STRIDE Model as a potentially strong security analysis and threat modeling tool for E2EE Messaging Applications and Social Media Networks

Karan Murthi

High School Student
Doha , Qatar

Abstract: Due to the increased reliance on social media networks brought on by the COVID-19 pandemic, individuals are now more vulnerable to threats like hackers and scammers. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) is a safe software development model that Microsoft's Security Development Lifecycle (SDL) has adopted to handle and mitigate these security vulnerabilities. Eavesdroppers on communication channels threaten E2EE (end-to-end encrypted) applications like messaging apps and social media networks. To counter this, the STRIDE model analyses the network's security properties, such as authentication, non-repudiation, confidentiality, integrity, availability, and authorisation, identifying potential threats and vulnerabilities. Additionally, the widespread adoption of social media platforms in the economy has prompted organisations and companies to prioritise information security and privacy, an emphasis reflected in the Agile, OWASP, and DevOps processes. This paper also emphasises the requirement for security-improving countermeasures. Implementing fail-safe defaults and balancing security requirements with shared state are suggested for E2EE applications. Two-Factor Authentication (TFA) through SMS and user awareness and education on online etiquette are suggested as ways to prevent dangers for social media networks. The efficacy of the STRIDE model for threat management in E2EE messaging apps and social media networks is examined in this study. This discussion summarises ideas from the arguments made by Sharma, et al. (2023) and Chowdhury, et al. (2023). The STRIDE model is helpful, but this research also recognises that technology continually evolves and that changes are needed to ensure the model can minimise threats in the future.

Keywords: STRIDE Model, E2EE Messaging Applications, Social Media Networks

1. Introduction

Like any data flow diagram (DFD), STRIDE captures key processes, data stores, and data flow between the main elements of the network – checking the process flow between trust boundaries and delegating partitioned data that are free from any forms of adversarial interference [5]. All data that were processed are then evaluated along the six key threats which are spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege which is done by negativing important security properties of the network which are authentication, non-repudiation, confidentiality, integrity, availability, and authorization [1].

In [5], an experiment was carried out to test E2EE susceptibility to threats of both applications that rely on the Signal protocol (like WhatsApp and Viber, since Viber uses the Double Ratchet algorithm, which is not directly using Signal protocol) and those that do not (like Telegram and Wickr Me, which have their own messaging protocols). The experiment created DFDs for each app based on the security properties published in their documentations, before adding a desktop client for monitoring. The figure below shows the threat model.

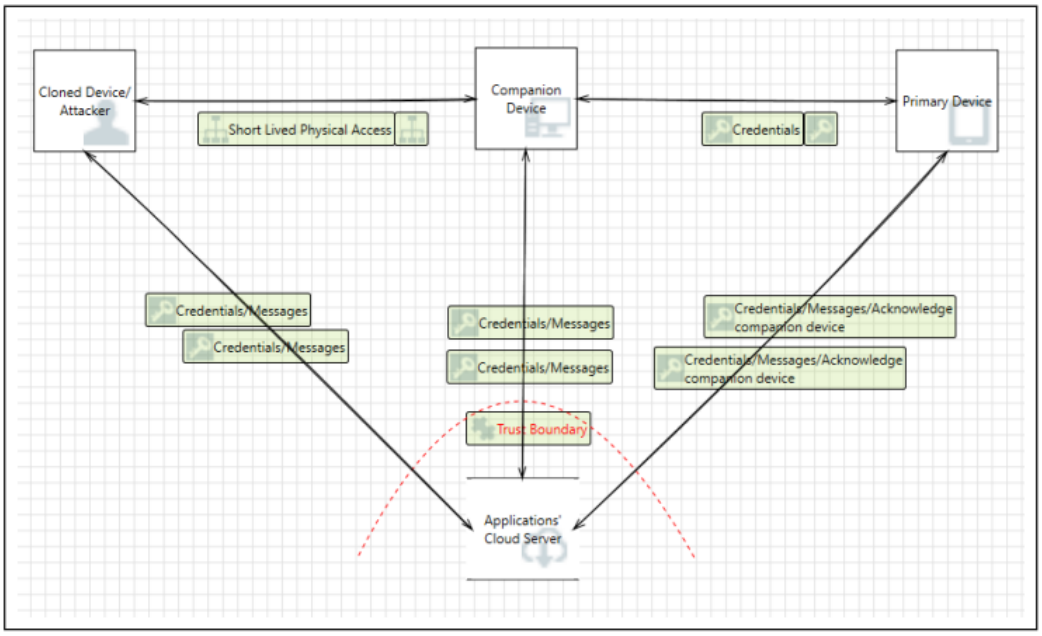

Figure 1: DFD for Signal, WhatsApp, and Telegram desktop applications

The experimental set up is as follows: one android phone and one iOS phone are used to receive SMS. A test for threats using STRIDE model was employed. Spoofing - The desktop client was installed in an attacker's machine and configured with a second account. The experiment then copied the state of the victim's machine and placed the state in the attacker's machine. No Tampering was performed on the victim's machine. Repudiation was performed when communication between the legitimate participant, the attacker, and other legitimate parties were repeatedly performed to check for any deviations in the communication route. Information disclosure was employed when the cloned desktop was set up for forward and backward secrecy. Denial of service attacks were performed to check if the victim can be thrown out of the network by the cloned machine. Elevation of privilege was run by capturing the credentials using a tls interceptor from the rooted device.

As E2EE mobile applications assume that threats will always come from eavesdroppers and that eavesdroppers need only decrypt authentication and key-sharing mechanisms, it removes all other elements from its consideration [5]. However, the experiment found some problems that could reside in the mal-boundary and go undetected for long periods, which are: a) attacker masquerading as a victim – the experiment shows that the attacker's machine does not influence the success of the attack but rather Signal authentication credentials (like username and password) can be easily retrieved from the SQLite database directory; b) forward secrecy can be compromised as the client state information contains the private pre-key and cloning the victim's desktop allows attackers to mirror everything that the victim has installed, resulting in successful attack; c) the experiment showed that E2EE mobile apps are un-scoped for threats, security and privacy consequences and is thus vulnerable to malicious entities. Although the dynamics of how the STRIDE Model can expose vulnerabilities vary from one mobile application's communications protocol to another, a general threat to vulnerability as discussed previously can be established.

2. STRIDE Model and Social Media Networks

STRIDE model threat evaluation for social media networks is relatively straightforward as discussed in [6]. To perform security analysis on major social media networks, the following were considered in [6]: **Spoofing** was performed by manipulating the data sent across social media networks to look like it has come from legitimate sources (email spoofing, MAC spoofing, and IP address spoofing). **Tampering** is modification of the information sent across nodes and **repudiation** denies the participation of the victim's device into the communication channel. **Denial of service** was also performed to make the victim unavailable to legitimate users.

In the paper presented by [6], STRIDE model checks for confidentiality, integrity, availability, authenticity, and accountability on the major assets used in social media networks (i.e., hardware, software, and data). The research then determines the risk levels of multiple threats, assigning them weight percentages and impact on security.

In the case of Facebook, compromised account attacks are the most prevalent way for users to lose partial or full control of their login credentials, either through phishing scams or by utilizing cross-site scripting and employing bots to gather login credentials. This can also be done by employing socware or malware in the form of events, pages or applications capable of redirecting links to malicious contents. Facebook is also plagued with identity clone attacks where malicious

wares create similar profiles on false pretenses, spreading malicious content into the network; creepers, cyberbullies, and clickjacking where victims are lured to click on a link only to be redirected somewhere that collects personal data and information [6].

Threat	Violated Property	Definition	Example
Spoofing	Authentication	Pretending to be someone else	Make fake Facebook account
Tampering	Integrity	Modify post on user's timeline	Delete/change post and message of others
Repudiation	Non-repudiation	Claim the real user	Multiple accounts and profile
Information Disclosure	Confidentiality	Unauthorized party gain access to Info	Malicious links, e.g., phishing URL
Denial of Service	Availability	Service unavailable to user	Overflow system, shutting down system

Figure 2: STRIDE threat model for Facebook

In Figure 2, the STRIDE Model easily identifies the THREAT Model of Facebook where each step of the STRIDE model was given an example (Spoofing by making fake Facebook account, tampering by deleting or changing posts, etc.).

3. Threat Modelling and Countermeasures

In the context of E2EEE, trust boundaries and administrative boundaries are two different things. Trust boundary is where security controls are in place and administrative boundaries are spaces where system policies that are designed to counter threats are stored. Pushing a lot of restrictions on the trust boundary will cause legitimate users to experience heavier load from security tasks which could impact the usability of the system [5]. On the other hand, changing the administrative boundary (loosening up) could result in the emergence of new threats, rendering the STRIDE threat model ineffective at best.
In [5], the following suggestions were proposed, to secure the E2EE communications channel: a) E2EE messaging applications are required to reconcile security requirements with shared state; and b) implement fail safe defaults where participants with access to devices should not be able to use the access maliciously.
In [6], it was found out that Two-Factor Authentication (TFA) can be performed via SMS to deter threats within social media networks, along with the generic discussions where user awareness and education on online etiquettes can be utilized to lower the risk of account exposure to online threats.

4. Conclusion

STRIDE model is decent threat management tool both for E2EE mobile applications and for social media networks as was seen in the paper. This doesn't mean, however, that STRIDE Model is an encompassing model already as threats to online security and privacy evolve as fast as the tools that are created to deter them. Nonetheless, the logical framework provided by the STRIDE Model to deter threats of attack is sufficient at this stage and could be useful in the next few versions of network security protocols.

5. References

[1] Howard, M. & Lipner, S. (2006). The security development cycle. Microsoft Press Redmond, vol 8.
[2] The OWASP Foundation. OWASP secure coding practices quick reference guide. https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf
[3] SAFECode. Practical security stories and security tasks for agile development environments. http://safecode.org/wp-content/uploads/2018/01/SAFECode_Agile_Dev_Security0712.pdf
[4] Microsoft. Secure DevOps. https://www.microsft.com/en-us/securityengineering/devsecops
[5] P. D. Chowdhury, M. Sameen, J. Blessing, N. Boucher, J. Gardiner, T. Burrows, R. Anderson, A. Rashid. (2023). Threat models over space and time: A case study of E2EE messaging applications. arXiv preprint: arXiv: 2301.05653
[6] K.R. Sharma. W. Chiu, W. Meng. (2023). Security Analysis on Social Media Networks via STRIDE Model. arXiv preprint: arXiv: 2303.13075