Practical implications of Intel SGX with Graphene

July 4th, 2019

Derk Barten
Robin Klusman
Software Guard Extensions (SGX)

- Untrusted system
- Trusted enclave
- Attestation
- Encrypted & isolated memory
- Integrity, confidentiality, isolation
Graphene-SGX

- Library OS
- Standard C library
- Unmodified applications
- Multi-process support
- Dynamic shared libraries
- Manifest

Diagram:
- Enclave
  - User application
  - Library OS
Related work
Use-cases

- **SGX**
  - DRM, Anti-cheat
  - Compilers
  - TLS termination
  - Databases
  - System logs
  - Middleboxes

- **Graphene**
  - No modifications required
  - Reduced development effort
  - Facilitate SGX research
Related work
Existing attacks on SGX

- Cache side channel attacks
  - Foreshadow
  - SgxPectre
  - BranchScope
  - CacheZoom
- Asyncshock
- Controlled channel
What are the practical implications of running arbitrary applications in Intel SGX using Graphene-SGX?
Security implications
Misaligned threat model

- Intel SGX
  - Operating system = untrusted

- Most applications
  - Operating system = trusted
Arbitrary applications are often not designed to guard against a malicious operating system.
Iago attacks

- Attacks by malicious kernel
- System calls
- Mitigation
  - Verification
Date / time manipulation

- `gettimeofday()`
- Reliant on OS supplied vDSO
- Not verified by Graphene

**Implications**
- Transaction order
- Kerberos
- 2FA token validity
- Rate limiting
ACCESS DENIED
Please wait 54 seconds.

Date / time manipulation demo
Environment variable manipulation

- Arbitrary environment vars
- Not present in manifest
- Not checked by Graphene
- Easily overlooked

- Implications
  - Influence execution
  - GCC Epoch
Framework maturity
Running applications in Graphene

- OS version support
- Framework bugs
- Disk writes
- Non trivial to port complex applications
Discussion & conclusions
Discussion

- Security may be compromised
- Can be mitigated
- Graphene as research project
- Not ready for production
Developers should take care when running arbitrary applications in SGX using Graphene, as there may be non-trivial security implications and framework bugs.
Future work

- Explore additional system calls
- Environment variable dependent applications
- Investigate SCONE/Panoply
Sources

Software Attestation

- Attestation data
- Attestation key
- Attestation signature
Software Attestation

SGX

- MRENCLAVE - Enclave Identity
- MRSIGNER - Sealing Authority
- Public key hash
- Attestation Key in μcode

Source: Intel documentation