SGX.Fail: How Stuff Gets eXtracted

Christina Garman

clg@cs.purdue.edu

Daniel Genkin

genkin@gatech.edu

PURDUE UNIVERSITY

Georgia Tech College of Computing
School of Cybersecurity and Privacy

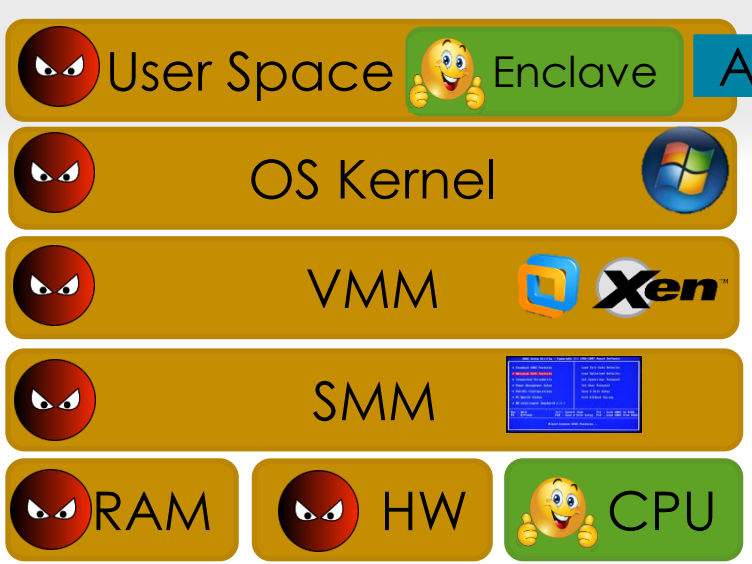
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

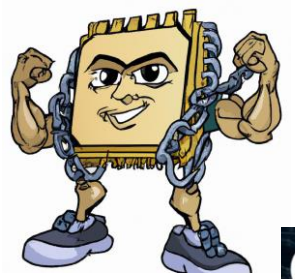
THE UNIVERSITY of ADELAIDE

Trusted Execution Environments

- Set of hardware features aimed to enforce data access control and isolation
- Confidentiality and Integrity are guaranteed by the HW
  - Even if everything but the CPU is corrupted
- Near native performance with strong security
- Many instantiations of this idea
- Today's focus: Intel SGX
  - Present on most x86 machines (since 2016)
  - Now moving from clients to servers
- Has attestation mechanisms for proving genuineness to remote clients
- Attestation is crucial for clients to trust the TEE platform



Remote Client

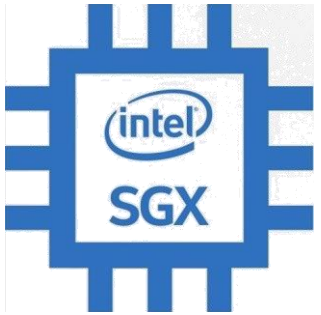


arm TRUSTZONE

arm CCA

AWS Nitro Enclave

AMD SEV-SNP

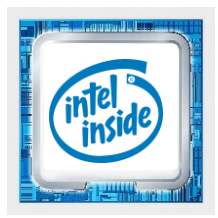


A Closer Look at Attestation Flow

3

A Closer Look at Attestation Flow

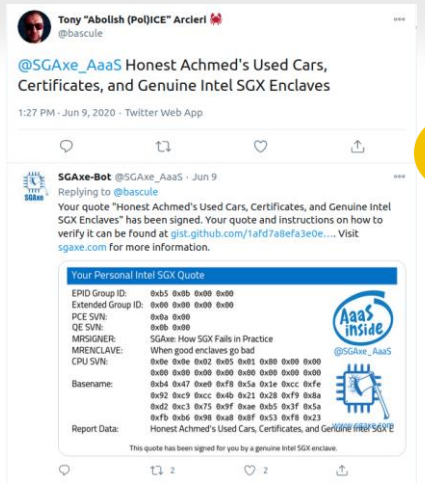
Attestation Key



CPU

on boot

BIOS

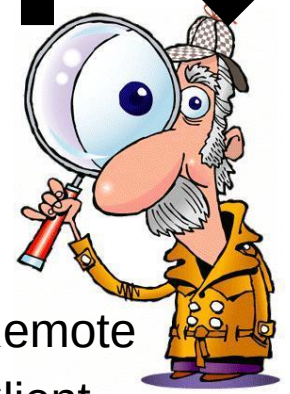


Quote

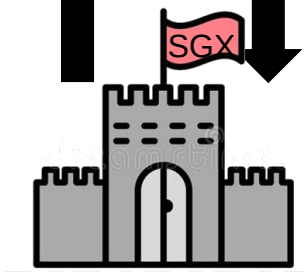
Intel Attestation Service (IAS)

Microcode Update

Group_ Out_of_ Date



Remote Client

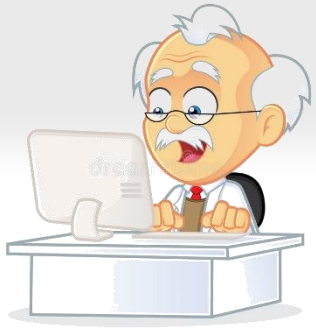


User Enclave

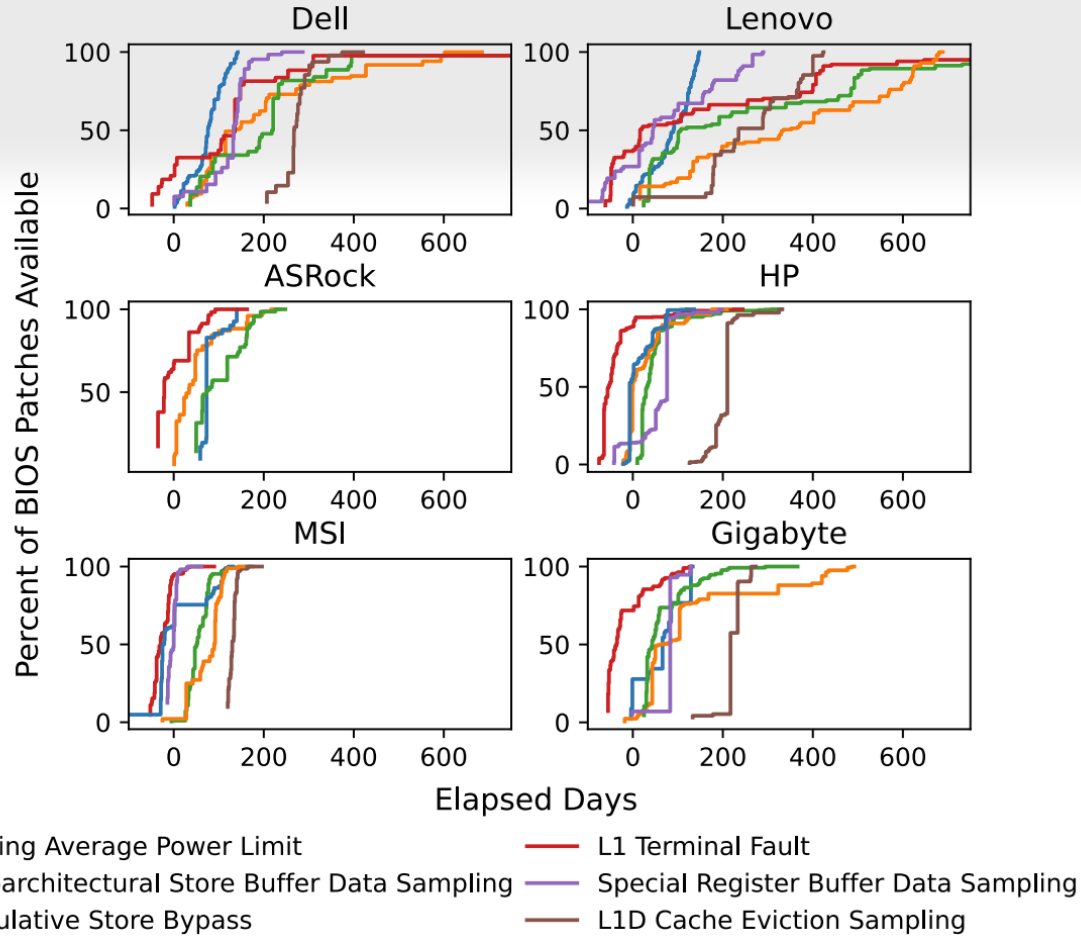
The BIOS is critical for post compromise recovery

4

Downsides of BIOS Updates



- Complicated manual process, requires experienced users
- BIOS vendors are slow
  - Afraid to brick systems (bye BIOS)
- We studied BIOS release times after major SGX vulnerabilities were made public
  - BIOS releases are between 37 and 329 days
  - …and now go install updates and reboot your infrastructure
- Vendor dilemma:
  - Allow unpatched machines and risk your secrets being exposed
  - Or make your users update their BIOS and hope nothing happens in the meanwhile
- Both approaches have issues



PowerDVD

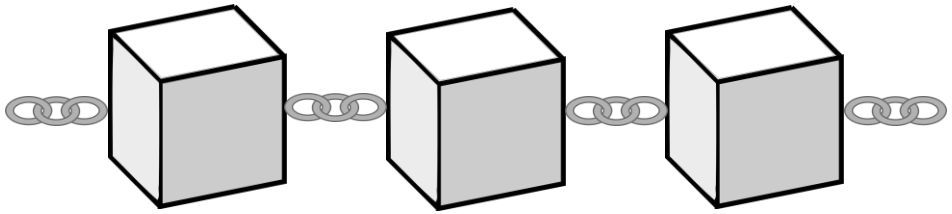
Or what can go wrong if you don't enforce SGX updates

- 4K UHD Blu-rays require disc encryption (and a secure execution environment on PCs)
- PowerDVD is the only software licensed for playing UHD Blu-rays on computers
  - Uses SGX for DRM via AACS2
  - Enclave is provisioned with keys that allow it to decrypt discs
- User base is large and potentially non-technical, which makes BIOS updates challenging
- PowerDVD trusts unpatched machines with GROUP_OUT_OF_DATE attestation status!
- Dumped PowerDVD enclave
- Reversed engineered the AACS 2.0 protocol
- Could extract disk decryption keys
- Potentially could watch movies on AMD and M1 machines
- Cannot enforce BIOS updates due to non-technical user base

FORESHADOW

Secret Network

- First production instance of Trusted Execution Environment (TEE)-based private smart contracts
- Launched in 2020, current market cap of over 100M USD
- Works by storing (the same) private key in every validator's enclave (derived from the consensus seed)
  - Transactions, contract state, on-chain data, etc. all encrypted to this key



Validator Enclave

- xAPIC disclosed in August 2022, with a public assertion that patching would not be enforced until March-April, 2023…

Unsealing Secret(s)

Theoretical Attacks

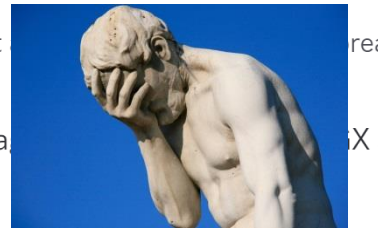
Evaluating potential attack vectors is integral to the formation of a protocol that is designed to be the fundamental privacy layer for all blockchain protocols. It is important to note that the majority of theoretical attacks that occur on TEEs (SGX in particular) happen within research labs.

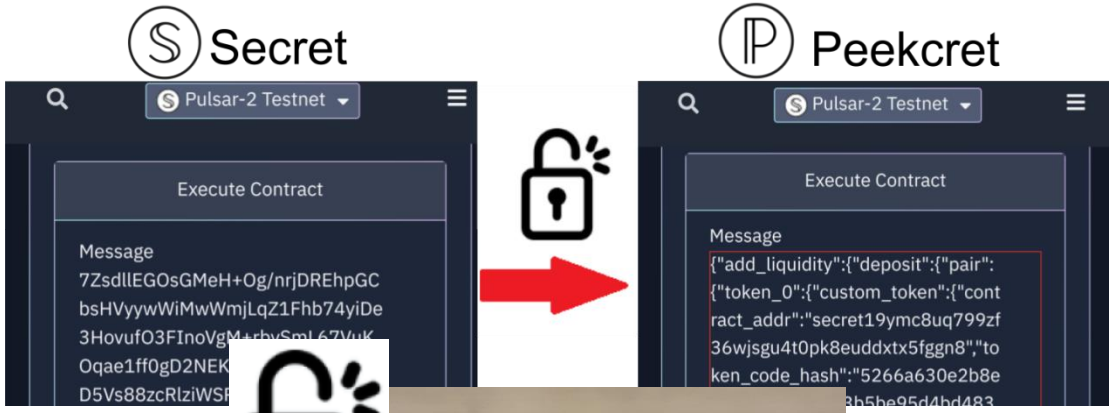
- Documentation says validator nodes must use SGX with SPS (e.g., servers), leading the community to believe that xAPIC did not affect it
  - (BUT this assertion was made in error, also allowing for validator nodes using easy-to-find machines)
  - Xeon CPUs share the same architectures as client CPUs, making them vulnerable to the same side channels
- We registered a computer onto the network as a validator node
- ANY node that registers as a validator is provisioned (so attack costs 1 SCRT, < 1 USD)
- Now we can extract the consensus seed!
- Keys derived from the consensus seed allow us to decrypt ANY transaction or contract state

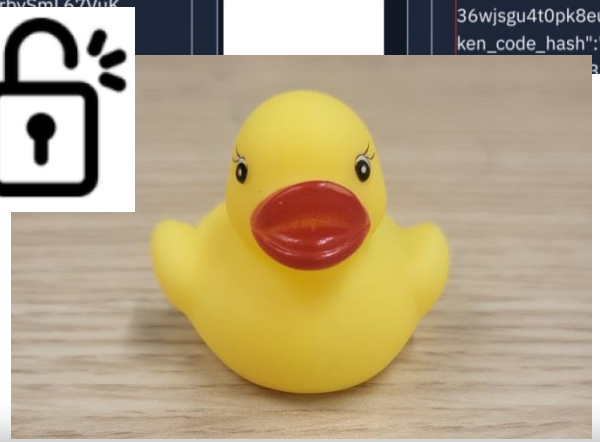
Hi, is secret … reakage? https://aepicleak.com/

Hey, not at all, these breaka… X SPS Server series

👍 1

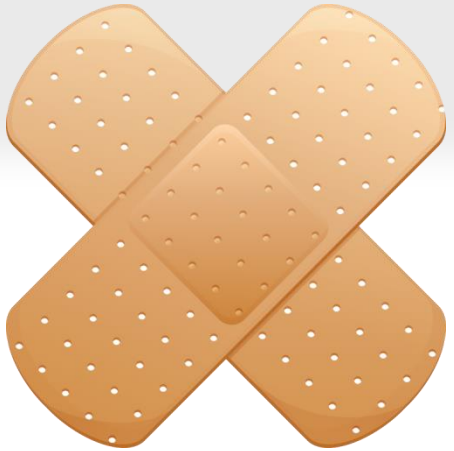




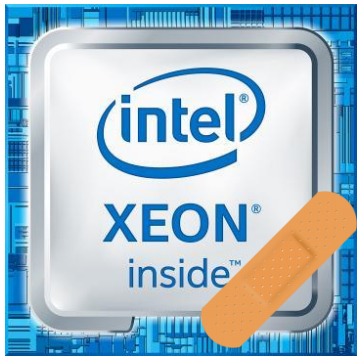


Mitigations?

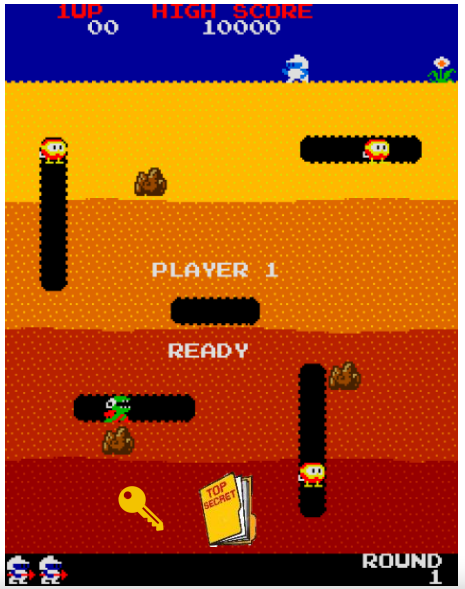
- Immediate: A “Registration Freeze” which revoked the developer SPID key with IAS, blocking all new node registration.



- Short-term: An allow-list was implemented so that only non-vulnerable processor types can again join. After TCB Recovery, only server hardware can join (as long as their microcode has been patched).

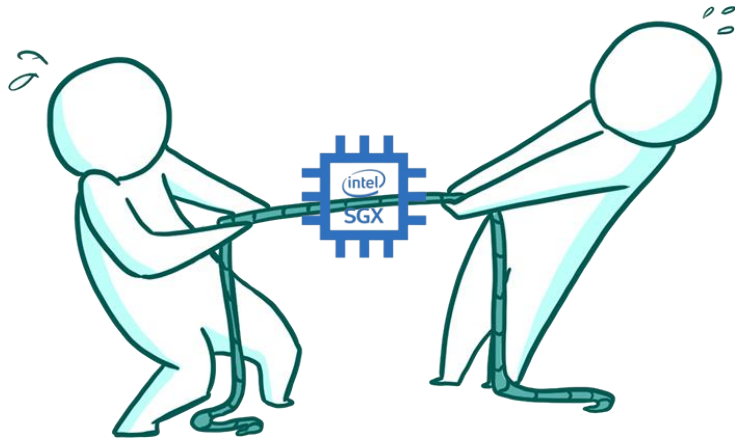


- Long-term: Develop a strategy for rolling the consensus seed. Move towards a more defense-in-depth system.



Lessons Learned

- There is constant tension between different SGX deployments
- Some need fast rollout of patches, TCB recovery, and attestation reports
- Some need significant time to rollout updates
- Single IAS lumps everyone in the same boat



Intel® S
SGX) T
Recove
Legacy

An Intel® Softwa
xAPIC (Intel-SA-
doing the follow

- Deferring t
attestation

Key Attestation Dates

- November 15, 2022 (Production Enforcement Phase 1): The Intel Attestation Production Environment (LIV) will enforce the presence of microcode and software updates on phase 1 platforms via Intel EPID attestation.

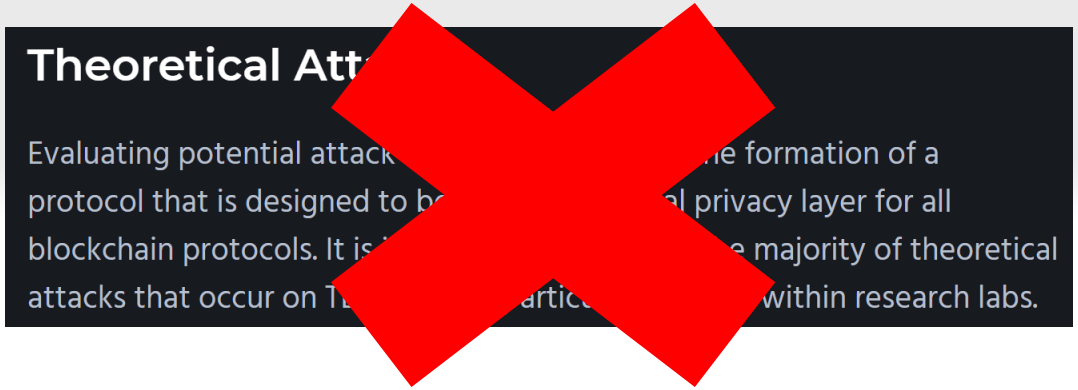
Intel SGX TCB Recovery Plans for Stale Data Read from Legacy xAPIC

An Intel SGX TCB recovery is planned for the enclave read scenario in Stale Data Read from Legacy xAPIC (Intel-SA-00657). Key dates are below:

- The Production Environment for Intel® SGX Attestation Service utilizing Intel® EPID (IAS-LIV) will enforce the presence of microcode and software updates on in-scope Intel® SGX platforms November 29, 2022.

Lessons Learned

- These attacks are not just theoretical!



- **Users:** learn about the impact on your data in the event that SGX is broken
- **Developers:** must plan ahead for the next TCB recovery (and assume SGX is going to break…)
- It is important to understand what information might leak via attacks
  - We've built a comprehensive categorization of publicly known hardware attacks, information leakages, and countermeasures
- Defense in-depth is still important. Side channels are an active research area.
- Future TEE designs need to include better mechanisms for fast and automatic updates.

Thank you!
Questions?

https://sgx.fail/

Stephan van Schaik, Alex Seto, Thomas Yurek, Adam Batori, Bader AlBassam, Christina Garman, Daniel Genkin, Andrew Miller, Eyal Ronen, Yuval Yarom

Frog put the cookies in SGX "There," he said. "Now we will not eat any more cookies."

"But we can use side channels x," said Toad.

"That is true," said Frog.