Unit 4 Seminar E-portfolio

Q. Read Shostack (2018) chapters 3 – 5 (that cover STRIDE and DREAD, Attack Trees, and Attack libraries) as well as Spring et al (2021) (that discusses the history and some failings with CVSS) and then create a threat model based on one of the following scenarios:

1. A large international airport based in the United States of America.
2. A large international bank based in the UK.
3. A large nuclear power station in France

Threat Modelling Exercises: Threat Model of an international Bank based in the UK.

Threat modelling assessment of a banking applications and operational activities are vital in banking business as its daily operations is becoming more complex and there is need to identify and address potential security vulnerabilities. These vulnerabilities can be classified under Credit/debit cards, operational Market, Liquidity, Operational, Compliance / Legal /Regulatory and Reputational risks (HSCB UK).

- **Identification of targeted components.**

Some of the identified components for a banking application would be user interface, data storage, data processing functions, authentication and authorization functions and network connections or third-party integrations (third-party payment processors e.g., PayPal, Stripe, Square).

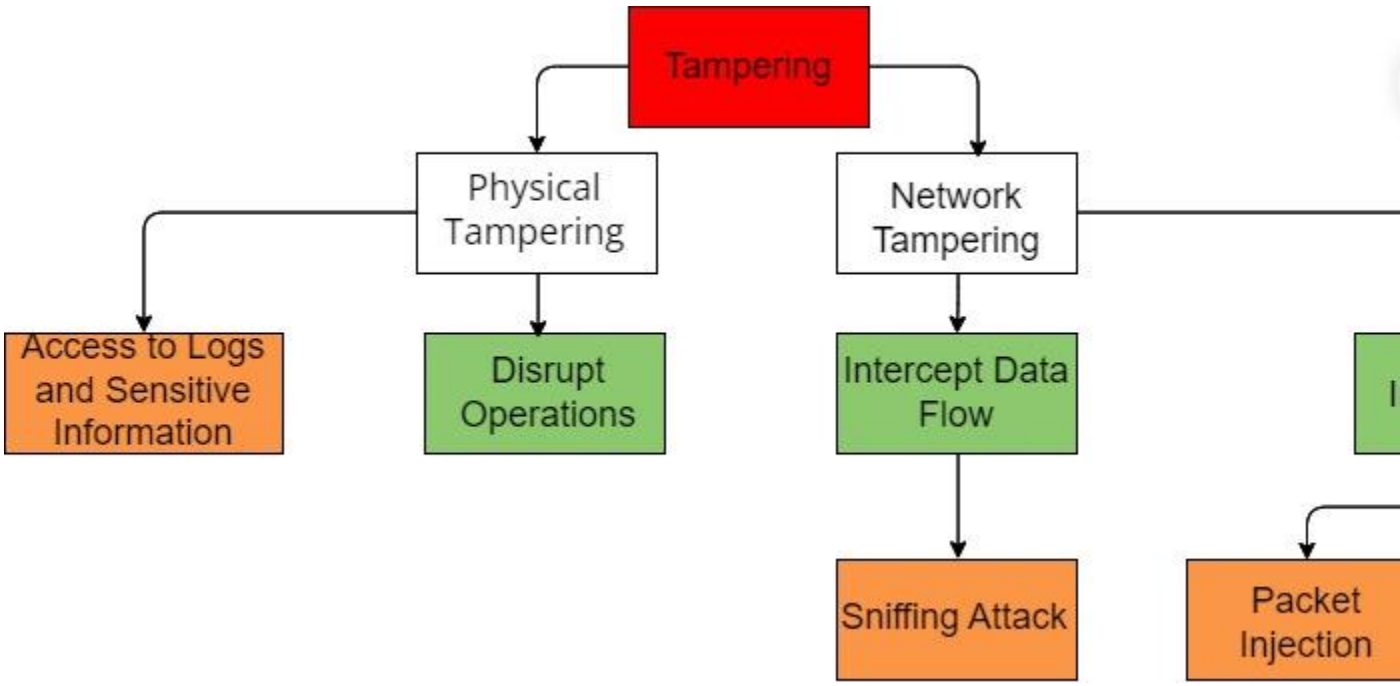
- **STRIDE Modelling assessment on an International Bank**

S/N	Threats	Definition	Potential Actor's Activities
1	Spoofing	Impersonation representing oneself or another entity to gain access to sensitive information	• Phishing attacks trick users into providing login credentials or personal information. • Impersonation of a bank or financial institution to gain access to customer account information. Employees and credit card customers are usually victims.

2	Tampering	Modifying data or functionality to gain unauthorized access or manipulate data	• Changing transaction details to redirect funds to an unauthorized account. • Modifying customer account data to gain access to sensitive information. These mainly remotely done by attackers or insider threat.
3	**Repudiation**	Denying responsibility for an action or transaction	• Disputing a legitimate transaction to obtain a refund or credit. • Falsely claiming that a transaction was unauthorized to avoid liability. Third party payment vendors are access customer's credentials with assist of insider and it will not be traced to them when the evidence is deleted.
4	**Information Disclosure**	Revealing sensitive information to unauthorized parties	• Accessing sensitive customer information through a data breach or other unauthorized means • Leaking transaction or account information through unsecured channels or data storage The above could fall into non-compliance of GDPR policy on data privacy.
	Denial of Service	Disrupting or impairing access to the application or its resources	• Launching a distributed denial of service (DDoS) attack to overwhelm the application's servers. • Crashing the application through intentional or unintentional means. This makes the system unavailable to the authentic user and competitors can use the threat to fight competition.
	Elevation of Privilege	Escalating user privileges to gain unauthorized access or perform unauthorized actions	• Exploiting a vulnerability in the application to gain administrative access. • Using a stolen or brute-forced user account to gain elevated privileges. The system Administrators are victim to attacker by disclosure of credential log-in.

The above has shown that banking application's potential vulnerability and threats could include phishing attacks to obtain login credentials, unauthorized modification of transaction details, and data breaches to access customer account information.

A sample of Attack Tree on Tampering threat of a Banking application System:



- **Evaluate the Severity of the Threats**

After identifying potential threats, the next step is to evaluate the severity of each threat based on the likelihood and impact of a successful attack. This can help prioritize which threats to address first and determine the level of effort required to mitigate each threat. From the above identified threats using CVSS scoring framework, a data breach that compromises customer account information would be considered a high-severity threat. This is evidenced by one of HSBC data privacy policy that states 'customers' and employees' trust and confidence in how data is collected, use, and share is very important to bank and that is why they continuously work to enhance the systems, processes, procedures, and controls. Also, a phishing attack with a low success rate would be considered a lower-severity threat.

- **Conclusion**

Threat modelling technique is an important process for identifying potential security vulnerabilities in a system and the STRIDE model is a tool for analysing and mitigating potential threats based on six categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. This assist to identify potential vulnerabilities, develop and implement mitigation strategies to secure a system against

potential security breaches. In summary. STRIDE is a model of threats that can be used as a framework in ensuring secure application design (Hewko.A,2021).

Reference:

- Hewko,A(2021),Software Secured, STRIDE Threat Modelling: What You Need to Know. Available from: https://www.softwaresecured.com/stride-threat-modeling/[Accessed 29 August 2023].

- HSBC, Operational risk, Available from: https://www.hsbc.com/who-we-are/esg-and-responsible-business/managing-risk/operational-risk#:~:text=They%20could%20include%20a%20failure,well%20as%20from%20external%20events. [Accessed 29 August 2023].

- Shostack.A. (2014) Threat Modelling : Designing for Security. Available from:https://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=1629177&pq-origsite=primo[Accessed 26 August 2023].

- University Essex Lecture Cast unit 3. Introduction to Threat Modelling and Management, Available from: https://www.my-course.co.uk/Computing/Cyber%20Security/SRM/SRM%20Lecturecast%202/content/index.html#/ [Accessed 25 August 2023].