Lecture Notes

On

Cyber Security

By

Mr. Sandeep Vishwakarma

Assistant Professor

Dr. A.P.J. Abdul Kalam

Technical University,Lucknow

Unit 3

Application Security:

Application security is defines as the protection of software applications against threats. Application security includes, requires or depends on various inter-related architectural categories of security, as follows:

Data security. This is largely concerned with protecting the confidentiality and integrity of data, typically in transit and storage. We note that a typical assumption in data security and cryptography, that end-points are trusted, does not generally hold in environments requiring application security.

Software security. We define this as the science and study of protecting software (including data in software) against unauthorized access, modification, analysis or exploitation. The term "software security" informally in relation to the security properties and level of inherent security in a software application (in the sense of protection against relevant attacks).

software protection consists of a broad collection of principles, approaches and techniques intended to improve software security, providing increased protection against threats ranging from buffer overflow attacks.

I*nformation security* means protecting information (data) and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information Security management is a process of defining the security controls in order to protect the information assets.

Information Security Principles

The three fundamental principles of security are availability, integrity, and confidentiality and are commonly referred to as CIA or AIC triad which also forms the main objective of any security program.

The level of security required to accomplish these principles differs per company, because each has its own unique combination of business and security goals and requirements.

All security controls, mechanisms, and safeguards are implemented to provide one or more of these principles.

Confidentiality

- Ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of confidentiality should prevail while data resides on systems and devices within the network, as it is transmitted and once it reaches its destination.
- Threat sources
    - Network Monitoring
    - Shoulder Surfing- monitoring key strokes or screen
    - Stealing password files

  - Social Engineering- one person posing as the actual
- Countermeasures
  - Encrypting data as it is stored and transmitted.
  - By using network padding
  - Implementing strict access control mechanisms and data classification
  - Training personnel on proper procedures.

Integrity

- unauthorized modification is prevented.
- Threat sources
  - Viruses
  - Logic Bombs
  - Backdoors
- Countermeasures
  - Intrusion Detection
  - Hashing
  -

Availability

- Availability ensures reliability and timely access to data and resources to authorized individuals.
- Threat sources
  - Device or software failure.
  - Environmental issues like heat, cold, humidity, static electricity, and contaminants can also affect system availability.
  - Denial-of-service (DoS) attacks
- Countermeasures
  - Maintaining backups to replace the failed system
  - IDS to monitor the network traffic and host system activities
  - Use of certain firewall and router configurations

Basic security principles for information systems development

Information security is concerned with the confidentiality, integrity, and availability of information. From these three 'pillars', the following principles must be applied when implementing and maintaining an information system:

- Accountability
- Trust
- Data management
- Isolation
- Change

Accountability

Within the information system itself, controls must be implemented to maintain the appropriate level of information security. In most cases, the system must authenticate users, and record an appropriate level of system activity for audit purposes.

Trust

It must be assumed that any information system will be under attack via a number of vectors. A variety of safeguards are required for all system components to maintain system security and the security of the information being processed and stored.

Internal threats must also be considered. For example, implementing least privilege in a business process, and through authorization mechanisms, will lower the risk of a successful exploitation of trust by a trusted system user.

Data management

- **Data classification**

Information may be classified in a number of different ways, reflecting its importance to the university. Information must be classified in terms of confidentiality , records management , and importance to the institution for the purposes of Business Continuity Planning.

- **Data minimization**

The collection and use of information must be restricted to that which is required to support the business processes implemented by the information system. Data minimization reduces the exposure in the event of a breach. For example, do not collect personal information such as Social Insurance Numbers or dates of birth unless absolutely required.

- **Data protection**

The appropriate level of physical and logical security controls must be implemented to protect data when transmitted, processed, and stored. Some examples:

- Use Transport Layer Security (TLS) to maintain the confidentiality and integrity of information in transit on the network.
- Use encryption to protect the confidentiality and integrity of information stored on mobile devices.
- Use locked doors, surveillance cameras, and motion detectors to maintain the physical security of data centers.

Isolation

Highly sensitive information, such as information classified as Highly Restricted, should be isolated from more public systems. Isolation:

- Reduces the exposure to attack.
- Allows for greater security controls to be applied on a smaller scale, helping with the control of costs.
- Helps with managing the flow of information between independent systems.
- Can be used as an access control technique within an information system.

Change

When not managed properly, change can have a negative impact on the confidentiality, integrity, and availability of information. Untested or unplanned changes could introduce vulnerabilities that, when exploited, lead to a breach. The changes could also introduce bugs that may compromise the integrity of information. The discovery of any of these kinds of issues after-the-fact often requires unplanned outages to resolve, which has a negative impact on availability.

Application Security:

Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application, identifying and prioritizing potential threats and documenting adverse events and the actions taken in each case. This process is known as threat modeling.

Need for Application Security:

Businesses, institutions, and government organizations are now acknowledging the fact that it is not enough to protect only their IT infrastructure with firewalls and various intrusion detection systems (IDS). Since the focus of attackers has shifted to exploiting vulnerabilities in application design, source code, runtime code, and deployment configurations, there is a consensus among software experts that security needs to become an integral part of the software development life cycle (SDLC). Application security can be enhanced only if software teams focus on:

- Capturing security requirements early in the project life cycle (according to the relevant Enterprise Information Security standards and the Compliance and Regulatory requirements)
- Reducing security vulnerabilities and risks by implementing secure coding practices
- Improving security features and functions (e.g., authentication, encryption or auditing)
- Integrating security as part of the project life cycle
- Considering the security hosting environment and the enterprise security infrastructure

Application Security Architecture:

Security Architecture Lifecycle (as he calls it) should be driven by a well-defined Risk Management Process and that it should comprises the four phases mentioned below:

- **APPLICATION ARCHITECTURE RISK ANALYSIS:** ensures that an application's risk exposure is in line with tolerance goals of stakeholders
- **APPLICATION SECURITY ARCHITECTURE AND DESIGN:** ensures the integrity of o Application Security Process via SDLC, Identity Management, Threat Management, and Vulnerability Management
  - ✓ Application Security Defense In Depth via Data, Applications, Host, Network Protection
  - ✓ Application Security Metrics via Audit, Assurance, and Risk Assessment

- **APPLICATION IMPLEMENTATION**: ensures that Risk Management, Security Policy and Standards, and Security Architecture decisions are reflected in the runtime implementation
- **APPLICATION OPERATION AND MONITORING**: measures security metrics in runtime environment

<u>Information Security Governance:</u>

Information security is perceived as a wholly technical issue. For companies, educational institutions, and non-profit organizations to make progress in securing their information assets, however, executives must make information security an integral part of core business operations. The best way to accomplish this goal is to highlight ISG as part of the internal controls and policies that constitute corporate governance. 1

Information security governance is the responsibility of the board of directors and senior executives. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, boards of directors will be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organizational resources.

Information Security Governance Objectives

Part of the objectives of ISG is to ensure that there is an accurate security framework that meets the objectives of the organization.
Candidates are tested on the broad requirements for effective ISG and what is required to develop a framework with an accompanying plan of action for implementing it.
Candidates will be required to understand the contents of the framework, which will generally consist of:

1. A comprehensive security strategy that is intrinsically linked with business objectives
2. Governing security policies that address each aspect of strategy, controls and regulation

3. A complete set of standards for each policy to ensure that procedures and guidelines comply with policy
4. An effective security organizational structure void of conflicts of interest and with sufficient authority and adequate resources
5. Institutionalized metrics and monitoring processes to ensure compliance, provide feedback on effectiveness, and provide the basis for appropriate management decisions.

The Information Security Governance and Risk Management domain entails the identification of an organization’s information assets and the development, documentation, implementation, and updating of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The candidate is expected to understand the planning, organization, roles, and responsibilities of individuals in identifying and securing organization’s information assets; the development and use of policies stating management’s views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary, and private information; third party management and service level agreements related to information security; employment agreements, employee hiring and termination practices, and risk management practices, and tools to identify, rate, and reduce the risk to specific resources.

Security Objectives:

Confidentiality
Integrity
Integrity

Relationships between Threat, Risk, and Countermeasure:

- **Threat Agent:** An entity that may act on vulnerability.
- **Threat**: Any potential danger to information life cycle.
- **Vulnerability:** A weakness or flaw that may provide an opportunity for a threat agent.
- **Risk** The likelihood of a threat agent exploits the discovered vulnerability.
- **Exposure:** An instance of being compromised by a threat agent.
- **Countermeasure / safeguard:** An administrative, operational, or logical mitigation against potential risk(s).

Security Controls:

Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

Categories of Security Controls:

- **Management (Administrative) Controls**. – Policies, Standards, Processes, Procedures, & Guidelines like Administrative Entities: Executive-Level, Mid.-Level Management
- **Operational (and Physical) Controls**. – 1) Operational Security (Execution of Policies, Standards & Process, Education & Awareness) eg.- Service Providers: IA, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc 2) Physical Security (Facility or Infrastructure Protection) eg. - Locks, Doors, Walls etc.
- **Technical (Logical) Controls**. – Access Controls, Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation. Eg.- Service Providers: Enterprise Architect, Security Engineer,

Security Architecture

Security architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible.

In security architecture, the design principles are reported clearly, and in-depth security control specifications are generally documented in independent documents. System architecture can be considered a design that includes a structure and addresses the connection between the components of that structure.

The key attributes of security architecture are as follows:

- Relationships and Dependencies: Signifies the relationship between the various components inside IT architecture and the way in which they depend on each other.
- Benefits: The main advantage of security architecture is its standardization, which makes it affordable. Security architecture is cost-effective due to the re-use of controls described in the architecture.
- Form: Security architecture is associated with IT architecture; however, it may take a variety of forms. It generally includes a catalog of conventional controls in addition to relationship diagrams, principles, and so on.
- Drivers: Security controls are determined based on four factors:
    - Risk management
    - Benchmarking and good practice
    - Financial
    - Legal and regulatory

The key phases in the security architecture process are as follows:

- **Architecture Risk Assessment**: Evaluates the business influence of vital business assets, and the odds and effects of vulnerabilities and security threats.
- **Security Architecture and Design:** The design and architecture of security services, which facilitate business risk exposure objectives.
- **Implementation**: Security services and processes are implemented, operated and controlled. Assurance services are designed to ensure that the security policy and standards, security architecture decisions, and risk management are mirrored in the real runtime implementation.
- **Operations and Monitoring**: Day-to-day processes, such as threat and vulnerability management and threat management. Here, measures are taken to supervise and handle the operational state in addition to the depth and breadth of the systems security.

Issues in Hardware security

Hardware security is vulnerability protection that comes in the form of a physical device rather than software that is installed on the hardware of a computer system.

The primary objective of hardware security is to prevent loss, damage, and any other compromise of information system assets, to ensure there are no interruptions of business services and activities. Hardware assets may require physical protection from various security threats. It may be necessary to ensure that hardware assets do not create or are not exposed to any environmental hazards. These controls additionally reduce the risk of unauthorized data access, unauthorized equipment removal, and disposal.

The term *hardware security* also refers to the protection of physical systems from harm. To assess the security of a hardware device, it's necessary to consider vulnerabilities existing from its manufacture as well as other potential sources such as running code and the device's data I/O on a network.

HARDWARE SECURITY OBJECTIVE

The primary objective of hardware security is to prevent loss, damage, and any other compromise of information system assets, to ensure there are no interruptions of business services and activities. Hardware assets may require physical protection from various security threats. It may be necessary to ensure that hardware assets do not create or are not exposed to any environmental hazards.

The information systems auditor during the audit would focus on the following four objectives:

1. Effective and efficient use of assets
2. Safeguarding of assets
3. Availability of assets to those permitted to use them
4. Maintenance of integrity of hardware

Hardware/Downloadable Devices (Peripherals)/Data storage

Physical components or materials on which data is stored are called storage media. Hardware components that read/write to storage media are called storage devices.
Storage devices hold data, even when the computer is turned off. The physical material that actually holds data is called storage medium. The surface of a floppy disk is storage medium. The hardware that writes data to or reads data from a storage medium is called a storage device. A floppy disk drive is a storage device.
Two main categories of storage technology used today are magnetic storage and optical storage.

Primary magnetic storage
o Diskettes
o Hard disks (both fixed and removable)
o High capacity floppy disks o Disk cartridges
o Magnetic tape

Primary optical storage
o Compact Disk Read Only Memory (CD ROM)
o Digital Video Disk Read Only Memory (DVD ROM)
o CD Recordable (CD R)
o CD Rewritable (CD RW)
o Photo CD

Magnetic Storage Devices Purpose of storage devices → to hold data even when the computer is turned off so the data can be used whenever needed. Storage involves writing data to the medium and reading from the medium. Writing data → recording the data on the surface of the disk where it is stored for later use. Reading data →retrieving data from the surface and transferring it into the computers memory for use.

Diskette drives, hard drives and tape drive all use the same type of medium → use similar techniques for reading/writing data. Surfaces of diskettes and magnetic tape are all coated with a magnetically sensitive material such as iron oxide.

The principle use to store data is that of polarization – all the ions in the magnetic material align themselves in one direction. Surfaces of disks are coated with millions of tiny iron particles so data can be stored on them.

Magnetic Disks:

Before the computer can use a diskette to store data, the disks surface must be magnetically mapped so that the computer can go directly to a specific point without searching through all the data. This process of mapping a disk is called formatting or initializing. It may be helpful to reformat disks from time to time as this deletes all the data on disk.

A hard disk may have several hundred tracks on each side of each platter. Each track is a separate circle. These are numbered from the outermost circle to the innermost, starting with zero. Each track on a disk is also split into smaller parts. Imagine slicing a disk as you would a pie. Each slice cuts across all the tracks resulting in short segments or sectors. A sector can contain up to 512 bytes. All the sectors are numbered in one long sequence so the computer can access each small area on the disk with a unique number. This scheme simplifies a 2 dimensional set of co-ordinates into a single numeric address.

Diskettes (Floppy Disks)

The diskette drive includes a motor that rotates the disk on a spindle and the read/write heads that can move to any spot on the surface of the disk as it spins. This allows the heads to access data randomly rather than sequentially – the heads can skip from one spot to another without having to scan through all the data in between. Diskettes spin at approx. 300 revolutions per minute.

The longest it can take to position a point on the diskettes under the read/write heads is the amount of time for one revolution – 0.2 second. The farthest the heads have to move is from the centre of the diskette to the outside edge (or vice versa). The heads can do this in less time – about 0.17 seconds.

Fundamental differences and similarities between Diskette and Hard Disk :

- A diskette contains a single flat piece of plastic (the disk) coated with iron oxide enclosed in vinyl or plastic cover. A hard disk contains one or more rigid metal platters coated with iron oxide permanently enclosed in a hard disk drive.
- Diskettes are small and portable (they can be removed from diskette drives). Hard disks are usually built into the computer and are not portable (unless the computer is). Exceptions are removable hard disks and external hard drives which can be detached from the system.
- Floppy disks store only 1.44 MB although special floppy disks offer higher capacity. New hard disks can store several thousand times as much data as a diskette. · Hard drives are much faster than diskettes, their disks spin faster and they locate data on the disks surface in much less time.

CD-ROM:

The familiar audio compact disk is a popular medium for storing music. In the computer world, the medium is called compact disk read only memory (CD-ROM). This uses the same technology used to produce music CDs. The CD-ROM drive for music or data reads 0s and 1s from a spinning disk by focusing a laser on the disks surface. Some areas of the disk reflect the laser light into a sensor, other areas scatter the light. A spot that reflects the laser beam is interpreted as a 1 and the absence of a reflection is interpreted as a 0.

Physical security of IT assets

Physical security **helps companies protect assets, including IT infrastructure and servers, that make their businesses run and that store sensitive and critical data**. Physical security encompasses measures and tools like **gates, alarms and video surveillance cameras**, but also includes another central element: an organization's personnel. Crucially, business and IT leaders need to **foster a culture of security in addition to investing in technology to protect the organization**, according to security experts.

Physical security is an essential element of protective security framework. Physical security measures provides the first line of defense against intrusion or attack, and the most visible form of deterrence against unauthorized removal of information and assets. Physical security also provides an important support to other personnel and administrative security measures.

How to mitigate physical security threats:

There are several ways to mitigate risk in the physical space, including adding control mechanisms like:

- Site layout
- Access controls
- Intrusion protection and detection
- Utility redundancy
- Elemental protection

Layout

Your organization's site layout is incredibly important to protect the assets it contains. People and hardware can fall victim to weather, crime, eavesdropping/voyeurism and emergencies if not properly prepared.

Lower visibility, for example, can be the difference between a criminal breaking into your building or the one next door. The fewer access points, like external doorways, the better. Consider using a keycard system to lock doors and track who accesses each space when. Store equipment containing sensitive information in spaces with no windows and scrutinized access.

Access

Access controls within your business prevent strangers, vendors and visitors from obtaining access to equipment or information they otherwise shouldn't have access to.

Intrusion Protection & Detection: Camera

Using secondary security equipment like motion detectors and closed circuit cameras complements the use of key cards. If the key process were subverted, the system would be alerted to a trespasser via motion detection and engage video recording of the event.

Utility Redundancy

Your business can also face threats from larger outside forces that may seem non-threatening, such as participation in the local power grid.

Anyone operating on a local power grid could be subject to a breach if the power goes out due to overuse. Having a backup plan for your utilities can lessen the impact of a threat by keeping your network interruption-free

Elemental Protection

Natural disasters are also a very real threat to physical security, particularly in areas where tornadoes, landslides, earthquakes and flooding are common. Be prepared:

- When choosing to relocate or open a new office, know the common environmental threats to that specific area.
- Plan your space appropriately so it has the proper safeguards.
- Monitor local weather reports.
- Institute preventative measures if you know a storm is coming.

Access control:

The purpose of access control is to grant entrance to a building or office only to those who are authorized to be there. The lock, along with its matching key, was the standard of access control for many years.

Today, instead of keys, we carry access cards or ID badges to gain entry to secured areas. Access control systems can also be used to restrict access to workstations, file rooms housing sensitive data, printers, as well as entry doors.

Access Control System Components

- Access Control Readers

To read the card you need a reader at the door. Different types of readers are: Standalone, wireless IP readers etc.

- Video Surveillance

Most of us might now the internet connected wireless camera from our own smart home setup.

- PIN Pad / Keypad

Pin pads are used for convenient access however often come with the insecurity of the codes being passed on to others. Sometimes the pin pad is on the lock itself, or installed as standalone pin pad or key pad on a reader so it does both functions: Read the card and reading pins.

- Keycard / Keyfob / Swipe Card

When an employee holds the keycard at the reader or swipes the card or keyfob, the reader reads a unique identifier that is recognized by the system as having access to the requested door or not.

- Alarm Systems

Fire alarm systems are quite different from burglary alarm systems in regards to what they do: The fire alarm system unlocks or keeps certain doors locked in case of an emergency while the burglary alarm system notifies someone, often a third party like the police or 24/7 call center that unauthorized access has happened.

CCTV: Closed Circuit Television

CCTV systems provide surveillance capabilities used in the protection of people, assets, and systems. A CCTV system serves mainly as a security force multiplier, providing surveillance for a larger area, more of the time, than would be feasible with security personnel alone. CCTV systems are used to support comprehensive security systems by incorporating video coverage and security alarms for barriers, intrusion detection, and access control.

A CCTV system links a camera to a video monitor using a direct transmission system. This differs from broadcast television where the signal is transmitted over the air and viewed with a television. New approaches within the CCTV industry are moving towards more open architecture and transmission methods versus the closed circuit, hard-wired connection systems of the past.

Intrusion Detection System:

Access control and Intrusion detection is a combined system of hardware and software components that lets the user control the physical access to the interior of a building, a room or another type of closed space, at the same time protecting the space from intruders who trespass or violate the physical perimeter in any other way from the outside.

The Access control and Intrusion detection system is typically a unified solution that integrates a processor from a central controlling server and peripheral components with access control software. The server is used to connect and manage all peripheral components (doors, locks, turnstiles, motion detectors, sensors, alarms and other access control endpoints) from access control software.

Backup Security Measures:

- Encrypt your backups if your software and hardware support it. As with laptop computers and other mobile devices, portable backup media need to be encrypted with strong passphrases especially if they're ever removed from the premises.
- Limit access to important data backup by implementing a system of strong passwords
- Use a fireproof *and* media-rated safe. Many people store their backups in a "fireproof" safe. Backup media such as tapes, optical disks and magnetic drives have a lower burning/melting point than paper and a standard fireproof safe only serves to provide a false sense of security.
- **S**et up an IT security department with someone appointed to constantly monitor for data loss events and imminent security threats.
- Obtain and use the latest copy of state-of-the-art anti-virus software appropriate for your computer systems
  - Make sure your computer systems are protected by a strong firewall to help keep unsafe network traffic out.