**Threat modelling exercise for a large international bank based in the UK.**

**Introduction**

The following exercise is based on the guidelines provided by the Threat Modelling Manifesto to capture all possible threats that an organization can face. As stated by Allen-Addy (2023), the Threat Modelling Manifesto is deliberately non-specific on how to develop the model to avoid overlooking important threats. However, the four-question framework provided by Shostack et al. (2020), together with the OWASP Threat Modelling Cookbook and the ATT&CK libraries, is used to apply the best possible practices.

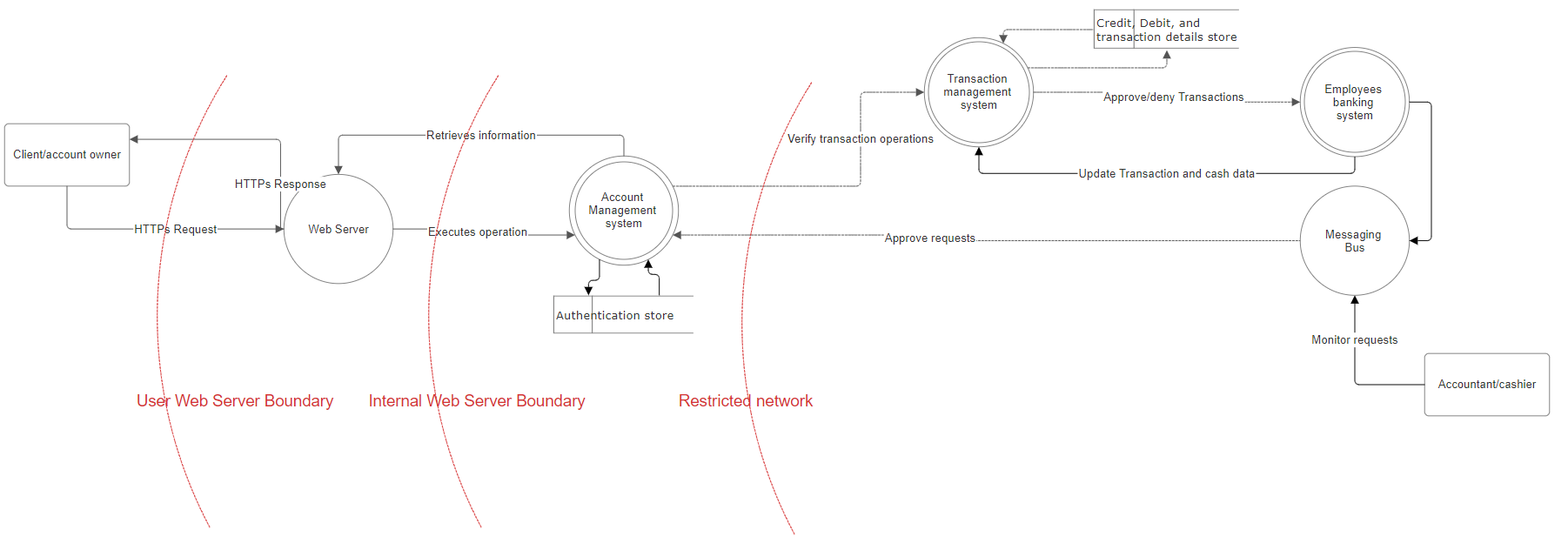
1. **What are we working on?**

A bank recently migrated its business to a cloud provider with the purpose to enhance security and overall business operations. Most of the infrastructure has already been migrated to a cloud provider, however, some local databases remain intact, along with an old web-based application used by everyday clients.

The main focused is on achieving successful and secure business operations while acknowledging the risks caused by human, system, environmental or other process-related interactions.

1. **What can go wrong?**

The below data flow diagram (DFD) depicts regular business operations when a user interacts with the bank's web-application. The requests are passed between multiple systems, ultimately increasing the risk possibilities described below as per STRIDE methodology (Jacob, 2023).



|  |  |
| --- | --- |
| **Threat** | **Risk** |
| **S**poofing | * Stealing personal or company information * Session hijacking * Bypassing access controls * Forgery of Web Tokens |
| **T**ampering | * An attacker intercepts a payment request made by a user and modifies the transaction data * An attacker performs a code injection in a platform application form |
| **R**epudiation | * An Illegal or malicious operation carried out by an adversary who denies their involvement * A user makes a transaction on the platform and then denies having made it |
| **I**nformation disclosure | * Extracting sensitive data in the platform API's * A disgruntled payment platform employee steals information from the user database and discloses it online |
| **D**enial of service | * Unresponsive application because of DDoS attack |
| **E**scalation of priviliges | * performing malicious actions, such as changing critical settings, tampering with transactions, or stealing sensitive information |

Additionally, common network related risks as proposed in ATT&CK library (2021) include:

* Adversary-in-the-Middle may seek to modify network traffic
* Adversaries may abuse Internet browser extensions to establish persistent access to victim systems
* Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network
* Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts

1. **What are we going to do about it?**

|  |  |
| --- | --- |
| **Risk** | **Mitigation** |
| Spoofing | * Don’t open attachments that you don’t expect to receive, especially if they have unusual file extensions **Regularly change your passwords** * **Check before you click** * **Use a dedicated secure browser** (Belcic & Farrier, 2021) |
| Tampering | * Enforce Encryption for Data-at-Rest and Data-in-Transit  Copy-on-Write File SystemsData Integrity using HMACs (Cypress Data Defense, 2020) |
| Repudiation | * Audit and logging mechanisms to track all system activity and suspicious actions (Thevarmannil, 2022) |
| Information disclosure | * Encryption of sensitive data and access control mechanisms to restrict data accessibilty (Thevarmannil, 2022) |
| Denial of service | * Load balancing and traffic filtering systems to mitigate traffic spikes and spread load evenly (Thevarmannil, 2022) |
| Elevation of priviliges | * Implementing the principle of least privilige and role-based access to limit the priviliges of each account (Thevarmannil, 2022) |
| Adversary-in-the-Middle | * Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce adversary in the middle (AiTM) conditions * Disable unnecessary legacy network protocols * Using network intrusion detection and prevention systems (Layne, 2023; Center for Threat-Informed Defense, 2020) |
| Browser Extensions | * Set a browser extension allow or deny list * (Ross, 2024; Center for Threat-Informed Defense, 2018) |
| Deploy malware | * Limit software installation * Update Software reqularly * Active Directory Configuration to ensure proper system and access isolation for critical network systems through use of group policy (Gumke et al, 2024; Center for Threat-Informed Defense, 2017) |
| Modifying web templates | * Leverage Antivirus/Antimalware tools * Network Intrusion Prevention * User Training   (Wiltse, 2022; Center for Threat-Informed Defense, 2018) |

1. **Did we do a good enough job?**

Above provided data flow diagram depicts the common business logic for a bank system. However, systems comprise of multiple interrelated interactions, ultimately enhancing the possibilities of a risk occurance. Above mentioned risks and mitigations are therefore general, whereas detailed threat models should be considered for separate use-cases, specific to business operations.

**References:**

* Allen-Addy, C. (2023) What is Threat Modeling Manifesto. IriusRisk. Available from: <https://www.iriusrisk.com/resources-blog/what-is-the-threat-modeling-manifesto> [Accessed 28 June 2024]
* Belcic, I. & Farrier, E. (2021) What Is Spoofing and How Can You Prevent it?. Avast. Available from: <https://www.avast.com/c-spoofing> [Accessed 28 June 2024]
* Center for Threat-Informed Defense (2021) MITRE ATT&CK. Available from: <https://attack.mitre.org/> [Accessed 28 June 2024]
* Cypress Data Defense (2020) How To Prevent Data Tampering in Your Business. Available from: <https://www.cypressdatadefense.com/blog/data-tampering-prevention/> [Accessed 28 June 2024]
* Jacob, A. (2023). Examples of STRIDE threats for payment applications. Medium. Available from: <https://medium.com/@arielhacking/examples-of-stride-threats-for-payment-applications-87a0ad0c3a21> [Accessed 28 June 2024]
* Shostack et al (2020) Threat Modeling Manifesto. Shostack + Associates. Available from: <https://shostack.org/blog/threat-modeling-manifesto/> [Accessed 26 June 2024]
* [Thevarmannil](https://www.practical-devsecops.com/author/misbahpdso/), M. (2022) What is STRIDE Threat Model?. practical-devsecops. Available from: <https://www.practical-devsecops.com/what-is-stride-threat-model/> [Accessed 28 June 2024]