computer user. Ex Bluetooth, wireless network etc.

Trends of Malware Attacks:

- More sophisticated
- Using increasingly deceptive social engineering techniques to entice users
- Blended, multi-faceted and phased attacks
- Large scale targeted attacks

- More powerful and destructive
- More prevalent through social networks and mobile devices.

Vulnerabilities exploited by Malware:

Once these vulnerabilities are discovered, malware can be developed to exploit the vulnerabilities before the security community develops a patch. Once malware compromises an information system, the malware may install additional powerful malware.

- Insecure software design and related software vulnerabilities
- Coding bugs
- Improper software configuration
- Poor user practices
- Inadequate security policies and procedures
- Social engineering
- Vulnerabilities in hardware

Challenges to fighting Malware:

- Do not have the resources or expertise to prevent or respond to malware attacks and associated secondary crimes from those attacks, such as identity theft, frauds and DDoS.
- Most security technologies are signature–based and can only detect known malware. Signature-based solutions are insufficient
- Global nature of the Internet as well as the complications of laws and jurisdictions bound by geographical boundaries to reduce the risks of being identified and prosecuted.
- Time lag between when a new malware is released by attackers, and when it is discovered and prevented.
- Common monolithic OS sharing same vulnerabilities
- Internet, social networks, mobile devices and clouds provide extensive connectivity, by which malware can be spread quickly.

LECTURE 20
Contingency and Disaster Recovery Planning

Contingency planning:

Multifaceted approaches to ensure that critical system and network assets remain reliable.
A contingency plan is sometimes referred to as "Plan B" or a backup plan because it can also be used as an alternative action if expected results fail to materialize. Contingency planning is a component of business continuity (BC), disaster recovery (DR) and risk management. A contingency plan is a course of action designed to help an organization respond effectively to a significant future incident, event or situation that may or may not happen.

Disaster Recovery Planning

Steps and procedures which personnel in key positions must follow to recover critical information systems in case of a disaster causing loss of services pf the systems.
A disaster recovery plan (DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events. The plan contains strategies on minimizing the effects of a disaster, helping an organization to quickly resume key operations or continue to operate as if there was no disruption.Disruptions can lead to lost revenue, brand damage and dissatisfied customers. The longer the recovery time, the greater the potential adverse business impact. A good DRP enables rapid recovery from disruptions, regardless of the source of the disruption.

Need for planning:

The purpose of planning is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event. The planning protects resources, minimizes customer inconvenience and identifies key staff, assigning specific responsibilities in the context of the recovery.

Possible causes for a disruption:

- Equipment failure
- Power outage
- Telecommunication network shutdown
- Software corruption
- Various attacks
- Human errors
- Strike
- Natural disasters

Plan Components: (Contingency Plan/ DRP Plan) [[ELABORATE IF NEEDED]]

1. Measures of disruptive events

   Identify and evaluate possible disruptive events:

   i. Identify most critical processes and requirements for continuing to operate in the event of an emergency

ii. Identify resources required to support most critical processes.

iii. Define disasters and analyze possible damages to most critical processes and their required resources

iv. Define steps of escalation in declaring a disaster

2. Response procedures and continuity of operations

Reporting procedures

a. Internal: notify IA personnel, management, and related departments
b. External: notify public agencies, media, suppliers, and customers

Determine immediate actions to be taken after a disaster happens

a. Protection of personnel
b. Containment of the incident
c. Assessment of the effect
d. Decisions on optimum actions to be taken
e. Taking account of the power of public authorities

3. Backup policies and processes, including off-site processing

i. Critical data and system files must have backups stored off-site.
Backups are used to:
   a. Restore data when normal data storage is unavailable
   b. Provide online access when the main system is down

ii. Not all data needs to be always online or available
   a. Backup takes time and need additional storage space
   b. Require extra effort to keep backup consistent with normal data storage
   c. Backup should consider data-production rates, data-loss risk and cost effectiveness

iii. Decide what and how often to backup depends on risks:
   a. Immediate loss of services: In case of power failure or application crash, any data that has not been saved will be lost. If the data is critical, users must be aware of this risk and make periodic "saves" automatically.
   b. Media losses: storage media has physical damage and cannot be read. Need to decide
      i. How often to do a complete backup?
      ii. Will incremental backups be done between two complete backups?
      iii. What media will be used for backup?
   c. Archiving inactive data: recent active data should be put onto a hard disk, while old inactive data can be archived to tape, CD or DVD

4. Plan for recovery actions after a disruptive event

a. High-level management must decide what the organization should do after a disruptive event happens.

Possible choices:

1. Do nothing: loss is tolerable; rarely happens and cost more to correct it.
2. Seek for insurance compensation: provides financial support in the event of loss, but does not provide protection for the organization's reputation.
3. Loss mitigation: isolate the damage and try to bring the system back online as soon as possible.
4. Bring off-site system online for continuous operation.

i. Do nothing: loss is tolerable; rarely happens and cost more to correct it.

b. Identify all possible choices, including cost/benefit analysis and present recommendations to high-level management for approval.

Types of Off-site processing:

a. Cold site: an empty facility located offsite with necessary infrastructure ready for installing back-up system when needed
b. Mutual backup: two organizations with similar system configuration agree to serve as a backup site for each other
c. Hot site: a site with hardware, software and network installed and compatible to production site
d. Remote journaling: online transmission of transaction data to backup system periodically to minimize loss of data and reduce recovery time
e. Mirrored site: a site equips with a system identical to the production system with mirroring facility. Data is mirrored to backup system immediately. Recovery is transparent to users

Cost wise: Mirrored>Remote>Hot>Mutual Backup>Cold Site.
Restore time: Mirrored<Remote<Hot<Mutual Backup<Cold Site.

Design Factors for Off-site Processing:

a. Availability of facility
b. Ability to maintain redundant equipment
c. Ability to maintain redundant network capacity
d. Relationships with vendors to provide immediate replacement or assistance
e. Adequacy of funding
f. Availability of skilled personnel

5. Guidelines for determining critical workload

a. Understand system's mission goal
b. Identify mission critical processes
c. Identify dependencies among various departments/personnel in the organization
d. Understand influence of external factors
    i. Government agencies and regulators
    ii. Competitors
    iii. Media

6. Individual employees' responsibilities in response to emergency situations

    a. Emergency response planning coordinator: coordinates the following activities:
        i. Establish contingency/disaster recovery plans
        ii. Maintain/modify the plans
        iii. Audit the plans

    b. High-level manager (department manager, VP, etc.)
        i. Understand process and mission goal of the organization
        ii. Monitor contingency/disaster recovery plans and keep plans updated

    c. All other employees
        i. Know contingency/disaster recovery plans
        ii. Understand own responsibilities and expectations
        iii. Know whom to contact if something not covered in plan happens

7. Emergency destructive procedures

    a. Under certain situations, an emergency response may focus on destroying data rather than restoring data
        i. Physical protection of system is no longer available
        ii. Critical assets (product design documents, list of sensitive customers or suppliers, etc.)

    b. An emergency destructive plan should contain
        i. Prioritized items that may need to be destroyed
        ii. Backup procedure for critical data at a secure off-site location
        iii. Specify who has authority to invoke destructive plan

Testing Contingency/Disaster Recovery Plan

Testing is an essential step in planning process as :
(Why Testing?)(Importance of testing)

a. A plan may look great on paper, but until it is carried out, no one knows how it will perform
b. Testing not only shows the plan is viable, but also prepares personnel involved by practicing their responsibilities and removing possible uncertainty

Methods of testing plan (Contingency or DRP):

a. **Walk-through**: members of key units meet to trace their steps through the plan, looking for omissions and inaccuracies
b. **Simulation**: during a practice session, critical personnel meet to perform dry run of the emergency, mimicking the response to true emergency as closely as possible
c. **Checklist**: members of the key units "check off" the tasks on list for which they are responsible. Report accuracy of the list

d. **Parallel testing**: ***backup processing*** occurs in parallel with ***production services that never stop***. ***If testing fails, normal production will not stop***.
e. **Full interruption**: ***production systems are stopped*** as if a disaster had occurred to see how backup services perform

LECTURE 21
Laws and Related Issues of IA

Laws:

Laws are rules that mandate or prohibit certain behavior in society. They are different from ethics, which define socially acceptable behaviors. Laws carry the sanctions of a governing authority and ethics do not.

Information Assurance Related/Relevant laws in the USA:

a. General Computer Crime Laws
b. U.S.A. Patriot Act

The official title of the USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001."

The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include:

a. To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
b. To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
c. To require all appropriate elements of the financial services industry to report potential money laundering;
d. To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.

Title I: Enhancing Domestic Security against Terrorism
Title II: Enhanced Surveillance Procedures
Title III: International money laundering abatement and anti-terrorist financing act of 2001
Title IV: Protecting the border
Title V: Removing obstacles to investigating terrorism
Title VI: Providing aid to public safety officers and their families when the officers are injured or killed in line of duty
Title VII: Increased information sharing for critical infrastructure protection
Title VIII: Strengthening the criminal laws against terrorism
Title IX: Improved intelligence
Title X: Miscellaneous

Key acts changed by the PATRIOT Act:

- Immigration and Nationality Act of 1952.

- give more law enforcement and investigative power to US Attorney General and to Immigration and Naturalization Service (INS).

- Bank Secrecy Act of 1970 (BSA)
    - make it harder for money launderers to operate and easier for law enforcement and regulatory agencies to police money laundering operations
- Foreign Intelligence Surveillance Act of 1978 (FISA)
    - allow government agencies to gather "foreign intelligence information" from both U.S. and non-U.S. citizens
- Electronic Communications Privacy Act of 1986 (ECPA)
    - allow surveillance of public network communication, including emails and web sites.
- Money Laundering Control Act of 1986
    - strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorists

c. Privacy related Laws

1. The Federal Privacy Act of 1974
    a. Protects records about individuals retrieved by personal identifiers such as a name, social security number, or other identifying number or symbol. An individual has rights under the Privacy Act to seek access to and request correction (if applicable) or an accounting of disclosures of any such records maintained about him or her.
    b. Prohibits disclosure of such records without the prior, written consent of the individual(s) to whom the records pertain, unless one of the twelve disclosure exceptions enumerated in subsection (b) of the Act applies.
    c. Ensure that government agencies protect the privacy of individuals' and businesses' information
    d. Hold those agencies responsible if any portion of the information is released without permission

2. Electronic Communications Privacy Act of 1986
    a. The Electronic Communications Privacy Act ("ECPA") was passed in 1986 to expand and revise federal wiretapping and electronic eavesdropping provisions. It was enacted to create promote " the privacy expectations of citizens and the legitimate needs of law enforcement."
    b. ECPA does include important provisions that protect a person's wire and electronic communications from being intercepted by another private individual. In general, the statute bars wiretapping and electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and the use or disclosure of information unlawfully obtained through wiretapping or electronic eavesdropping.
    c. In 2001, changed to allow surveillance of public network communication, including emails and web sites.

d. In addition to criminalizing the actual wiretapping or electronic eavesdropping, ECPA also prohibits an individual from disclosing such information obtained illegally if the person has reason to know that it was obtained illegally through the interception of a wire, oral, or electronic communication.

3. Health Insurance Portability and Accountability Act (HIPAA)

a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

b. A major goal of the Privacy Rule is to make sure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public's health and well-being.

c. The Privacy Rule permits important uses of information while protecting the privacy of people who seek care and healing.

d. It protects the confidentiality and security of health-care data by establishing and enforcing standards and by standardizing electronic data interchange.

e. While the HIPAA Privacy Rule safeguards PHI, the Security Rule protects a subset of information covered by the Privacy Rule. This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called electronic protected health information, or e-PHI.

f. Five fundamental principles:

i. Consumer control of medical information

ii. Boundaries on use of medical information

iii. Accountability for privacy of private information

iv. Balance of public responsibility for use of medical information for the greater good measured against impact to the individual

v. Security of health information

d. Export and Espionage Laws

1. Economic Espionage Act of 1996 (EEA)

a. The Economic Espionage Act of 1996 was signed into law by President Clinton. It makes the theft or misappropriation of trade secrets a criminal offense. It is unique in that it is the first federal law to broadly define and severely punish such misappropriation and theft.

b. It is designed to prevent abuse of information gained by an individual working in one company and employed by another

c. The EEA contains two separate provisions that criminalize the theft or misappropriation of trade secrets.

i. The first provision, codified at 18 U.S.C. § 1831, is directed towards foreign economic espionage and requires that the theft of the trade secret be done to benefit a foreign government, instrumentality, or agent.

ii. The second provision makes criminal the more common commercial theft of trade secrets, regardless of who benefits. 18 U.S.C. § 1832.

e. U.S. Copyright Laws
f. Freedom of Information Act

1. Freedom of Information Act (FOIA)
   a. The Freedom of Information Act (FOIA) gives any person the right to request access to records of the Executive Branch of the United States Government. The records requested must be disclosed unless they are protected by one or more of the exempt categories of information found in the FOIA.
   b. Agencies are required to disclose records upon written request except for those records that are protected from disclosure by any of the nine FOIA exemptions or by one of the three special law enforcement record exclusions. This right of access is enforceable in U.S. courts. Since its enactment the FOIA statute has been amended several times.

2. The Electronic Freedom of Information Act (E-FOIA)
   a. Amendments of 1996 to FOIA require agencies to provide the public with electronic access to any of their "Reading Room" records that have been created by them since November 1, 1996. Each agency shall make available for public inspection and copying final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases and a general index of the records.

Computer Ethics

A set of moral principles that regulate the use of computers. Computer ethics is a field of applied ethics that addresses ethical issues in the use, design and management of information technology and in the formulation of ethical policies for its regulation in society. Computer ethics address issues related to the misuse of computers and how they can be prevented. It primarily imposes the ethical use of computing resources. It includes methods to avoid violating the unauthorized distribution of digital content. The core issues surrounding computer ethics are based on the use of the internet, internet privacy, copyrighted content, software, and related services, and user interaction with websites.

The Computer Ethics Institute provides their Ten Commandments of Computer Ethics as a code of computer ethics. The Ten Commandments of Computer Ethics were created in 1992 by the Computer Ethics Institute to provide "a set of standards to guide and instruct people in the ethical use of computers." The code is both short and fairly straightforward.

The Computer Ethics Institute’s Ten Commandments of Computer Ethics are:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people’s computer work.
3. Thou shalt not snoop around in other people’s computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people’s computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people’s intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.