CS-573 Fundamentals of Cyber Security

THREAT-ASSET MATRIX

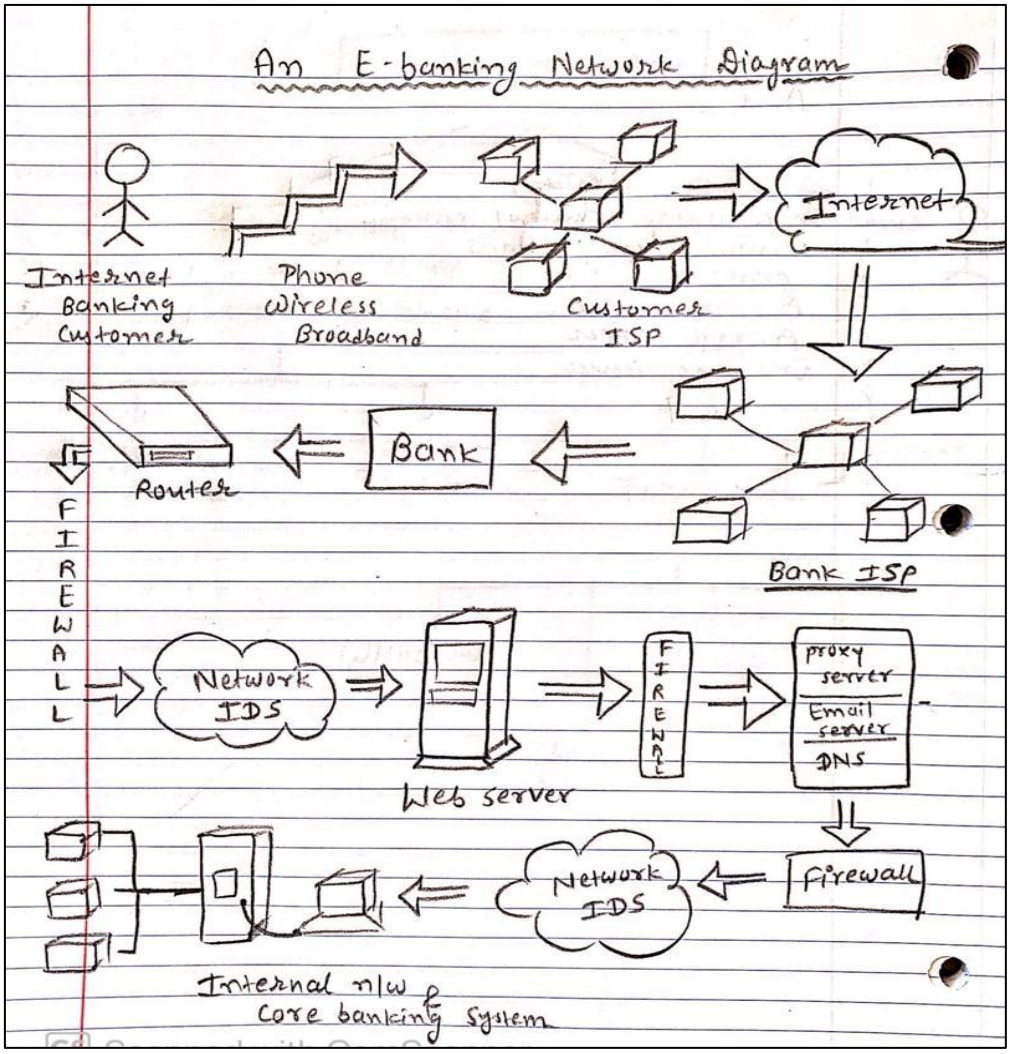
FOR AN E-BANKING

Name: Nidhi Chovatiya **CWID: 10457344**

In this study, a fictitious enterprise network for an E-banking is drawn, and a threat-asset matrix is created with the valued assets of this network and the threat types. Then, based on the probabilities and consequences, the security risk value for each cell in the matrix is estimated.

According to these elements such as, hardware, software, components, user, etc. we can determine the assets of the network.

Fictitious Enterprise Network for E-banking



Threat-Asset Matrix

We can decide the estimated value of the risk from the following formula,

Estimated Risk Value = Estimated Probability x Estimated Consequence

Estimated Probability and Consequence ratings are on a scale of 1-3

1 = Low
2 = Medium
3 = High

Assets/Threats	**Confidentiality**	**Integrity**	**Availability**	**Theft/Fraud**
E-commerce application	P=2| C=3| R=6	P=2| C=3| R=6	P=1| C=2| R=2	P=3| C=2| R=6
Web server	P=3| C=2| R=6	P=2| C=2| R=4	P=1| C=1| R=1	P=1| C=1| R=1
Application server	P=3| C=2| R=6	P=2| C=2| R=4	P=1| C=1| R=1	P=1| C=1| R=1
Security management	P=3| C=3| R=9	P=3| C=3| R=9	P=2| C=3| R=6	P=2| C=3| R=6
Firewall	P=3| C=3| R=9	P=3| C=3| R=9	P=1| C=3| R=3	P=1| C=1| R=1
Network IDS software	P=3| C=3| R=9	P=3| C=3| R=9	P=1| C=1| R=1	P=1| C=1| R=1
Phone	P=2| C=1| R=2	P=2| C=1| R=2	P=2| C=1| R=2	P=3| C=1| R=3
Core processing system	P=2| C=3| R=6	P=2| C=3| R=6	P=2| C=2| R=4	P=2| C=2| R=4
Computer	P=1| C=3| R=3	P=1| C=3| R=3	P=1| C=3| R=3	P=1| C=3| R=3
Router	P=2| C=3| R=6	P=1| C=1| R=1	P=1| C=1| R=1	P=1| C=1| R=1
Internet banking server	P=1| C=3| R=3	P=3| C=3| R=9	P=2| C=3| R=6	P=2| C=3| R=6
Students	P=2| C=3| R=6	P=1| C=3| R=3	P=1| C=3| R=3	P=1| C=3| R=3

Details of Each Cell of the Threat-Asset Matrix

Confidentiality: It gives an access to sensitive information by attacker

Integrity: It maintains the consistency, accuracy, and measure that how much data is trustable.

Availability: It checks the availability of Services and Data and ensures that it works properly.

Theft/Fraud: It Acquires Data or Services which are illegal.

E-commerce Application:

Actual Website built using Web Technologies like Node, React, JavaScript, etc.

- **Confidentiality**: Popular E-commerce websites are always under the raider for attacks to steal username and passwords of users and which results in identity theft and false orders.
- **Integrity**: E-commerce websites face a lot of Counterfeit products and products with inaccurate information, also fake reviews, and prices to scam the legit user.
- **Availability:** Since the website and its services are mostly accessed through the cloud the probability of the website being down is quite low and the consequences of it are also moderate because it is very easy to switch the website to a different server and isolate the issue.
- **Theft / Fraud**: E-commerce websites often prone to stealing of products without paying.

Web Server:

Server used to host the website and to manage the Domain. The web server and Internet banking server may have host-based intrusion detection system (IDS) software monitoring the server and its files to provide alerts of potential unauthorized modifications.

- **Confidentiality:** Web servers are the ones which are constantly hit by cyberattacks to get in the information and gain access, but they do not hold a lot of sensitive information and includes data for the website and other front-end services and acts as a gateway to interface with the backend APIs
- **Integrity:** Web servers are responsible to fetch and send accurate data to the APIs in-order to display accurate information to the user. An anomaly in this process can directly affects what the user will see on the website.
- **Availability:** Web servers are abundantly available by the domain hosts and are constantly switched between to balance load and maintenance.

Application Server:

Application Servers are used to maintain and manage the operation of different APIs used in the system.

- **Confidentiality:** Application servers are responsible to manage different APIs and to fetch and manipulate data on API calls and require specific authentication tokens and headers to process which can be prone to breaches and attacks
- **Integrity:** API calls made to the SQL Servers are at risk when there is data manipulation in the main data frame and can create an ambiguity on the overall consistency of the data.
- **Availability:** Application servers are built to sustain large amount of API calls and interfacing across different systems in the organization.

Security management:

- **Confidentiality:** High probability of being accessed from unauthorized users as it is threatened by the external threats even if it is protected with strict rules. If someone accesses it, the consequence would be very high because they are the main part of the system.
- **Integrity:** High probability of being changed by unauthorized users as it is threatened by the external threats. If someone changes it, the consequence would be very high as it may behave wrong which would be dangerous for the system.
- **Availability:** Low probability of being unavailable as it must always be ready to get controlled, but the consequence would be very high when it is not available as there may be an emergency that needs to be controlled at that moment
- **Theft/Fraud:** Low probability of being a subject of Theft/Fraud, but the consequence would be very high because they are the main part of the system.

Firewall:

a firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules. The Internet banking server has a firewall filtering Internet traffic from its internal network.

- **Confidentiality:** Firewalls act like the first line of defense and is used to tackle most of the cyber-attacks. It is used to monitor all traffic and is also affected the most during a cyber-attack. That's why it has high probability as well as high consequences.
- **Integrity:** High probability and high consequences, as the data packets which impersonate actual packets are of high chance to pass through the firewall making the system very vulnerable to attacks.
- **Availability**: At an event of firewall failures most systems also have backup firewalls installed to replace the damaged firewall.

Network IDS software:

Network IDS software may reside at different points within the network to analyze the message for potential attack characteristics that suggest an unauthorized intrusion attempt.

Confidentiality: Network IDS software is used to affected by mostly unauthorized users; hence it has high probability as well as high consequences.

Integrity: As it is resided at the various points within the network, for analyzing the message, it has high probability as well as high consequences.

Availability: Network IDS software are abundantly available; hence it has a low probability as well as consequences.

Theft/Fraud: There are very less chances for theft or fraud, so it has a low probability as well as consequences.

Computers

- **Confidentiality**: Unlikely to be accessed from unauthorized users as they are protected with strict rules but if someone access them, the consequence would be very high because it can be dangerous for the system.

- **Integrity:** Unlikely to be changed by unauthorized users as they are protected with strict rules. passwords but if someone changes it, the consequence would be very high as they may behave wrong which would be dangerous for the system.

- **Availability**: Low probability of being unavailable (computers can be locked in a certain time) but the consequence would be very high because there may be an emergency that needs to be controlled.

- **Theft/Fraud**: Unlikely to be a subject of Theft/Fraud as they are protected with strict rules, but the consequence would be very high because they may contain sensitive data.

Phones:

- **Confidentiality:** Medium probability of being accessed from unauthorized users. They are protected with strong passwords, but they can be easily moved from one place to another. If someone accesses them, the consequence would be low because they do not contain any sensitive data or have any control mechanism.

- **Integrity:** Medium probability of being changed by unauthorized users as they are protected with strict passwords. If someone changes them, the consequence would be low as they do not contain any sensitive data or have any control mechanism.

- **Availability:** Low probability of being unavailable and the consequence would be low as they do not contain any sensitive data or have any control mechanism.

- **Theft/Fraud:** High probability of being a subject of Theft/Fraud as they can be easily moved from one place to another, but the consequence would be low as they do not contain any sensitive data or have any control mechanism.

Core processing software:

Confidentiality: It has medium probability, but high consequences as it is affected to the system.

Integrity: It has medium probability, but high consequences as it is accessed by the unauthorized user.

Availability: Medium probability of being unavailable, also the consequence would be medium when they are not available at an emergency.

Theft/Fraud: Medium probability of being a subject of Theft/Fraud, also the consequence can be medium, not too high not too low.

Router:

The router will typically send the transaction around the other application servers directly to the Internet banking server unless it is a non-banking transaction.

- **Confidentiality**: Routers frequently go through ddos and wireless attacks in-order to gain access to the internal network. While all internal servers are connected through LAN and not WAP local users and system can be damaged by such attacks.
- **Integrity & Availability:** Routers are primarily used for packet transfer and routers between wireless systems and do not affect the duty of transferring data and receiving it.

Internet Banking Server:

The Internet banking server has a firewall filtering Internet traffic from the bank's internal network.

- **Confidentiality:** As it has a firewall for filtering, it has the low probability, but it has a very high consequences, as it is connected to the web service.
- **Integrity:** As it is connected to the internet it has very high probability as well as the high consequences.
- **Availability:** Medium probability of being unavailable, but the consequence would be very high when they are not available at an emergency.
- **Theft/Fraud:** Medium probability of being a subject of Theft/Fraud, but the consequence can be very high when losing them.

Student:

Internet banking customer sends an e-banking transaction through their Internet Service Provider (ISP) via a phone, wireless, or broadband connection.

- **Confidentiality:** Medium probability of being forced by unauthorized people to ask information about the system. The consequence would be high if third parties are able to get some sensitive information.
- **Integrity:** Low probability of being forced by unauthorized people to change some information with the system but the consequence would be high if they do something wrong
- **Availability:** Low probability of being unavailable, but the consequence would be very high when they are not available at an emergency
- **Theft/Fraud:** Low probability of being a subject of Theft/Fraud, but the consequence can be very high when losing them.

Assets/Threats	**Estimated Total Risk Value**
Security management	30
Internet banking server	24
Firewall	22
Core processing system	20

Network IDS software	20
E-commerce application	20
Students	15
Web server	12
Computer	12
Application server	12
Phone	9
Router	9