CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks

September 11th 2018
CHES, Amsterdam, The Netherlands

Fergus Dall, Gabrielle De Micheli, Thomas Eisenbarth, Daniel Genkin, Nadia Heninger, Ahmad Moghimi, and Yuval Yarom
Intel Software Guard Extensions

1. Set of instructions aiming to guarantee confidentiality and integrity of applications that run inside untrusted environments.
2. Protects enclaves of code and data.
Enclaves

- Enclaves are isolated from the software running on the computer.
- SGX controls the entry to and exit from enclaves.
Remote attestation: EPIID

Trust is based on the EPIID key!
Why need IAS? Revocation!
All quotes are encrypted by SGX.
Unlinkability

impossible to identify the platform that produced a signature on some message $m$. 
Unforgeability

impossible for an attacker to forge a valid signature on some previously-unsigned message, without knowing a non-revoked secret key.
Our results

• **First cache attacks** on Intel’s EPID protocol implemented inside SGX.

• Recover part of the enclave’s long term secret key.

• Malicious attestation server (Intel) can break the **unlinkability guarantees** of SGX’s remote attestation protocol.
EPID: setup

• An issuer:

• A revocation manager:

• A platform:

• A verifier:
EPID: algorithms

1\(^k\) $(gpk, isk)$

$(gpk, isk)$

$sk$

Client

Platform

Verifier

Setup

Join

Sign

Verify

issuer

platform

platform

platform

Client

Verifier

$m, sk$

$\sigma$

$\sigma$

Yes/No

$\sigma$

Verifier
The signing algorithm

• Secret key: $f + \text{Intel’s signature on } f$
• Randomly choose: $B \in G$ and compute
  \[ K := B^f \]
• How to sign?

Non-interactive zero knowledge proof of knowledge:

“\text{"I know an unrevoked } f \text{ such that } K := B^f\text{"}”

• Requires computing $A^r$, where $A$ is some value.
• Signature $\sigma$ has the values $K, B$ and $s \leftarrow r + Hf$
Attack idea

• Recover side-channel information about the length of the nonce $r$ from $A^r$.

• After many observations, use length data to mount a lattice attack to recover the value of $f$.

• Break unlinkability.
How unlinkability is broken?

• \( f \) is unique per platform and private.
• The attacker knowns a signature \( \sigma = (K, B, \ldots) \) on some message \( m \) and \( f \).
• He can check if \( K = B^f \).
• If yes, then the signature was issued by the platform whose key is \( f \).
CPU vs memory

Caches are used to bridge the gap.

- Divides memory into *lines*
- Stores recently used lines

- In a *cache hit*, data is retrieved from the cache
- In a *cache miss*, data is retrieved from memory and inserted to the cache
The Prime+Probe Attack

• Allocate a cache-sized memory buffer
  • **Prime:** fills the cache with the contents of the buffer
  • **Probe:** measure the time to access each cache set
    – Slow access indicates victim access to the set
In our attack

• The signing algorithm requires computing $A^r$.

• Exponentiation uses some variant of square and multiply with fixed windows of bits.

• Quoting enclave recodes the nonce $r$ to have fewer non-zero bits.
Scalar multiplication algorithm

\textbf{MultPoint}(point } P \text{, window size } w \text{, scalar } r): \\
\textbf{Initialize } P : P_0 \leftarrow O \\
\text{For } i \leftarrow 1 \text{ to } 2^{w-1} \text{ do:} \\
\quad P_i \leftarrow P \cdot P_{i-1} \\
\quad i \leftarrow \max(j : r_j \neq 0) \\
\text{s } \leftarrow P_{r_i} \\
\text{i } \leftarrow i - 1 \\
\text{While } i \geq 0 \text{ do:} \\
\quad s \leftarrow r^{2w} \\
\quad s \leftarrow s \cdot P_{r_i} \\
\quad i \leftarrow i - 1 \\
\text{End while} \\
\text{Output: } s \\

• Scalar of length 256 bits \rightarrow \text{recoded scalar of length 52} \rightarrow 51 \text{ loop iterations.} \\
• Bits 256 and 255 are 0 \rightarrow \text{recoded scalar of length 51} \rightarrow 50 \text{ loop iterations.}
Counting loops

- Monitor cache access patterns during the computation of the main loop.

- One **period** corresponds to one **loop iteration**.
- Number of periods gives us information on the **number of iterations**.
A lattice attack

Side channel information about the length of $r$.

**Goal:** Solve for $f$.

- Many samples $\{(s, H)\}_i$ such that:
  \[
  s \equiv r + Hf \mod p
  \]
- Information about the number $l_i$ of most significant zero bits in $r_i$.
- We learn $|s_i - H_i f| = |r_i| < \frac{p}{2^{l_i}}$

hidden number problem and obtain $f$. 
Recovering $f$

10 600 signatures required if only using 49-loop samples to get 37 error-free samples.

- Use samples of different loop lengths
- Reduce the number of signatures with manual inspection: less than 7 500 observed signatures to obtain enough 49-loop observations for a full key recovery.
Conclusion

• We finally have $f$.

• **Limitations**: we can’t run the attack ourselves as all the EPID signatures are encrypted with Intel’s public key!

• A malicious Intel could break the unlinkability guarantee.

• Thank you!
Thank you!

CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks

Fergus Dall, Gabrielle De Micheli, Thomas Eisenbarth, Daniel Genkin, Nadia Heninger, Ahmad Moghimi, and Yuval Yarom
In our experiments, **8000 signatures** necessary to enough error-free samples for key recovery.
Recoding the nonces

• Non-adjacent form (NAF) encoding:
  a. no two sequential non-zero digits.
  b. signed digits

• Example:
  a. binary: \((0,1,1,1) = 2^2 + 2^1 + 2^0 = 7\)
  b. 2-NAF: \((1,0,0,-1) = 2^3 - 2^0 = 7\)

• Generalization to \(w\)-NAF: work in base \(2^w\).
• The quoting enclave *recodes* the scalar \(r_f\) using some variant of \(w\)-NAF.

\[
r_f = (r_1, \cdots r_n) \text{ s.t.:}
\]
1. \(r_f = \sum_i 2^w \cdot i \cdot r_i\)
2. \(-2^w - 1 \leq r_i \leq 2^w - 1\).

• Example: \((0, 0, 1, -25) = 2^{5\cdot1} \cdot 1 + 2^{5\cdot0} \cdot (-25) = 7\)