Designing SGX Applications for Recoverability

Paul Crews

ptcrews@cs.stanford.edu

Stanford University, Google*

YArch 2022

*This work was performed in the context of a course at Stanford University. Current affiliation: Google LLC

Disclaimer: This work was performed in the personal capacity of the author (Paul Crews) and does not represent the views of Google or Alphabet.

Intel SGX provides strong security guarantees

…that are sometimes broken.

Enclave Security Property Compromised	Examples
Confidentiality	Page Fault Attacks[1,2], Plundervolt[3], Foreshadow[4], SGAxe[5]
Integrity	Plundervolt[3]
Attestation	Plundervolt[3], Foreshadow[4], SGAxe[5]

1. Shweta Shinde, Zheng Leong Chua, Viswesh Narayanan, and Prateek Saxena. 2016. Preventing page faults from telling your secrets. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. 317–328.
2. Jo Van Bulck, Nico Weichbrodt, Rüdiger Kapitza, Frank Piessens, and Raoul Strackx. 2017. Telling your secrets without page faults: Stealthy page table-based attacks on enclaved execution. In 26th {USENIX} Security Symposium ({USENIX} Security 17). 1041–1056.
3. Kit Murdock, David Oswald, Flavio D Garcia, Jo Van Bulck, Daniel Gruss, and Frank Piessens. 2020. Plundervolt: Software-based fault injection attacks against Intel SGX. In 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 1466–1482.
4. Jo Van Bulck, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. 2018. Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution. In 27th USENIX Security Symposium (USENIX Security 18). USENIX Association, Baltimore, MD, 991–1008. https://www.usenix.org/conference/usenixsecurity18/presentation/bulck
5. Stephan van Schaik, Andrew Kwong, Daniel Genkin, and Yuval Yarom. 2020. SGAxe: How SGX fails in practice.

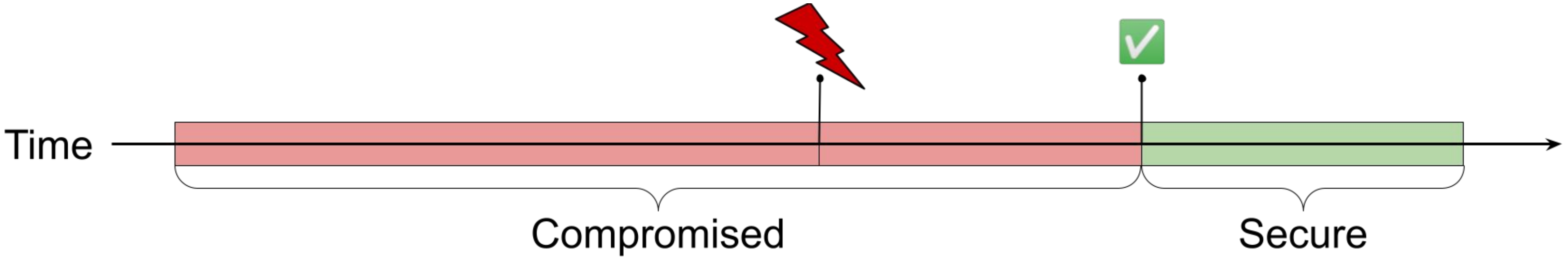
Motivation

What security guarantees can a vulnerable enclave provide?

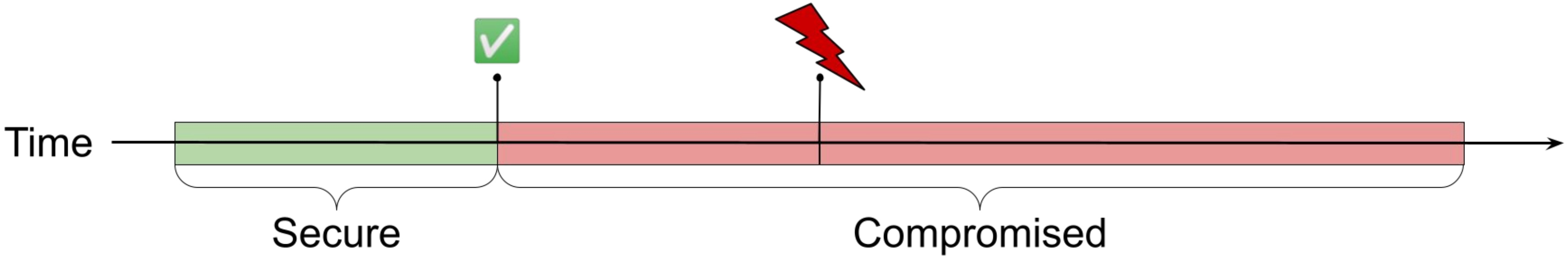
What applications are suitable for such an enclave?

Recoverability and Bounded Lookback

Idea: Design SGX applications to handle compromises by bounding the attacker

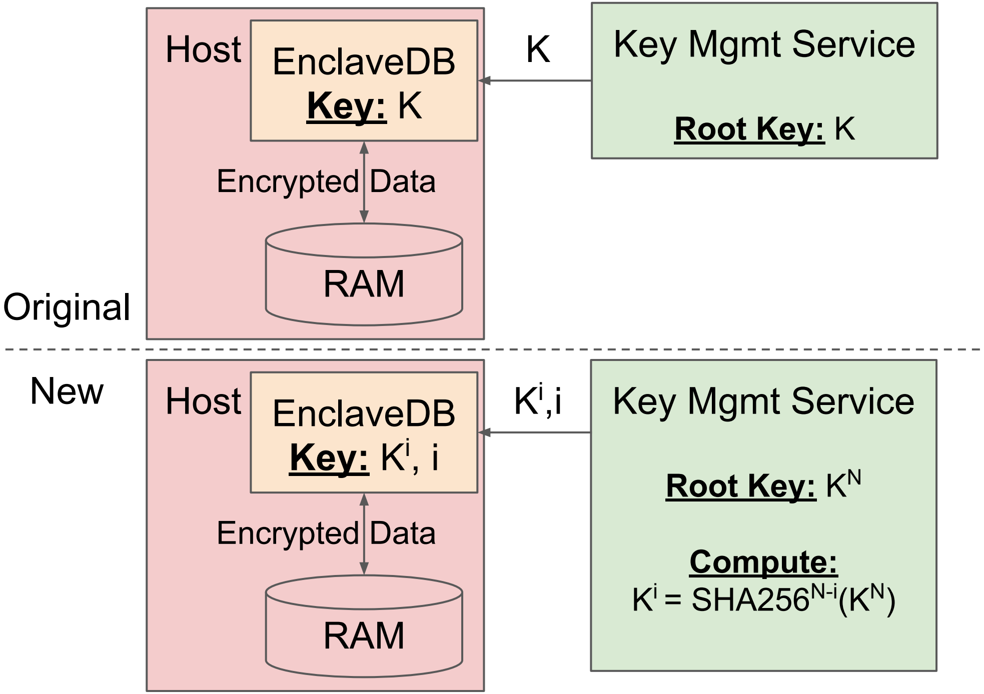


(a): Recoverability



(b): Bounded Lookback

Analysis and Implementation: EnclaveDB[1]



Original

Host

EnclaveDB

Key: K

Encrypted Data

RAM

K

Key Mgmt Service

Root Key: K

New

Host

EnclaveDB

Key: K^i, i

Encrypted Data

RAM

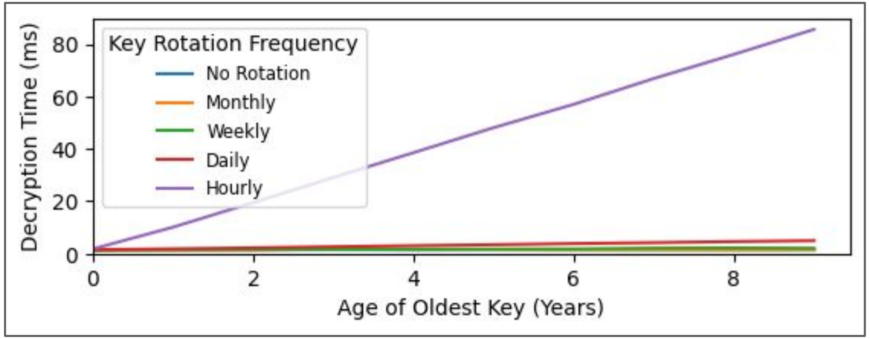
K^i,i

Key Mgmt Service

Root Key: K^N

Compute:

$K^i = SHA256^{N-i}(K^N)$



EnclaveDB decryption overhead

[1] Christian Priebe, Kapil Vaswani, and Manuel Costa. 2018. EnclaveDB: A Secure Database Using SGX. In 2018 IEEE Symposium on Security and Privacy (SP). 264–278. https://doi.org/10.1109/SP.2018.00025

Conclusion

- Identified issues with existing enclave assumptions
- Proposed new threat model, definitions for vulnerable enclaves
- Analysed EnclaveDB and prototyped recoverability

Future Work

- Implement a recoverability library for SGX
- Examine how application design influences recoverability, bounded lookback
- Generalize to other trusted hardware (AMD SEV-SNP, Intel TDX, TPMs)