Contents

[Database 2](#_Toc155219141)

[CSRF 3](#_Toc155219142)

[XSS 3](#_Toc155219143)

[Authentication 5](#_Toc155219144)

[SSL 5](#_Toc155219145)

[IPsec 6](#_Toc155219146)

[Intrusion Detection System 7](#_Toc155219147)

[Firewalls 9](#_Toc155219148)

[Firewall vs IDS 9](#_Toc155219149)

[Ports 10](#_Toc155219150)

[Confidentiality Policy 10](#_Toc155219151)

[Stupid Laws 11](#_Toc155219152)

A Replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.

Solution: sequence number, session keys, one time key (like OTP)

# Malware

1. Virus
2. Worm
3. Logic bomb
4. Trojan Horse
5. Backdoor
6. Spyware
7. Ransome ware
8. Scare ware
9. Keylogger
10. Browser Hijacker
11. Zombie

Virus:

* Memory based-how they live in memory
* Obfuscation based-how they hide
* Target based-how they spread
* Payload based-what they do

DB Security

# Database

SQL Injection (SQLi) is performed by an attacker when he gives malicious queries(unexpected commands) to database server. This can result in

* DOS attack
* Execute arbitrary system commands.
* Modify or delete data

Types of attacks:

* In-band attack (tautology, piggyback(adding additional query beyond intended, piggy backing attack on top of a legitimate request ), end of line)
* Out-of-band attack(email)
* Inferential attack(illegal queries( descriptive error page), blind sql injection(true/false questions by attacker to infer data))

Defenses:

* Encrypt Database
  + Full – bad idea
  + Every instance (value) – bad idea
  + Records or columns - best
* Database Access Control options
* Defensive Coding(stronger data validation checks in input/forms)
* Runtime Prevention
* Detection(signature, anomaly, code analysis)

Also take prevention against Inference attacks by

* Detect possible attacks in DB design (divide into multiple table, )
* Runtime query detection (deny if greater than limit)

Perturbation – adding noise to statistics database

* Data perturbation
  + Data swapping
* Output perturbation
  + Random-sample query
  + Statistic adjustment

WEB Security

# CSRF

Cross Site Reference Forgery is an attack depending on the weakness of the web application occurring when a user’s cookie saved in browser can be used to access a trusted site by attacker without user’s knowledge. Its impact can vary from just accessing the trusted site to performing transactions or changing the credentials to fully take over.

Defenses:

* Not performing actions based on just saved cookies but instead authenticate user first for every session.
* STP (Synchronizer Token Pattern)
* Origin / Referrer Headers

# XSS

Cross Site Scripting is an attack where user’s interaction with a vulnerable application can be compromised by an attacker (adds a malicious script). So an attack can do:

* Cookie Theft
* Keylogging
* Phishing

There are three types:

* Reflected

Reflected XSS involves the injection of a malicious script that is reflected back to the user in the web page's response.

* + Attacker stealing info with user interaction.
  + **Providing the user with a bad link (a vulnerable site) and including a script in it.**
  + The vulnerable site echoes back user’s input that can be accessed by attacker because of the script he included earlier.
  + Vulnerable site
  + Bad input
* Stored

Stored XSS involves **permanently storing the script on the target server**.

* + Attacker compromising server to steal info of user.
  + Malicious script is inserted into victim server.
  + **User accesses vulnerable site himself and malicious script gets executed.**
  + Attacker receives info.
* DOM Based

DOM-based XSS occurs when the **injection and execution happen within the Document Object Model on the client side.**

* + **Providing the user with a bad link (a vulnerable site) and including a script in it.**

Defenses:

* Encoding

Escaping user input so browser only interpret it as data not code.

* Validation

Allowing code but filtering out malicious parts

* + Whitelisting/blacklisting
  + Sanitize/reject.
* Input handling context
* Inbound/outbound (validation before receiving/validation before sending)
* Client-Side/Server-Side (to prevent persistent + DOM based attacks)
* Validate all headers, cookies, input fields, query strings etc.
* Adopt the policy “what is allowed”. (What is not allowed policy is difficult to manage and not fully possible)

# Authentication

* Repudiable – password and id
* Non-repudiable - biometric
* Basic auth involving Server.
  + Password based (use salt)
  + Biometric (False acceptance, False rejection)
    - Verification: smart card with pin, compared with one stored template
    - Identification: biometric info with no IDs, compared with N stored templates
* Challenge-Response – Symmetric and Asymmetric
* Centralized auth – Kerberos (client, AS and TGS, Application Server)
* OATH (an organization developing open standards for security), adding multiple layers of security like two factor authentication.

Network Security

# SSL

All three achieved in SSL:

* Confidentiality(encrypted, only for intended user),
* Integrity(unchanged),
* Authentication(legitimate sender)

At transport layer, above TCP

Handshake after TCP handshake

Client: Hello extension (list of algos, session key)

Server: Hello extension (selected algo, session key)

Client: Pre Master key (secret key either client provides or generated by p^ab mod q)

Client server exchange random number

Session Creation

Master keys = (secret, client random, server random)

Master key = Pseudo Random function (master keys)

* Key + seq no = mac generation
* Add to compressed data
* So compressed data + mac + padding
* Now perform encryption with algo key (optional)
* Protected data

# IPsec

1. Transport Mode

* Light
* Header visible

1. Tunnel Mode
   * Heavy
   * Original Header not visible
   * New header added

Difference in AH and ESP

* Just of confidentiality(ESP encapsulates)

Defenses:

* Origin / Referrer Headers

# Intrusion Detection System

Three classes of intruders:

Masqueraders:

* Not authorized
* Penetrate system’s access controls.
* Exploits a legitimate user’s account.
* Usually outside

Misfeasors:

* Legitimate user
* Access not authorized OR
* Misuses access
* Usually Inside

Clandestine User:

* Seizes supervisory control.
* Evades auditing and access controls. OR
* Suppresses audit collection.
* Can be inside or outside.

Types of attacks 7

1. Performing a remote root compromise of an e-mail server
2. Defacing a Web server
3. Guessing and Cracking passwords
4. Copying a database containing credit card numbers
5. Viewing sensitive data ( i.e. Payroll records and media without authorizations)
6. Running a packet sniffer on a workstation to capture usernames and passwords
7. Using an unattended, logged-in workstation without permission

Components 3

1. Sensors
2. Analyzers
3. UI

Basic Principles

1. Lessen damage. (remove intruder asap)
2. Prevent intrusion. (act as deterrent)
3. Improve intrusion prevention measures from data collected.

Ways of classifying IDS

1. Anomaly Based
   * Collection of information about legitimate user
   * Then statistical tests to observe
   * Any distinct from usual behavior is intrusion
   * **Primary strength:** recognize novel attacks
   * Usually generate many false alarms
   * Does not require prior knowledge of security flaws
2. Misuse Detection/ Signature based
   * Observe events on system
   * Set of rules to identify attack
   * Auto analyze and generate rules for historical audit
   * Requires large database rules to be effective.
   * Does not require prior knowledge of security flaws
3. Specification Based - Hybrid Detection:
   * System behavior described through functionalities and policies
   * Any thing outside this is considered intrusion
   * Combines strengths of anomaly based detection(novel attacks detection ) and misuse detection (known attacks detection)
   * Specification development difficult and expensive.

Not proper detection – false security

Too false alarms – time waste

Types of IDS

Host based:

Monitors events on a particular host

Drawback: what info to record and what not (to reduce analysis burden)

System specific activity.

No additional hardware needed.

Network based:

Monitor network traffic, devices, and protocols.

Cost of ownership reduced.

Operating system independent.

Honey pots: lure a potential attacker away from critical system. ~ static decoy

Deception Technology: proactive measure to lure, detect and defend. ~dynamic traps

* Honey Nets
* Decoy Files

Interaction Level

* High: apps, changing content, activity
* Medium: can actually log in
* Low: TCP/IP advertising, logon prompts

# Firewalls

**Packet Filtering**

Rules defined (no match/default -> reject recommended), uses info on transport level only (packet details)

**Stateful Packet Inspection**

Extension to traditional packet filtering, instead of each packet maintains state (connection information) hence easy to define rules for connections instead of each packet , but also overhead

**Application Proxy**

* Allows data in/out of process based on its type e.g allowing only HTTPS traffic to a website
* Can act on single computer or network layer
* More secure than packet filters
* Overhead on each connection

**Circuit-level Proxy**

* Relays TCP segments from one connection to other without examining contents.
* Security functions consists of determining which connections will be allowed.

## Firewall vs IDS

* Firewalls are essential for controlling access and protecting against unauthorized entry
* IDS play a crucial role in identifying and responding to suspicious activities that may evade the firewall’s initial barrier.

Both complement each other and together provide defense-in-depth.

* Firewalls block traffic, focus on access control.
* IDS alerts, focus on monitoring and detecting

## Ports

Port 80 – web sever/ http

Port 25 – mail server

Port 53 – DNS traffic

Port 443 – HTTPS

Port 20 – FTP

# Confidentiality Policy

Bell LaPadula (BLP)

* Confidentiality
* No read up
* No write down

BIBA

* integrity

Clark-Wilson

* Extended integrity of BIBA
* Commercial applications
* Well formed transactions
* Separation of duties
* Three rules
  + Prevent data modification by unauthorized parties.
  + Prevent unauthorized data modification by authorized parties.
  + Maintain internal and external consistency

Chinese Wall / Brewer Nash

* Conflict of interest

# Stupid Laws

**Laws:** allows/prohibit from certain behavior (derived from ethics)

**Ethics:** socially acceptable behavior among a group of people based on cultural mores(fixed moral attitudes)

**Liability**: legal obligation to make restitution.

**Restitution**: compensate for wrongs done.

**Due Care:** aware

org should act legally and ethically and should be aware of consequences

**Due Diligence:** active-taking actions

maintain standards of due care and ensure effective actions are in place.

**Jurisdiction**: court’s right to hear a case within its territory.

**Policies:** acceptable/ unacceptable behavior at workplace (ignore is a defense, not acceptable in case of laws)

Criteria for policy enforcement:

1. Dissemination
2. Review
3. Comprehension
4. Compliance
5. Enforcement

PECA, DMCA, WTO

Only deter if three conditions present

* Fear of penalty
* Fear of penalty apprehension
* Fear of penalty enforcement(applied)

10 commandments

ACM

SANS

ISACA

ISC2