CONTENTS

❑❑❑

CHAPTER 1 Information Security : Attacks and Vulnerabilities

Syllabus Topics

Introduction to information security : Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Attack Surface, Malware, Security-Functionality-Ease of Use Triangle

Types of malware : Worms, viruses, Trojans, Spyware, Rootkits

Types of vulnerabilities : OWASP Top 10 : cross-site scripting (XSS), cross site request forgery (CSRF/XSRF), SQL injection, input parameter manipulation, broken authentication, sensitive information disclosure, XML External Entities, Broken access control, Security Misconfiguration, Using components with known vulnerabilities, Insufficient Logging and monitoring, OWASP Mobile Top 10, CVE Database

Types of attacks and their common prevention mechanisms : Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs

Case-studies : Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit

Syllabus Topic : Introduction to Information Security

1.1 Introduction to Information Security

GQ. 1.1.1 Define Information Security.

UQ. 1.1.2 What is Information Security? Explain Asset, Risk, Threat, Vulnerability with respect to Information Security. (MU - April 2019)

- Information security (InfoSec) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions.
- InfoSec is part of information risk management.
- InfoSec is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information.
- Its responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Syllabus Topic : Asset

1.1.1 Asset

GQ. 1.1.3 Define Asset.

- An asset is any data, device, or other component of the environment that supports information-related activities.
- Assets generally include software (e.g. mission critical applications and support systems), hardware (e.g. servers and switches) and confidential information.
- Assets should be protected from illegal access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.

Syllabus Topic : Access Control

1.1.2 Access Control

GQ. 1.1.4 What is an Access Control? Explain its steps with example.

- An Access control is a way of limiting access to a system or to physical or virtual resources.
- An Access control is a process by which users are granted access and certain privileges to systems, resources or information.
- The access control mechanisms are built start with identification and authentication.
- It is generally considered in three steps :
  1. Identification
  2. Authentication
  3. Authorization

1. Identification

- Identification is an assertion of someone and something.
- For Example: If a person makes the statement "Hello, my name is RAM" they are making a claim of who they are but their claim may or may not be true. Before RAM can be granted access to protected information it will be necessary to verify that the person claiming to be RAM really is RAM.

2. Authentication

- Authentication is act of verifying a claim of identity.
- For Example: When RAM goes into a bank to make a withdrawal, he tells the bank teller he is

RAM, a claim of identity. The bank teller asks to see a photo ID, so he hands the teller his Pan Card. The bank teller checks the Pan Card to make sure it has RAM printed on it and compares the photograph on the Pan Card against the person claiming to be RAM.

- If the photo and name match the person, then the teller has authenticated that RAM is who he claimed to be. So, by entering the correct password, the user is providing evidence that he is the person the username belongs to.

Authorization

When a person or computer has been successfully identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform, so this is called authorization.

Syllabus Topic : CIA

1.1.3 CIA

GQ. 1.1.5 Explain CIA in details.

- The Term Confidentiality, integrity and availability, also known as the CIA triad, which is a model designed to guide policies for information security within an organization.
- Confidentiality is a set of rules that restrict access to information, integrity is assurance that the information is accurate and trustworthy and availability is a guarantee of authentic access to the information by authorized people.

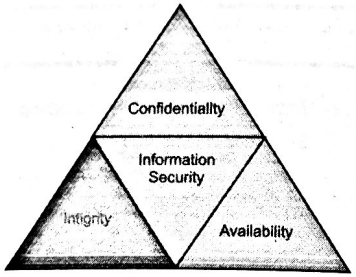


Fig. 1.1.1 : CIA Triads

1. Confidentiality

- Confidentiality is nothing but privacy.
- Confidentiality is designed to prevent sensitive information from reaching the wrong people and making sure that the right people can in fact get it.
- User Id's and passwords, access control lists and policy based security are some of the methods from which confidentiality is achieved.

2. Integrity

- Integrity is assures that the data or information system can be trusted.
- It is ensures that edited by only authorized persons and remains in its original state when at rest.
- Data encryption Standard and hashing algorithms are key processes that providing integrity

3. Availability

- The Data and information systems are available whenever required.
- Hardware maintenance, software upgrading /patching and network optimization ensures availability.

Syllabus Topic : Authentication

1.1.4 Authentication

GQ. 1.1.6 Define Authentication.

- Authentication is the process of recognizing a user's identity.
- Authentication is the mechanism of associating an incoming request with a set of identifying credentials.
- The credentials provided by user are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.
- Authentication might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product or document is not counterfeit.

Syllabus Topic : Authorization

1.1.5 Authorization

GQ. 1.1.7 Define Authorization.

- Authorization is a security mechanism which determines access levels or user/client privileges related to system resources including files, computer programs, services, data and application features.
- Authorization is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.
- For example, human resources staff are authorized to access employee records and this policy is usually formalized as access control rules in a computer system.

Syllabus Topic : Risk

1.1.6 Risk

GQ. 1.1.8 Define Risk. Explain Risk Management in details.

- Risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
- Risk is the intersection of assets, threats, and vulnerabilities.

Risk = Asset + Threads + Vulnerability

- Risk is a function of threats exploiting vulnerabilities to obtain damage or destroy assets. Thus, threats may exist, but if there are no vulnerabilities then there is little/no risk. Similarly, we can have vulnerability, but if you have no threat, then you have little/no risk.

Risk Management

- Information security risk management (ISRM) is the process of managing risks associated with the use of information technology.
- It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets.

Stages of Risk Management

1. Risk Identification
2. Risk Assessment
3. Risk Treatment

1. Risk Identification

- It is act of identifying positive & negative risk that affects to particular object.
- It can identify risk related Assets, threads, vulnerabilities and control.

2. Risk Assessment

Risk Assessment is the process of combining the information you've gathered about assets, vulnerabilities, and controls to define a risk.

Risk = (threat x vulnerability x asset value) - security controls

3. Risk Treatment

Once a risk has been assessed and analyzed, an organization will need to be select treatment options like : Remediation, Mitigation, Transference, Risk acceptance, Risk avoidance

Syllabus Topic : Threat

1.1.7 Threat

GQ. 1.1.9 Define Threads.

- Threat can be anything that can take advantage of vulnerability to breach security and negatively erase, alter, harm object or objects of interest.
- A threat is something that may or may not happen, but has the potential to cause serious damage.
- Threats can be like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
- The Following are Information Security Threads:
  - o Insider threats
  - o Viruses and worms
  - o Botnets
  - o Phishing attacks
  - o Distributed denial-of-service (DDoS) attacks

Syllabus Topic : Vulnerability

1.1.8 Vulnerability

GQ. 1.1.10 Define Vulnerability.

- Vulnerability is a term that refers to a flaw in a system that can leave it open to attack.
- Vulnerability may also refer to any type of weakness in computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
- Vulnerabilities are information security and information assurance professionals seek to reduce.
- Reducing vulnerabilities provides fewer options for malicious users to gain access to secure information.
- Computer users and network personnel can protect systems from vulnerabilities by keeping software security patches up to date.
- Vulnerability can harm five kinds of system securities that include: Reliability, confidentiality, usability, entirety, and undeniableness.
- The most common computer vulnerabilities include :
  1. Bugs
  2. Weak passwords
  3. Software that is already infected with virus
  4. Missing data encryption
  5. SQL injection
  6. Buffer overflow
  7. Missing authorization
  8. Use of broken algorithm
  9. Download of codes without integrity checks
  10. Unrestricted upload of dangerous file types

Syllabus Topic : Attack

1.1.9 Attack

GQ. 1.1.11 Define Attacks. Enlist its types& explain in details.

- An attack is an information security threat that involves an attempt to obtain, alter, remove, destroy, implant or reveal information without authorized access or permission.
- It happens to both individuals and organizations.
- There are many different kinds of attacks, including but not limited to passive, active, botnet, targeted, clickjacking, brandjacking, phishing, spamming, inside and outside.
- There are two types of attacks :
  1. Passive Attacks
  2. Active Attacks

1. Passive Attacks

- A passive attack is one that does not affect any system, although information is obtained.
- For example: wiretapping

2. Active Attacks

- An active attack has to cause major damage to an individual's or organization's resource because it attempts to alter system resources or affect how they work.
- For Example: virus or malware

Syllabus Topic : Attack Surface

1.1.10 Attack Surface

GQ. 1.1.12 Define Attack Surface. How to measure attack surface?

- The attack surface of a software environment is the sum of different points where an unauthorized user can try to enter data to or extract data from an environment, so keeping the attack surface as small as possible is a basic security measure.
- There are three steps to understand attack surface:
  1. Visualize
  2. Find indicators of exposures
  3. Find indicators of compromise

1. Visualize

Visualize system of an enterprise is the first step, by mapping out all the devices, paths and networks

2. Find indicators of exposures

- The second step is to correspond each indicator of a vulnerability being potentially exposed to the visualized map in the last step.
- One IOE can be "missing security controls in systems and software"

3. Find indicators of compromise

This is an indicator that an attack has already succeeded.

Syllabus Topic : Malware

1.1.11 Malware

GQ. 1.1.13 Define Malware.

UQ. 1.1.14 What is malware? Explain in brief concept of Virus. (MU - April 2019)

- Malware is also known as malicious software.
- It is any program or file that is harmful to a computer user.
- Types of malware can include viruses, worms, Trojan horses and spyware.
- These malicious programs can perform a variety of different functions such as encrypting or deleting sensitive data, stealing, altering or

hijacking core computing functions and monitoring users' computer activity without their permission.

Syllabus Topic: Security-Functionality-Ease of Use Triangle

1.1.12 Security-Functionality-Ease of Use Triangle

GQ. 1.1.15 Define Security- Functionality-Easy-of-Use with diagram

- In any implementation of security controls, all three factors like Security, Functionality, and Ease of Use, have to be considered carefully, searched for the balanced trade-off for all stakeholders.

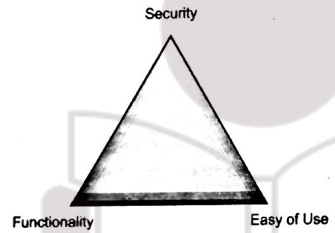


Fig. 1.1.2 : Security-Functionality-Ease of Use Triangle

- When we implement any higher level of security it is going to impact on functionality and ease of use.
- So whenever we develop any application with security keeping in mind as a being security project manager, security test engineer or security developer we need to make sure that we have balanced all these three things.
- So if we are trying to make any application easy to use , lots of security weaknesses occurs
- For Example: Website Login

1. Easy to Use

To make application easy to use, we can offer only email address as login. But From this users who have not registered to application may have access to application as well as any user can access any user data.

2. Functionality

- To make this login little complex, we can use combination of username and passwords. But this method is not effective in the case of brute force (Automatic username and password inputs for application) attacks.

3. Security

For extended level of security we can implement CAPTCHA to prevent application from brute force attacks. To add some more layer of security in applications we can use OTP or Secure tokens.

Syllabus Topic :Types of Malware

1.2 Types of Malware

GQ. 1.2.1 Enlists the types of Malware

There are following types of Malware:

1. Worms
2. Viruses
3. Trojans
4. Spyware
5. Rootkits

Syllabus Topic : Worms

1.2.1 Worms

GQ. 1.2.2 Define Worms.

- A worm is a type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.

- A Worm uses a computer network to spread itself, relying on security failures on the target computer to access it.
- It is often use parts of an operating system that are automatic and invisible to the user.
- Worm infection spreads without user interaction. All that is necessary is for the worm to become active on an infected system.
- Worms were spread through infected storage media, such as floppy disk which, when mounted on a system, would infect other storage devices connected to the victim system. USB are still a common vector for computer worms.

Examples of Worms

1. Email worms:

- An email worms uses a PC's email client to spread itself.
- It will either send a link within the email that, when clicked, will infect the computer or it will send an attachment that whenever opened, it will start the infection.
- As far as worm is installed, it will search the host computer for any email addresses contained on it.
- Then it will start the process again, sending the worm without any input from the user.
- A well-known example of Email Worm is the "ILOVEYOU" worm, which infected millions of computers worldwide in 2000.

2. Internet Worms

- An Internet worms are completely autonomous programs. It uses an infected machine to scan the Internet for other vulnerable machines.
- So when a vulnerable machine is located, the worm will infect it and begin the process again.

Syllabus Topic : Viruses

1.2.2 Viruses

GQ. 1.2.3 Define Virus. Enlist its type & explain in details.

- A virus is a malicious program that self-replicates by copying itself to another program. Means, the virus spreads by itself into other executable code or documents.
- The purpose of creating a virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design viruses with malicious intent and prey on online users by tricking them.
- The most common viruses are:
  - **Boot Sector Virus :** These viruses infects the master boot record and it is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media.
  - **Direct Action Virus :** These viruses also called non-resident virus, it gets installed or stays hidden in the computer memory. They stay attached to the specific type of files that it infect.
  - **Resident Virus :** Resident viruses get installed on the computer. These type of viruses are difficult to identify and it is even difficult to remove a resident virus.
  - **Multipartite Virus :** These viruses spread through multiple ways. It is infects both the boot sector and executable files at the same time.
  - **Polymorphic Virus** : These viruses are difficult to identify with a traditional anti-virus program. It is because the polymorphic viruses alter its signature pattern whenever it replicates.

Syllabus Topic : Trojans

1.2.3 Trojans

GQ. 1.2.4 Define Trojans.

- A Trojan horse (Trojan) is a type of malware that is often disguised as legitimate software.
- It can be employed by cyber-thieves and hackers trying to gain access to users' systems.
- Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. So when it activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.
- These actions can include : Deleting data, Blocking data, Modifying data, Copying data
- Disrupting the performance of computers or computer networks

Syllabus Topic : Spyware

1.2.4 Spyware

GQ. 1.2.5 Define spyware.

- A Spyware is any software that installs itself on computer and starts covertly monitoring your online behaviour without your knowledge or permission.
- It is a kind of malicious software that secretly gathers information about a person or organization and relays this data to third parties.
- A Spyware is installed without user consent by methods such as a drive-by download, a deceptive pop-up window or a trojan included with a legitimate program.
- It uses your internet connection to relay personal information such as username, address, interests, browsing habits, preferences or downloads and also other forms of spyware hijack your browser to point it to another website, cause your device to send texts or place calls automatically, or shows annoying ads even when you are offline.
- Spyware that steals your all details like username, password or other credentials is referred to as a "key logger" which is an insidious prerequisite for cyber crime.
- A spyware infection can be detected when unwanted behaviours and degradation of system performance occurs.
- A Spyware can eat up CPU capacity, disk usage and network traffic. The stability issues such as failure to boot, applications freezing, difficulty connecting to the internet and system crashes are also common.

Syllabus Topic : Rootkits

1.2.5 Rootkits

GQ. 1.2.6 Define Rootkits.

- A rootkit is a collection of malware created to get access to a target computer and often hides its existence or the existence of other software.
- A rootkit is concatenation of "root" which is the privileged account on Unix-like OS and the word "kit" which is refers to the software components that implement the tool.
- It can be installed by an attacker directly or remotely by exploiting a known vulnerability and once installed; it hides and runs with administrator privilege.
- Rootkit detection is difficult because it intercepts operating system calls by antivirus and returns a good version of the software. It either duplicates or replaces Operating system files making it difficult to detect it.

Syllabus Topic : Types of Vulnerabilities

1.3 Types of Vulnerabilities

GQ. 1.3.1 Enlist different types of vulnerability

GQ. 1.3.2 What is OWASP Mobile Top 10? Explain any one in details.

UQ. 1.3.3 Define the term vulnerability. Explain any two from following (MU - April 2019)

a. XSS b. SQL Injection

c. Insufficient logging and Monitoring

- The Open Web Application Security Project (OWASP) is an international non-profit organization dedicated to web application security.
- OWASP's core principles are that all of their materials be freely available and easily accessible on their website and making it possible for anyone to improve their own web application security.
- The materials they offer include documentation, , videos, tools and forums.
- OWASP Top 10 is best-known project.

There are following types of vulnerabilities as given below:

1. Cross-site scripting(XSS)
2. cross site request forgery (CSRF/XSRF)
3. SQL injection
4. input parameter manipulation
5. Broken authentication
6. sensitive information disclosure
7. XML External Entities
8. Broken access control
9. Security Misconfiguration
10. Using components with known vulnerabilities
11. Insufficient Logging and monitoring

Syllabus Topic : Cross-Site Scripting (XSS)

1.3.1 Cross-Site Scripting (XSS)

- A Cross-site scripting(XSS) vulnerabilities occur when web applications allow users to add custom code into a url path or onto a website that will be seen by other users.
- It can be exploited to run malicious JavaScript code on a victim's browser.
- For example, an attacker could send an email to a user that appears to be from a trusted bank, with a link to that bank's website. This link have some malicious JavaScript code tagged onto the end of the url so if the bank's site is not properly protected against cross-site scripting, then that malicious code will be run in the user's web browser when they click on the link.
- Prevention strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and sanitizing user-generated content.
- We can use modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.

Syllabus Topic : Cross Site Request Forgery (CSRF/XSRF)

1.3.2 Cross Site Request Forgery (CSRF/XSRF)

- The Cross-Site Request Forgery (CSRF) is an hacker that forces an user to execute unwanted actions on a web application in which they are currently authenticated.
- This hacker specifically target only state-changing requests, not theft of data.
- Since the hacker has no way to see the response to the fake request.

- With a little help of social engineering (like sending a link via email or message), an hacker may trick the users of a web application into executing actions of the hacker's choosing.
- If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests such as changing their email address, transferring funds, and so on.
- If the victim is an administrative account, cross site request forgery can compromise the entire web application.

Syllabus Topic :SQL Injection

1.3.3 SQL Injection

UQ. 1.3.4 Define the term vulnerability. Explain any two from following (MU - April 2019)

a. XSS

b. SQL Injection

c. insufficient logging and Monitoring

- An Injection attacks happen when entrusted data is sent to a code interpreter through a form input or some other data submission to a web application.
- For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that input is not properly secured, this would result in that SQL code being executed. This is known as SQL injection attack.
- Injection attacks can be prevented by validating and sanitizing user-submitted data. Moreover a database admin can set controls to minimize the amount of information an injection attack can expose.

Example SQL Injection Attack Scenarios

- **Scenario 1:** The following application uses untrusted data in the construction of the following vulnerable SQL call

```
String SQL = "SELECT * FROM users WHERE uID='"
+ request.getParameter("id") + "';
```

- **Scenario 2** : In second scenario, an application's blind trust in frameworks may result in queries that are still vulnerable(Hibernate Query)

```
Query HQLQuery = session.createQuery("FROM
users WHERE uID='" +
request.getParameter("id") + "'");
```

- In both above cases, the attacker changes the 'id' parameter value in their browser to send: ' or '1'='1.

For example

http://example.com/app/usersView?id=' or '1'='1

This modification is the meaning of both queries to return all the records from the accounts table. More dangerous attacks could delete or modify data or even invoke stored procedures.

Syllabus Topic :Input Parameter Manipulation

1.3.4 Input Parameter Manipulation

- The input Parameter manipulation attack is based on the manipulation of parameters exchanged between client and server in order to modify application data like user details and permissions, quantity of products and price
- This information is stored in the form of cookies, hidden form fields, or URL Query Strings which is used to increase application functionality and control.
- This attack can be performed by a malicious hacker who wants to utilize the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack.
- For above given cases tools likes Web scarab and Paros proxy are mostly used.

- The attack success depends on lack in integrity and logic validation mechanism errors, and its utilization can result in other consequences including SQL Injection, XSS, file inclusion, and path disclosure attacks.

Syllabus Topic : Broken Authentication

1.3.5 Broken Authentication

In Broken authentication, weaknesses or backhoes can allow an attacker to either capture or bypass the authentication methods that are used by a web application.

1. It permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
2. It permits brute force or other automated attacks.
3. It permits default, weak, or well-known passwords, such as "Pass1" or "admin ".
4. It uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers", which cannot be made safe.
5. It uses plain text, encrypted, or weakly hashed passwords.
6. It has missing or ineffective multi-factor authentication.
7. It exposes Session IDs in the URL (e.g., URL rewriting).
8. It does not rotate Session IDs after successful login.
9. It does not properly invalidate Session IDs. User's sessions or authentication tokens are not properly invalidated during logout or a period of inactivity.

- The major goal of an attack is to take over one or more accounts and for the attacker to get the same privileges as the attacked user.
- **Example :** In Credential stuffing, use of lists of known passwords is a common attack. So if an application does not implement automated threat or credential stuffing protections, the application can be used as a password oracle to determine if the credentials are valid.

Syllabus Topic : Sensitive Information Disclosure

1.3.6 Sensitive Information Disclosure

- If web applications don't protect sensitive data such as credit card details, personal information and passwords, etc.
- In this case, attackers can gain access to this data and utilize same information for nefarious purposes.
- One popular method for stealing sensitive information is using a man-in-the-middle attack.
- Data exposure risk can be reduced by encrypting all sensitive data as well as disabling the caching of any sensitive information in web application.
- In web application, developers should take care to ensure that they are not unnecessarily storing any sensitive data. Caching means temporarily storing data for re-use.
- For example, web browsers will often cache web pages so that if a user revisits those pages again and again with same time span, the browser does not have to fetch the pages from the web.

Syllabus Topic : XML External Entities

1.3.7 XML External Entities

- XML External Entities is an attack against a web application that parses XML input.
- This input can reference an external entity which attempting to exploit vulnerability in the parser.

- An external entity is refers to a storage unit such as a hard drive.
- An XML parser can be trick into sending data to an unauthorized external entity which can pass sensitive data directly to an attacker.
- The best ways to prevent XML External Entity attacks are to have web applications accept a less complex type of data, such as JSON, or at the very least to patch XML parsers and disable the use of external entities in an XML app.
- XML is a markup language intended to be both human-readable and machine-readable. Because of its complexity and security vulnerabilities, it is now being phased out of use in many web applications.

Syllabus Topic : Broken Access Control

1.3.8 Broken Access Control

- Access control means a system that controls access to information or functionality.
- It allows attackers to bypass authorization and perform tasks as though they were privileged users such as administrators.
- For example a web application could allow a user to change which account they are log in as simply by changing part of a url , without any other verification details.
- An Access controls can be secured by ensuring that a web application uses authorization tokens and sets tight controls on them.
- Many services issued authorization tokens when users logged in.
- In every privileged request that a user makes will require that the authorization token be present. So this will be a secure way to ensure that the user is who they say they are, without having to constantly enter their login credentials on web application.

Syllabus Topic : Security Misconfiguration

1.3.9 Security Misconfiguration

- Security misconfiguration is most common vulnerability on the list.
- It is often the result of using default configurations or displaying excessively unhandled exception.
- For instance, an web application could show a user overly-descriptive errors which may reveal vulnerabilities in the application, so this can be reduced by removing any unused features in the code and make sure that error messages are more general.

Syllabus Topic :Using Components with Known Vulnerabilities

1.3.10 Using Components with Known Vulnerabilities

- Many web developers use different components such as libraries and frameworks in their web applications.
- These components are pieces of software that help developers avoid unnecessary work and provide needed functionality.
- The common example include front-end frameworks like React and smaller libraries that used to a/b testing or add share icons. Some attackers looking for vulnerabilities in these components which they can then use to arrange attacks. Like an attacker trying to find a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit.
- The Component developers often offers security patches and updates to plug up known

vulnerabilities, but web application developers don't always have the patched or most-recent versions of components running on their applications.

- To minimize the risk of components with known vulnerabilities, web developers should remove unused components from their projects and also ensures that they are receiving components from a trusted source and ensuring they are up to date.

Syllabus Topic : Insufficient Logging and monitoring

1.3.11 Insufficient Logging and Monitoring

- Utilization of insufficient logging and monitoring is the problem of nearly every major incident. the attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.
- Insufficient logging and monitoring occurs any time like:
- Auditable events, such as login to web site, failed logins, and high-value transactions are not logged.
- Warnings and errors generate no or unclear log messages.
- Logs of applications are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response processes are not in place or effective.

Syllabus Topic : OWASP Mobile Top 10

1.4 OWASP Mobile Top 10

GQ. 1.4.1 Enlist & explain OWASP Mobile Top 10 in details.

The following are OWASP Mobile Top 10 Best Practices :

1. Improper Platform Usage
2. Insecure Data Storage
3. Insecure Communication
4. Insecure Authentication
5. Insufficient Cryptography
6. Insecure Authorization
7. Client Code Quality
8. Code Tampering
9. Reverse Engineering
10. Extraneous Functionality

1. Improper Platform Usage

- Mobile platforms provide a number of features that developers can access but improper use of these features can leave your app exposed to attacks.
- It describes this vulnerability as common and easily exploitable.
- The actual ease of exploit and acuteness of the impact largely depends on the type of specific exploit and an extent to which perpetrator managed to gain control.
- To prevent these following rules and guidelines created by platform holders allow you to make sure that all platform features are used in a correct way

2. Insecure Data Storage

- Insecure data storage creates the current category that kept the same name, but became more clear and comprehensive.
- Now days attack vector here varies greatly. From third party applications using cache, cookies and other information to gather protected data, to

adversary being able to physically obtain the device and view information, we need to handle data storage correctly in multiple ways. This includes encryption, authentication, and properly handling all caching features.

- Insecure data storage can be extremely easy to exploit.
- Privacy violations, as well as lost and leaked data are a steep price to pay for skimping on mobile security.
- Depending on the application, business impact can be severe.

3. Insecure Communication

- Insecure communication is an extremely common vulnerability present in the majority of apps with client-server structure. While developers often punctual about protecting authentication procedure and data at rest, they rarely bother to encrypt data in proper motion.
- If they didn't encrypting data in transit ,their app will faces man in middle attack/
- These attacks typically came from a network device like a router, a malicious software on device etc.
- If you not use encryption and open your mobile app that can easily exploitable vulnerability which can lead to data loss and bears severe impact on business.
- The best way to protect data is encryption and thorough verification of data and also OWASP is to apply additional encryption to the data before sending it.

4. Insecure Authentication

- Insecure authentication encompasses both weaknesses in session handling and authentication procedure. For mobile app, perpetrators usually create customize tools in order to bypass the client-side app entirely and submit a request directly to the server.
- Authentication schemes for mobile apps are much leaner than for regular web applications. Since most apps will need to work offline, a user is provided with an offline authentication option that can be exploited.
- This can cause in perpetrator gaining full control of the system. They can anonymously steal or delete data, or issue commands to the app or to the server, etc.
- This may lead to severe technical and business impact.
- The best way to avoid this problem is to use online authentication whenever possible while processing all authentication requests server-side.

5. Insufficient Cryptography

- Insufficient cryptography deals with the vulnerability that can have an extremely nasty business impact because it results in perpetrator obtaining decrypted information from a mobile device.
- Depending on the applications, extremely personal information can be compromised, which leads to user backlash and even potential lawsuits.
- The best way to avoid insufficient cryptography is to follow the best practices and standards used in cryptography.

6. Insecure Authorization

- Insecure Authorization deals with server-side vulnerabilities during the authentication procedure.
- These vulnerabilities regarding authentication gained prominence in cyber security landscape as of late.
- Insecure authorization is extremely common and can be hard to detect, while also posing a severe business impact.
- This is why they gained an additional prominence in both OWASP Web Application and Mobile Top 10.
- The best way to protect these issues is to make sure that user rights are always checked server-side and also verify any requests from a client independently server-side, making sure that they belong to the authorized user.

7. Client Code Quality

- Client code category focuses on vulnerabilities created due to coding mistakes.
- No code is perfect and hackers can find those errors and exploit them to gain access to the system.
- Best examples of this are buffer overflows and memory leaks.
- Letting a buffer overflow slip through testing can allow the hacker to gain control over the whole map, potentially leading to theft of private data, and even control over devise itself.
- The only way for dealing with such vulnerabilities is to maintain consistent coding standards across the board and to write a well-commented code that is easy to read.

8. Code Tampering

- Code tampering category covers any modifications that adversary can perform on the code of the app. There are a many of ways to do this, including method/class hooking, dynamic hooking, patching, etc.
- Hackers can use code tampering to gain access to premium features, violating copyright and completely bypassing existing distribution model for the app.
- Hackers can add malware to the app via direct changes to the binaries, or to resources.
- Alteration app is then distributed via third-party distribution platforms, resulting in lost sales and reputation damages for the original developers.
- This vulnerability can be difficult to detect. The best way to protect it is to use anti-tampering techniques, as well as root and jailbreak detection.

9. Reverse Engineering

- It is extremely widespread and not always done with malicious intentions. Sometimes people do it for study, sometimes they do it for write their own completely legitimate apps.
- But often hackers will use the technique to gain the information needed to exploit security vulnerabilities and decrypt data. Information on encryption algorithms used, as well as general workings of a back-end server is critical to protect.
- Every app is susceptible to reverse engineering. So if any damage from it can often be limited, this is not a reason to not protect it. We can use various tools to obfuscate the code is the best way to deal with reverse engineering.

10. Extraneous Functionality

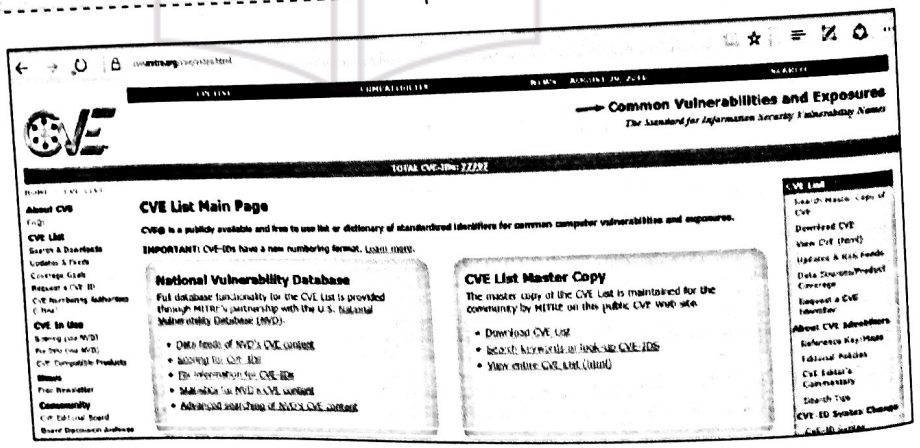
- Extraneous Functionality has been added to the list in 2016 in order to cover and extremely severe, but common vulnerability – functionality found in the app that shouldn't be there.
- This vulnerability occurs when developers don't remove additional features, created during the development process to make it easier to test the app.
- One example of this feature is a developer account that allows to completely bypass security checks and provides a wide set of privileges. It is a backdoor that gives attacker full control over the app. Such vulnerabilities are easy to exploit, but also easy to catch and remove too.

Syllabus Topic : CVE Database

1.4.1 CVE Database

GQ. 1.4.2 Explain CVE database.

- Common Vulnerabilities and Exposures (CVE) is the standard for information security vulnerability names.
- It is a dictionary of publicly known information security vulnerabilities and exposures.
- It is free for public use.
- CVE is a program launched in 1999 by MITRE, a non profit that operates research and development centers sponsored by the federal government, to identify and catalog vulnerabilities in software or firmware into a free "dictionary" for organizations to improve their security.
- Its main purpose is to standardize the way each known vulnerability or exposure is identified.
- Standard IDs allow security administrators to access technical information about a specific threat across multiple CVE-compatible information sources.



Syllabus Topic : Types of Attacks and their Common Prevention Mechanisms

1.5 Types of Attacks and their Common Prevention Mechanisms

GQ. 1.5.1 Enlist the types of Attacks.

UQ. 1.5.2 Define attacks and explain type of attack. (MU - April 2019)

The following are different types of attacks available:

- Keystroke Logging
- Denial of Service(Dos/DDos)
- Waterhole attack
- brute force
- phishing and fake WAP
- Eavesdropping
- Man-in-the-middle
- Session Hijacking
  - o Clickjacking
  - o Cookie Thef
  - o URL Obfuscation
  - o Buffer overflow
  - o DNS poisoning
- Arp Poisoning
- Identity theft
- Iot Attacks
- BOTs and BOTNETs

Syllabus Topic : Keystroke Logging

1.5.1 Keystroke Logging

GQ. 1.5.3 Explain Keystroke Logging attack in details.

- **Keystroke logger** is a software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard.
- The user who installed the software or hardware device can then view all keys typed in by that user.
- Because these software and hardware devices monitor, the keys typed in a user can easily find user passwords and other information a user may not wish others to know about.
- Keystroke loggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keystroke loggers can also be embedded in spyware allowing your information to be transmitted to an unknown third party.
- This is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker.
- The attacker then handle them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack.
- For example, a keystroke logger will reveal the contents of all e-mail composed by the user. It is commonly included in rootkits.
- A keystroke logger normally consists of two files: a DLL file which does all the work and an EXE file which loads the DLL and sets the hook.

Therefore when you deploy the hooker on system, these two files must be present in the same directory.

Syllabus Topic : Denial of Service (DoS/DDoS)

1.5.2 Denial of Service (DoS/DDoS)

GQ. 1.5.4 what is Denial of Service attack ?

UQ. 1.5.5 Explain the term DoS and list the types of DOS attack. (MU - April 2019)

- A Denial-of-Service (DoS) attack is an attack which shut down a machine or network by making it inaccessible to its intended users.
- Denial-of-Service attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
- In both cases, the DoS attack disposes legitimate users (i.e. members, employees, or account holders) of the service or resource they expected.
- Victims of DoS attacks often target web servers of high-profile organizations such as banking, media companies, ecommerce, and or government and trade organizations.
- DoS attacks do not typically affect in the theft or loss of significant information or other assets but they can cost the victim a great deal of time and money to handle.
- The general methods of this attacks are flooding services or crashing services.
- Flood attacks occur when the system receives too much traffic for the server to buffer request which will cause them to slow down and eventually stop.

Syllabus Topic : Waterhole Attack

1.5.3 Waterhole Attack

GQ. 1.5.6 Explain Waterhole attack .

- Watering hole is a computer attack in which the victim is of a particular group (like organization, industry, or region).
- In watering hole attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malicious software.
- Coincidently, some member of the targeted group becomes infected.
- Hackers looking for specific information may only attack users coming from a specific IP address.
- This also makes the hackers harder to detect.

Defense techniques: Web applications are often infected through zero-day vulnerabilities on browsers or other software. A defense against known vulnerabilities is to apply the latest software versions to remove the vulnerability that allowed the web application to be infected. This is monitor by users to ensure that all of their software is running the latest version. An additional defense is for companies to monitor their web applications and networks and then block traffic if any malicious content is detected.

Example : 2017 Ccleaner attack

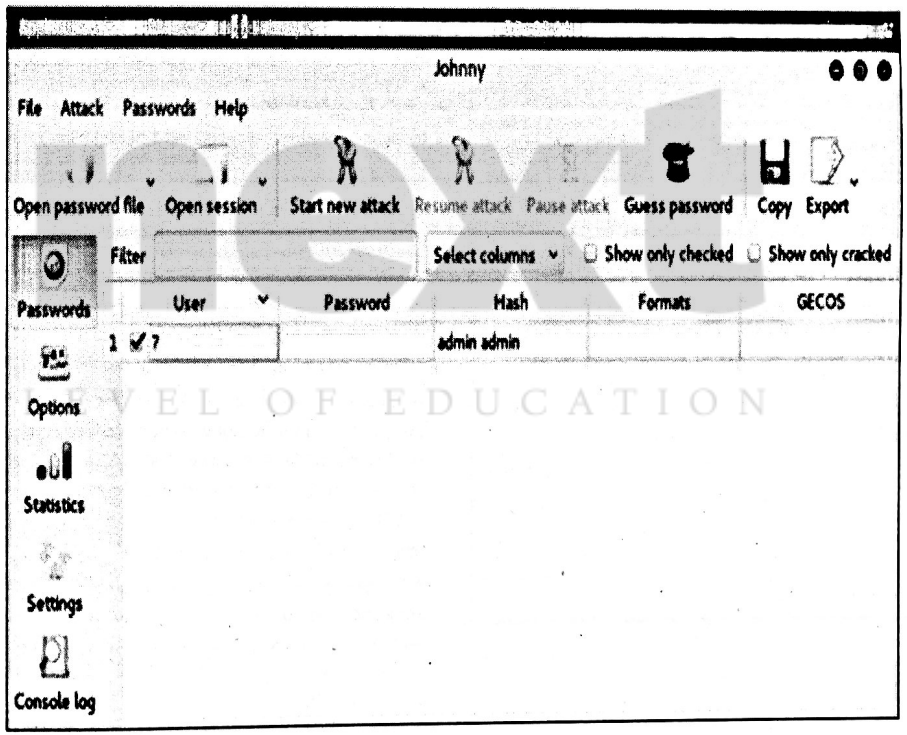
- From August to September 2017 the installation binary of Ccleaner distributed by the vendor's download servers included malicious software.
- Ccleaner is a popular software used to clean potentially unwanted files from Windows computers, widely used by security-minded users.
- The distributed binaries installers were signed with the developer's certificate making it likely that an attacker compromised the development and used this to insert malware.

Syllabus Topic : Brute Force

1.5.4 Brute Force

GQ. 1.5.7 Explain Brute Force attack in detail.

- In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and capital and small letters to break the password.
- Brute force attack has a high probability of success, but it requires an enormous amount of time to process all the combinations.
- This attack is slow and the hacker requires a system with high processing power to perform all those permutations and combinations faster.
- John the Ripper(Johnny) is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.



Syllabus Topic : Phishing and Fake WAP

1.5.5 Phishing and Fake WAP

GQ. 1.5.8 What is phishing ?

GQ. 1.5.9 what is Fake WAP ?

Phishing

- Phishing is a type of social engineering attack often used to steal user data, including login details and credit card numbers.
- Phishing occurs when an attacker, masquerading as a trusted entity, trick a victim into opening an email, text message, or instant message.
- The recipient is then duped into clicking a malicious link, which can lead to the installation of malware in system, the freezing of the system as part of a ransomware attack or may be the revealing of sensitive information.

Fake WAP

- A hacker can use fake Wireless Access Point(WAP) just for fun , which connects to official public place WAP.
- Once people get connected to fake WAP, then hacker can access that data.
- There are three main things that hackers are trying to do with a fake WAP:
  - Steal your password and login
  - Man in the middle attack
  - Device control

Syllabus Topic : Eavesdropping

1.5.6 Eavesdropping

GQ. 1.5.10 Explain Eavesdropping attack.

UQ. 1.5.11 Explain the following terms : a. Eavesdropping b. Man-in-the-middle

(MU - April 2019)

- An eavesdropping attacks are also known as a sniffing or snooping attack.
- It is an incursion where someone tries to steal information that computers, phones, or other devices transmit over the network.
- This attack takes advantage of unsecured network communications to access the data being sent and received.
- These attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

Syllabus Topic : Man-in-the-middle

1.5.7 Man-in-the-middle

GQ. 1.5.12 Explain Man-in-the-Middle attack in detail.

UQ. 1.5.13 Explain the following terms: a. Eavesdropping b. Man-in-the-middle

(MU - April 2019)

- **A man-in-the-middle attack** is type of the cyber attack.
- In Man-in-The-Middle attack, malicious hackers put himself into a conversation between two parties, resemble both parties and gains access to information that the both parties were trying to send to each other.
- This attack allows a malicious intender to intercept, send and receive data meant for someone else, or not meant to be sent at all, without outside party knowing until it is too late. This attacks can be abbreviated in many ways, including MITM, MiM, MitM or MIM.

Syllabus Topic : Session Hijacking

1.5.8 Session Hijacking

GQ. 1.5.14 What is Session Hijacking?

UQ. 1.5.15 Define session Hijacking. Describe the three steps involved in session hijacking.

(MU - April 2019)

- The Session Hijacking attack consists of the utilization of the web session control mechanism
- This mechanism is normally managed for a session tokens.
- HTTP communication uses many different TCP connections, so the web server needs a method to recognize every user's connections.
- The most useful method depends on a token is that, the Web Server sends response to the client browser after a successful client authentication.
- A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in other parts of the header of the http request, in the header of the http requisition as a cookie, or yet in the body of the http requisition.
- This attack accommodates the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

Syllabus Topic : Click jacking

1.5.9 Click jacking

GQ. 1.5.16 Explain click jacking attack.

- Click jacking, also known as a "UI redress attack".
- This attack happens when an attacker uses multiple layers(either transparent or opaque) to trap a user into clicking on a button or link on another page as user were intending to clicks on the top level page.
- The attacker is hijacking clicks means for victim page and redirects them to another page.
- That pages mostly owned by another application, domain, or combination of both.
- Using a same technique, keystrokes can also be hijacked.
- With a carefully organized combination of text boxes style sheets and, iframes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame which is controlled by the attacker.
- For example, imagine an attacker who builds a web site that has a button on it that says "click here for a free mobile".
- The attacker has loaded an iframe with your mail account on top of that web page, and lined up exactly the "delete all messages" button directly on top of the "free mobile" button.
- The usertries to click on the "free Mobile" button but instead actually clicked on the invisible "delete all messages" button.
- In essence, the attacker has "hijacked" the user's click, hence this attack has get the name "Click jacking".

Syllabus Topic :Cookie Theft

1.5.10 Cookie Theft

GQ. 1.5.17 Explain Cookie Theft attack.

UQ. 1.5.18 What is Cookie Theft? Explain its functionality. (MU - April 2019)

- Cookie theft attack occurs when a hacker copies unencrypted session data and uses it to imitate the real user.

- Cookie theft also occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network.
- When the username and password for a given site will be encrypted, the session data travelling back and forth i.e. cookie is not.
- A hacker can access sites and perform malicious actions by imitating a person's cookie over the same network.
- The hacker is monitoring the network depending on the sites accessed, it could be anything from making fake posts in that individual's name to transferring money out of a bank account and so on.
- Hacker uses hacking software which made him easier to carry out such attacks by monitoring the packets going back and forth.
- This attack can be avoided by only logging in over Secure Socket Layer(SSL) connections or employing HTTPS protocol to encrypt the connection.
- Moreover, the best way is not to access sites over unsecured networks.

Syllabus Topic :URL Obfuscation

1.5.11 URL Obfuscation

GQ. 1.5.19 Explain URL Obfuscation attack.

- An obfuscated URL is a web address that has been obscured or concealed, which has been made to imitate the original URL of a legitimate website.
- It is done to make victim access a spoof site rather than the intended destination. These are one of the phishing attacks that can fool Internet users.
- The spoof site is often an identical copy of the original one in order to fool victims into revealing login and other personal information. It is also called a hyperlink trick.
- Obfuscated URL is used by legitimate websites to hide the true URLs of certain pages so that they cannot be accessed directly by the victims or allow certain procedures to be bypassed.
- Obfuscated URL is also used as an anti-hacking procedure.
- Obfuscated URL is termed as security through obscurity.

Syllabus Topic :Buffer overflow

1.5.12 Buffer Overflow

GQ. 1.5.20 Explain Buffer overflow attack in detail.

- A **buffer** is a temporary area for data storage and when more data gets placed by either program or system process, the extra data gets overflows.
- It causes some of that data to leak out into other buffers, which can over write or corrupt whatever data they were holding.
- In a **buffer-overflow attack,** the extra data sometimes holds specific instructions for actions intended by a attacker or malicious hacker.
- for example, the data could trigger a response that damages files, unveils private information or changes data.
- Hacker would use a buffer-overflow to take advantage of a program that is waiting on a user's input.
- There are two types of buffer overflows:
  1. stack-based
  2. heap-based.

1. **Stack-based buffer overflows :** Theses are more common among hackers, utilized applications and programs by using what is known as a stack which is memory space used to store victim input.
2. **Heap-based buffer overflows :** These are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program.

Syllabus Topic : DNS Poisoning

1.5.13 DNS Poisoning

GQ. 1.5.21 Explain DNS poisoning attack in details

- In DNS poisoning, it is the act of entering wrong information into a DNS cache so that DNS queries return an incorrect response and users are redirected to the wrong websites.
- It is also known as 'DNS spoofing.'
- IP addresses are the 'room numbers' of the Internet which enabling web traffic to arrive in the right places.
- DNS resolver caches are the campus directory as they store faulty information, traffic goes to the wrong places until the cached information is getting corrected
- There is no way for DNS resolvers to verify the data in their caches, so incorrect DNS information remains in the cache until the it expires, or else it is removed manually.
- A number of vulnerabilities make DNS poisoning possible, but the chief problem is that DNS was built for a much smaller Internet and based on a principle of trust.
- A more secure DNS protocol called DNS Sec has aims to solve some of these problems, but it has not been widely adopted yet.

Syllabus Topic : ARP poisoning

1.5.14 ARP Poisoning

GQ. 1.5.22 Explain Arp poisoning in details.

- In Address Resolution Protocol (ARP) poisoning, when an attacker sends falsified ARP messages over a local area network to link An hacker's MAC address with the IP address of a legitimate computer or server on the network.
- Once the hacker's MAC address is linked to an authentic IP address, the hacker can receive any messages directed to the authorized MAC address.
- As a result, the hacker can intercept, block or modify communicates to the authorized MAC address.
- ARP is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link Layer protocol.
- The protocol operates below the network layer as a part of the interface between the network and link layer of OSI Model.
- ARP is used when IPv4 is implemented over Ethernet.

Syllabus Topic : Identity Theft

1.5.15 Identity Theft

GQ. 1.5.23 Explain Identity Theft attack .

- Identity theft also known as identity fraud.
- It is a crime in which an utilize to obtains key pieces of personally identifiable information like pan card or driver's license numbers, in order to pretend someone else.

- The information can be used to obtain credit card, merchandise and services in the name of the user, or to provide the thief with false credentials.
- Identity theft is categorized two ways:
  1. True name Identity theft
  2. Account take over Identity theft

1. **True-name identity theft :** It means the thief uses personal information to open new accounts. The thief might open a new credit card account to establish cellular phone service or open a new checking account in order to obtain blank checks.
2. **Account-takeover identity theft :** It means the imposter uses personal information to gain access to the person's existing accounts. Typically, these thief will change the mailing address on an account and run up a huge bill before the victim whose identity has been stolen realizes there is a problem. The internet has made such attacks easier for an identity thief to use the information they have stolen, because they made transactions without any personal interaction.

Syllabus Topic : IoT Attacks

1.5.16 IoT Attacks

GQ. 1.5.24 Explain IoT attacks.

- Internet of Things (IoT) delivers considerable benefits to users but it also brings unrivalled security challenges.
- A part of the central security issue is that connected devices share implicit trust.
- This shared trust between connected devices means that the devices automatically transmit their data to each other immediately once recognition without first running any malware detection tests.
- The worst-case scenarios of these IoT security which gives dangers result in physical harm or even the loss of life.
- The first IoT security attacks began in 2016, and more are anticipated. Here's a rundown of the attacks, expectations for future attacks, and what safety measures IT professionals can use to increase IoT's protection.

Syllabus Topic BOTs and BOTNETs

1.5.17 BOTs and BOTNETs

GQ. 1.5.25 Explain botnet attack.

- A botnet is a network of systems combined together with the purpose of remotely taking control and distributing malware.
- botnet operators Controlled via Command-and-Control-Servers (C&C Server).
- They are used by criminals on a grand scale for many thing like exploiting online-banking data, stealing private information, DDos-attacks or for spam and phishing emails.
- Botnets consist of many different devices, all connected to each other – from smart phones, computers, laptops, and tablets to now also those "smart" devices.
- They have two main characteristics in common:
- They are enabled with internet and they are able to transfer data automatically over the network.
- Anti-spam technology can identify pretty reliably if one machine sends thousands of similar emails, but it's a lot harder to identify if those emails are being sent from various devices that are part of a botnet.
- All of them have same goal to sending thousands of email requests to a target in hopes that the platform crashes while facing to cope with the enormous amount of requests.

Syllabus Topic : Case-Studies, Recent Attacks – Yahoo

1.6 Case-studies

1.6.1 Recent attacks – Yahoo

Introduction

In December 2014, Yahoo's security team discovered that Russian hackers had obtained its credential like the usernames, email addresses, phone numbers, birthdates, passwords and security questions/answers for at least 3 billion Yahoo user accounts.

Background

- Yahoo's Chief Information Security Officer (CISO) stating giving various internal reports to SEC(Members of Yahoo senior Management) regarding the stolen of hundreds of millions of Yahoo users' personal data had occurred
- After the major attach in 2013 ,Yahoo's internal security team thereafter was aware that the same hackers were continuously targeting Yahoo's user database throughout 2015 and early 2016, and also received reports that Yahoo user details were for sale on the dark websites.
- Yahoo Company disclosed vast majority of the passwords involved had been hashed using the robust bcrypt algorithm.
- After couple of months, in December, they hide that earlier record with the disclosure that a breach in 2013, by a different group of hackers had compromised 1 billion accounts.
- Besides names, email addresses and passwords, dates of birth that were not as well protected as those involved in 2014 and also security questions and answers were compromised.
- Yahoo revised that estimate in October of 2017 and saying that, all 3 billion user accounts had been compromised.
- The breaches knocked an estimated $350 million off Yahoo's sale price. Verizon eventually paid $4.48 billion for Yahoo's core Internet business. The agreement called for the two companies to share regulatory and legal liabilities from the breaches.
- The sale did not include a reported investment in Alibaba Group Holding of $41.3 billion and an ownership interest in Yahoo Japan of $9.3 billion.
- Yahoo, founded in 1994, had once been valued at $100 billion. The company changed its name to Altaba, Inc after the sale.

Evaluation of the Case

- This case is not so much about the breach but it is about the cover up.
- Yahoo ran into trouble with the SEC, other regulators and civil opponent because it failed to disclose its data breaches in a reasonable amount of time.
- If Yahoo's properly investigate this case then post-breach injuries could have been largely avoided, and responded to, and disclosed the breaches in real time.
- SEC disclosures in particular must account for known incidents that could be viewed as material for securities law purposes.
- Yahoo was roundly applauded for its outstanding cooperation with law enforcement agencies investigating the attacks. These investigations go nowhere without extensive victim involvement. Yahoo stepped up in that regard, and that seems to have helped with the SEC, at least.
- Lawyers must play a key role in the investigation and response to cyber incidents, and their jobs

may depend on it. Cyber incident investigations are among the most complex types of investigations that exist. This is not an area for dabblers and rookies.

- Organizations need to hire in-house lawyers with actual experience and expertise in cyber security and cyber incident investigations.
- Yahoo's senior executives knew of the breaches well before they were disclosed. But they delay to disclose all this scenario in timely fashion.
- The failures of Yahoo's senior executives illustrate precisely why the board of directors now must play a critical role not just in proactive cyber security, but in overseeing the response to any major cyber incident.
- The board must check senior management when it makes the wrong call on incident disclosure.

Conclusion

- Securities fraud actions may fare much better than consumer data breach actions. The significant stock drop coupled with the clear misrepresentations about the material fact of a massive data breach created a strong securities class action that led to an $80 million settlement.
- The lack of financial harm to consumers whose accounts were breached is not a problem for securities fraud complainers.
- Consumer data breach class actions are routinely going to reach the discovery phase. The days of early dismissals for lack of standing are disappearing quickly.
- This change will make the proper internal investigation into incidents and each step of the response process much more critical.
- Although the jury is still out on how any particular federal judge will sentence a particular hacker, the data is trending in a very positive direction for victims.
- At least at the federal level, hacks focused on the exploitation of personal information are being met with stiff sentences in many cases.
- A hacker's best hope is to earn government-sponsored sentencing reductions due to extensive cooperation.
- This trend should encourage hacking victims to report these crimes to federal law enforcement and to cooperate in the investigation and prosecution of the cybercriminals who attack them.

Syllabus Topic : Adult Friend Finder

1.6.2 Adult Friend Finder

- In mid of October 2016, More than 412.2 million accounts are hacked Friend Finder Network, which included casual hook up and adult content websites like Adult Friend Finder was breached.
- Hackers collected 20 years of data on six databases that contains names, email addresses and passwords.
- The passwords were protected only by the weak SHA-1 hashing algorithm, which meant that 99 percent of them had been cracked by the time LeakedSource.com published its analysis of the entire data set of this site on November 14.
- CSO Online's Steve Ragan reported at the time that, "a researcher who goes by 1x0123 on Twitter and by Revolver in other circles posted screenshots taken on Adult Friend Finder (that) show a Local File Inclusion vulnerability (LFI) being triggered."
- He said the vulnerability, discovered in a module on the production servers used by Adult Friend Finder, "was being exploited."
- The hacked databases included site membership data, such as if the user was a VIP member, the IP address last used to log in, browser information, and if the user had paid for items.

- ZDNet verified the portion of data by contacting some of the users who were found in the data breach.
- Adult Friend Finder Vice President Diana Ballou issued a statement saying, "We did identify and fix a vulnerability that was related to the ability to access source code through an injection vulnerability."

Syllabus Topic : eBay

1.6.3 eBay

- In May 2014, 145 million users compromised by ebay data breach.
- The online auction giant reported a cyber attack in May 2014 that it said exposed names, email addresses, dates of birth and encrypted passwords of all of its 145 million users.
- The company said hackers got into the company network using the credentials of three corporate employees, and had completed inside access for 229 days, during which time they were able to make their way to the user database.
- They asked its customers to change their passwords, but financial information, such as credit card numbers, was stored separately and was not compromised.
- The company was criticized at the time for a lack of communication informing its users and poor implementation of the password-renewal process.
- The CEO of ebay, John Donahue said the breach resulted in a decline in user activity, but had little impact on the bottom line – its Q2 revenue was up 13 percent and earnings up 6 percent, in line with analyst expectations.

Syllabus Topic : Equifax

1.6.4 Equifax

- In July 29 2017,Equifax suffers data breach with personal information including Social Security Numbers, birth dates, email addresses, and in some cases drivers' license numbers of 143 million consumers; 209,000 consumers also had their credit card data exposed.
- Equifax, one of the largest credit bureaus in the U.S., said on Sept. 7, 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 147.9 million consumers.
- The breach was discovered on July 29, but the company says that it likely started in mid-May.

Syllabus Topic : WannaCry

1.6.5 WannaCry

Introduction

- The WannaCry Ransomware attack was a cyber attack conducted on a large scale, targeting only the Microsoft Windows operating systems.
- The WannaCry ransomware is spreading by email phishing, initial infection was likely through an exposed vulnerable SMB Port rather than email phishing as initially assumed.
- Ransomware attack would encrypt all the files in your computer ,to decrypt this one was asked to pay approximately $300 worth in bitcoins.

Background

1. Windows 8, 2003 and XP users were the main victims of such cybercrime, because the last released security update for XP was in April 2014, and many users didn't install the newer update as of March this year.

2. Microsoft stopped supporting these versions of windows, but to fight this cyber attack an emergency update was released for them.
3. There were many users using an unlicensed windows software. This thing makes them all the more vulnerable.
4. The WannaCry Ransomware attack has been carried out using tools that were stolen from the US security agency NSA, which had been stockpiling on a number of vulnerabilities around Windows OS, MacOS, etc.
5. This attack had exploited a vulnerability in Windows OS called Eternal Blue.

Evaluation

- They paid the asked amount still there are no recorded cases of anyone's computer getting decrypted after making the required payment.
- While trying to find the size of the attack, a person named Marcus Hutchins accidentally discovered a "kill switch" coded in the malware. He registered a domain name for the DNS sinkhole , which stopped the spreading of the virus like a worm that drastically slowing down the spread of the virus, giving time to come up with defensive measures.
- A person named Adrian Guinet introduced a "WannaKey", a solution to the WannaCry ransomware based on its flaws. He advised that it wouldn't work if the infected computer was rebooted or if the malware overwrote the decryption key.

Conclusion

1. WannaCry ransomware attack impacted a number of businesses, institutions and hospitals all over the world.
2. Businesses like Renault and Nissan had to pause their activities after some of their computers were affected.

- In hospitals, computer systems used for various purposes were affected, like computers and MRI scanners.
- Many critics said that WannaCry ransomware attack could have been prevented if people took steps to solve the defect on which the attacks were based, earlier.
- Some people even blame the governments for their inability to secure vulnerabilities.
- Estimates state that around 200,000 to 300,000 computer systems were affected in WannaCry ransomware attack in approximately 150 countries.

Syllabus Topic : Target Stores

1.6.6 Target Stores

Introduction

- In December 2013, major data breach of Credit/debit card information and/or contact information occurs that compromised 110 millions of users.
- The data breach actually began before Thanksgiving, but was not discovered until several weeks later.
- They initially announced that hackers had gained access through a third-party HVAC vender to its point-of-sale (POS) payment card readers, and had collected about 40 million credit and debit card numbers.
- By January 2014, the company upped that estimate, reporting that personally identifiable information (PII) of 70 million of its users had been compromised.
- That included names, email addresses, addresses, and telephone numbers.
- At the end, they got the final estimate is that the breach affected as many as 110 million customers.

- Later on, the Target's CIO resigned in March 2014, and its CEO resigned in May. The company recently estimated the total cost of the breach at $162 million.
- The company was upgrades with making significant security improvements. But, in May 2017 the settlement announced that gave Target 180 days to make specific security improvements that were described by Tom Kellermann, CEO of Strategic Cyber Ventures and former CSO of Trend Micro, as a "slap on the wrist." He also said that, "represents yesterday's security paradigm," since the requirements focus on keeping hackers out and not on improving incident response.

Syllabus Topic : Uber

1.6.7 Uber

- Uber creates and operates a mobile application that allows riders to connect with Uber drivers using their mobile phone. Uber collects certain personal information from riders, including name, phone number, email address, address and payment instrument.
- Uber also collects data from drivers, including driver license information, licensing information, and vehicle registration and vehicle inspection documentation.
- Uber also collects the live geographic location of riders and drivers in real time.
- As early as in September 2014, Uber experienced a data breach where Uber driver names and driver license numbers were accessed by hackers.
- In early 2014 an Uber engineer posted an access ID for Uber's third-party cloud storage on Github.com, this website designed to allow software engineers to collaborate.
- That post was accessible to the general public.
- On May 12, 2014, someone involved with Uber accessed the database that included Uber driver names and driver license numbers, etc.
- Uber discovered the breach in September 2014 but did not provide any notice to the affected drivers or regulators.
- The incident gave rise to multiple investigations by the Federal Trade commission (FTC) and state attorney general offices.
- In addition, Uber faced actions in several other states as well as federal class action lawsuits arising out of the breach.
- The Federal Trade Commision(FTC) expanded a prior settlement with Uber based on the company's failure to disclose the November 2016 breach.
- In Uber case, the FTC alleged that the San Francisco-based firm failed to live up to its claims that they closely monitored employee access to consumer and driver data, on an ongoing basis but in reality, Uber rarely monitored internal access to personal data. Uber reached a settlement with the FTC in August 2017 through a consent decree.
- They agreed to third-party audits for twenty years and to adopt a rigorous privacy-protection program.
- In April 2018, the FTC revised its complaint and proposal order after they disclosed the November 2016 breach.
- Uber has to submit the revised order to the FTC all of the reports from the required third-party audits as well as to disclose certain information regarding rewards Uber offers to individuals who report vulnerabilities in its software.

Syllabus Topic : JP Morgan Chase

1.6.8 JP Morgan Chase

- The JP Morgan chase largest bank in the nation was the victim of a hack during the summer of 2014 that compromised the data of more than half of all US households i.e. 76 million + 7 million small businesses.
- The data included contact information including names, addresses, phone numbers and email addresses as well as internal information about the users, according to a filing with the Securities and Exchange Commission.
- This bank said that none of customer money had been stolen and there was no evidence that account information for such affected customers account numbers, user IDs, passwords, dates of birth and Social Security numbers was compromised during this attack.
- The hackers were reportedly able to gain root privileges on more than 90 of the bank's servers that meant they could take actions including transferring funds and closing accounts.
- According to the SANS Institute, this bank JP Morgan spends $250 million on security every year.
- Federal authorities indicted four men, charging them with the JP Morgan hack plus other financial institutions in November 2015.
- The hackers GeryShalon, Joshua Samuel Aaron and Ziv Orenstein faced 23 counts, including identity theft, unauthorized access of computers, securities and wire fraud and money laundering that netted them an estimated $100 million.
- But they didn't identify the network that helped this fourth hacker for this breach.
- Shalon and Orenstein they both are Israelis, pleaded not guilty in June 2016. Aaron was arrested at JFK Airport in New York in December.

Syllabus Topic : Bad Rabbit

1.6.9 Bad Rabbit

- On October 2017, in Europe a new massive ransomware campaign rapidly spread .
- The malware dubbed Bad Rabbit rapidly infected systems of more than 200 major organizations mostly in Germany, Russia, Ukraine, Turkey and Japan in a few hours.
- It compromised systems at several big Russian media outlets, the Interfax news agency, and Fontanka.ru confirmed the malware hit them.
- The Odessa International Airport has reported on a cyber attack on its information system, but it is still unclear it is the same attack.
- IlyaSachkov is the head of Russian cyber-security firm Group-IB, told the TASS press agency that "In a number of the businesses, the work has been fully unfit servers and workstations square measure encrypted,"
- Initially, the Bad Rabbit campaign was not initially hit to the USA and other Western countries but according to antivirus firm Avast, threat has also been detected in the USA. bleepingcomputer.com reported, Theoretically, if a U.S. organization had infected partners in the targeted regions and were on the same WAN with

SMB access, Bad Rabbit could have spread laterally to the computers located in the USA,

- The US-CERT also warned of using unpatched and unsupported software, as they published a security advisory on the Bad Rabbit campaign.
- The US-CERT published alert that US-CERT has received multiple reports of ransomware infections, known as Bad Rabbit, in many countries around the world.
- A suspected variant of Petya, Bad Rabbit, is ransomware malicious software that infects a computer and restricts user access to the infected machine until a ransom is paid to unlock it, US-CERT discourages individuals and organizations from paying the ransom, as this does not guarantee that access will be restored. Using unpatched and unsupported software may increase the risk of proliferation of cyber security threats, such as ransomware.
- Many experts pointed out that the Bad Rabbit ransom ware is Petya-like malware the comparison of the source code with NotPetya revealed the existence of reused pieces of code.
- Hackers demands 0.05 bitcoin ransom (~ $280 at time of the attack) from victims to unlock their systems.
- The Bad Rabbit ransomware spread via drive-by download attacks like attackers are using fake Adobe Flash players' installer to trick victims into installing the malware.

Chapter Ends...

□□□