Summaries

- Braiterman et al 2020: Threat modeling manifesto
    - Four guiding questions: What are we working on? What can go wrong? What are we going to do about it? Did we do a good enough job?
    - Useful patterns for threat modelling: systematic (thorough) approach, using both theory and creativity, diverse team, utilizing tools, continuous refinement, understanding the bigger picture
    - Unhelpful patterns: “hero threat modeler” mindset, overfocusing, analyzing problems without reaching for solutions, a single threat model
- Shostack 2022: Welcome to the Worlds Shortest Threat Modeling Course
    - Collaboration is vital to threat modeling
    - Sketching is often the first part of answering "what are we working on?"
    - Your threat model should be recorded. Typically drawing tools are used.
    - Data flow modeling is used in threat modeling. 5 elements: outside entities, processes (under your control), data flows, data stores, trust boundaries
    - STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privileges) is a mnemonic used to think about possible threats.
    - Threat modeling informs risk management.
    - At the end of threat modeling, you should ask if participants would recommend it to others. If the answer is no, the threat modeling needs to be improved.
- OWASP CheatSheets Series Team 2021: Threat Modeling Cheat Sheet
    - Threat modelling should be constantly updated and maintained (and ideally integrated into the development process).
    - Four basic steps
        - System modeling – understand the system to understand which threats most apply to it
        - Threat identification and ranking
        - Mitigations
        - Review and validation
    - After identifying threats, they are typically ranked by severity.
    - Risk responses
        - Mitigate (must be actionable, not hypothetical), must be documented

        - Eliminate
        - Transfer
        - Accept
    - Questions for review
        - Does the DFD accurately reflect the system?
        - Have all threats been identified?
        - For each threat, has a response been agreed upon?
        - Are mitigation approaches effective?
        - Has the model been documented?
        - Can mitigations be tested and can success or failure be measured?
- Ep159 Vastaamo: https://darknetdiaries.com/episode/159/
    - Cyberattack on a psychological services company called Vastaamo in Finland in 2020. A hacker got personal information and therapy notes for over 30,000 people. He held the data ransom for 40,000€ and leaked therapy records daily until they were paid. He also tried to blackmail individuals whose data he had. The company's security was very lackluster and hacking it was easy, according to the hacker.
    - The hacker accidentally posted his entire home directory on the darkweb, so some people were able to find the hacker's IP address and the server he used. The police had a prime suspect, a Finnish man named Julius Kivimäki, but couldn't find him for years. In 2023, the hacker was found in Paris hiding under a false ID.
    - The impact was severe since victims were largely people struggling with mental health issues. Some people even ended their lives because of it. The company also collapsed because of this, and the CEO was prosecuted for failing to protect the data and sentenced to a 3-month prison sentence.

Security hygiene

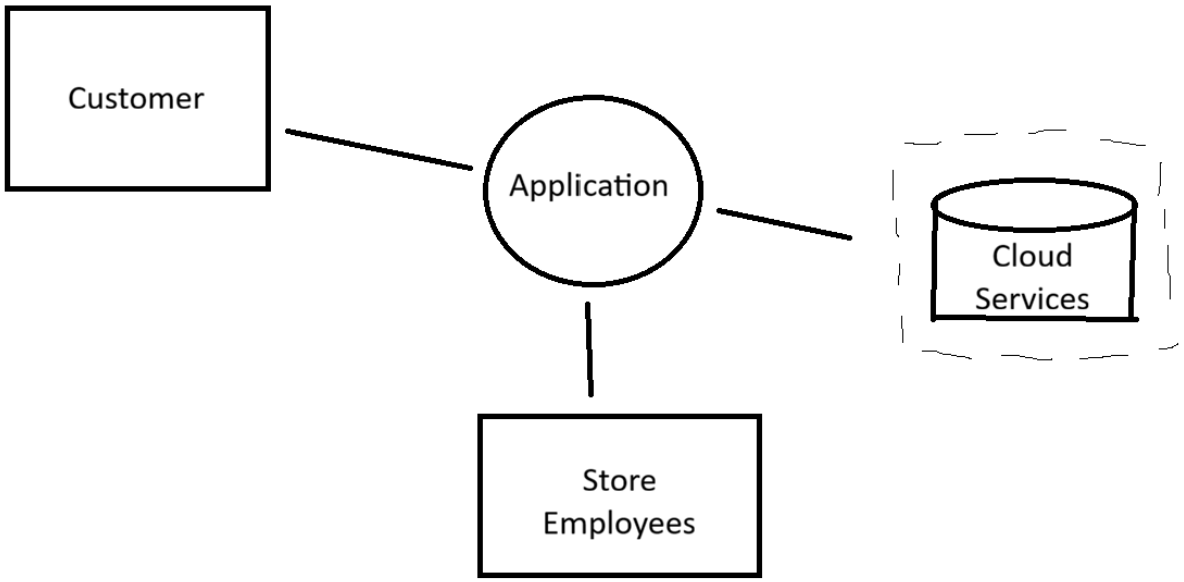
- Use different passwords.
- Use randomized passwords.
- Do not share your passwords.
- Do not write passwords and keep them in obvious locations.
- Change passwords periodically.
- Do not click links from emails if you don’t recognize the sender and/or the link.
- Don’t send private information via email.

- Don’t click on pop-up ads.
- Don’t download something from the internet if you don’t know what it is and where it came from.

Imaginary Company’s Threat Model

Storemart is a department store with an app that allows customers to place online orders to pick up in the store. The company’s assets include customer data (names, phone numbers, emails, order history, purchase method) and their application. The customer data is the highest priority. Customers interact with the application and expect a smooth purchasing experience, being able to purchase directly with the application, save their data for future purchases, find information about previous purchases, and receive personal recommendations.

Below is the systems model for the company:



Using the STRIDE model, some identified risks include access through the application by accessing employee or customer passwords, intercepting a customer’s session via their network, tampering with the application’s code, accessing users’ payment information and making purchases, employees sharing customer data, DDoS attacks making the application unusable, and a user manipulating the application to gain advanced privileges. The biggest risks, based on probability and potential monetary loss, are gaining employee passwords and accessing users’ payment information. These are the most likely to occur and can lead to serious losses, not to mention a loss in customer trust. The lowest risks are the application’s code being altered (high loss but very low probability) and DDoS attacks (low losses).

Some of the threats to the application’s integrity can be mitigated by adding security features to the software. In addition, employees can be trained continuously on good password practices and the use of confidential data to mitigate risks, and requiring employees to update passwords periodically can help. Two factor authentication can help prevent

unwanted purchases on customers' accounts. Customers' sessions being intercepted via insecure networks is a risk that can be transferred to the customer because of the company's inability to prevent this issue. DDoS attacks are a risk that can be accepted given their low priority.

According to the Finnish government, local threats to cyber security are on the rise. The number of serious attacks in 2025 increased significantly and software vulnerabilities became more frequent. Phishing attempts have also become more common. Attackers are typically international and most attackers are individuals, however, threats from the Russian and Chinese government are ongoing concerns. (Finnish Government 2025) It is highly unlikely that Storemart would need to worry about attacks from a government; rather, it is the individual actors that are likely to attack them.

After threat modeling is completed, the team needs to assure that the plan is acceptable and all risks are addressed properly. Once the plan is implemented, there should be measures put in place to access their effectiveness, maintain the plan, and alter the plan as new risks are discovered or measures are found to be lacking.

Sources

Finnish Government 2025. Cyber security threat level remains high – serious cases on the rise. URL: https://valtioneuvosto.fi/en/-/38197657/cyber-security-threat-level-remains-high-serious-cases-on-the-rise?languageId=en_US. Accessed: 20 January 2026.