Review of

# FORESHADOW: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution

Jo Van Bulck et al.

---

## What is the problem?

Security objectives of Intel SGX (Software Guard Extensions) are not met by the current implementations. They are still susceptible to a processor vulnerability that allows for unauthorized memory access in transient out-of-order executions.

## Summary

Foreshadow leverages a speculative execution bug that leaks enclave secrets in plaintext due to a vulnerability that allows for unauthorized memory accesses. The attack can be mounted by an unprivileged adversary without root access to victim's machine. They further prove the attack by demonstrating the extraction of full cryptographic keys and validate it by remote attestation responses.

## Key Insights

- The paper identifies that despite Intel SGX's aim to be resilient to kernel-level full privileged adversaries, the current implementations of the SGX processors are still vulnerable to unprivileged, user-space level adversaries.
- Foreshadow exploits a micro architectural implementation bug but does not undermine the architectural design of SGX.
- Hyper-threading is a side channel by design!

## Strengths

- Discovering and effectively mounting an attack on the remote attestation service that also affects multiple other entities. For example, using Foreshadow, they extracted the attestation keys that are used by the Quoting Enclave to approve the authenticity of the enclaves. By design, the attacker can masquerade to a third-party that they are a genuine enclave and conduct information exchange, but in reality, the attacker's code is run elsewhere, completely outside of SGX's control. This breaks the system of trust entirely as any body could obtain quote that prove authenticity.
- The next generation of Foreshadow attacks also break VM isolation, allowing malicious VMs running on shared cloud can access other VMs data.

## Weaknesses

- Current attack framework is limited if there is an increased cache pressure on the first/last cache lines. Which they claim can still be overcome by improved Foreshadow attacks.
- Although the attack outlines a way to forge attestations in the anonymous mode, the recommended pseudonymous mode would allow the third party viewing the attestation to

spot the fact that these attestations come from a different platform. This is not necessarily a weakness of the paper, but a simple way of avoiding the attack, if the third party wishes to.

## Summary of Key Results

- Foreshadow is a novel exploitation of an implementation bug in the kernel's microarchitecture that even works for a user-space unprivileged attacker.
- By a way of addressing privacy concerns, Intel QE implements a EPID group signature scheme. This further amplifies the reach of the attack because in an anonymous mode, the attacker can obtain a single EPID private key from the compromised machine and can forge signatures for the entire group containing millions of other SGX capable CPUs.

## Open Questions

- Since the most common configuration is to have hyper threading enabled, is there a way for Intel to somehow create mitigations to such attacks while supporting it?
- Is hyper threading really a fundamental security vulnerability? Do its benefits really warrant having a fair amount research going into supporting it while protecting security?