Forking Attacks: Two Ways, No Worries

Matija Roncevic
matija.roncevic@fau.de
Friedricht-Alexander-Universität Erlangen-Nürnberg

1 INTRODUCTION

Almost every noteworthy application has embraced cloud computing. The range of applications that benefit from cloud services spans from small smartphone apps to sophisticated large language models to commonly used GitHub repositories. The clear reason for its popularity is the ability to store, manage, and process data more efficiently than ever before. The shift to cloud services offers numerous advantages, including scalability, flexibility, and cost-effectiveness. However, it also introduces significant security challenges. With the inclusion of numerous critical applications and sensitive data, the importance of secure environments has increased. Cloud security involves a diverse range of practices, technologies, and policies aimed at protecting data, applications, and services distributed across cloud environments. The baseline of protection is realized by implementing firewalls and encryption; however, the sophisticated and evolving nature of cyber threats often outpaces the safety measures these solutions provide. This calls for advanced security solutions that can safeguard data even in potentially compromised environments.

Trusted Execution Environments (TEE) like Intel Software Guard Extensions (SGX) is such an advanced security solution. Intel SGX is a set of hardware-based security features that create isolated execution environments, known as enclaves [2]. [Enclaves are secure areas of memory where sensitive data and code can be executed and stored in isolation from the rest of the system.] These enclaves are designed to protect sensitive data and code from being accessed or modified by unauthorized parties, even if the operating system is compromised. SGX provides a robust mechanism for ensuring the confidentiality and integrity of data processed in the cloud. Despite its strengths, Intel SGX still has its own vulnerabilities. The enclaves itself are in fact isolated from adversaries, however the relaiability on the inputs can‘t be ensured without additional savety meassures. Those attacks are labeled as rollback attacks. More explanation about rollbacks, maybe in background? Forking attacks on the other hand, aim on creating multiple instances of an enclave, leading to unauthorized data access and manipulation. This is accomplished by running those simulainously and exploiting the fact, that all those enclaves will return correct but often stale states. I.e. counters for passwort attempts can be reset to gain unlimited tries, despite the limit for tries is set to an finite number [1]. Understanding these attacks and developing effective mitigation strategies is essential for ensuring the security and trustworthiness of cloud-based applications relying on SGX.

2 BACKGROUND

The concepts which are discussed in this paper, will be explained further to provied an comprenhensive knowledge beforhand.

TEEs aim to increae the saveness of data and exacerbate the tempering with crucial code sections, by allowing the processor to have protection through different implementations like Intels SGX enclave system.

3 BODY

4 CONCLUSION

5 REFERENCES

[1] - ESCCC [2] - NFW