Mitigating interrupt-driven attacks against enclaved execution

Frank Piessens*[1]

[1]KULeuven – Belgique

Résumé

Enclaved execution is a security mechanism that supports the run time creation of enclaves that shield software components from all other software on the platform, even from privileged system software.
Hardware-support for enclaved execution is available in academic processor prototypes, and in commercial processors with Intel's Software Guard Extensions (Intel SGX).

Implementations exist both for small IoT-level microprocessors as well as for high-end processors that power the cloud.

Enclaved execution is a powerful security primitive, that is used to support confidential computing, and that has been proposed as a key mechanism to support end-to-end security for distributed applications.

However, the research community has also developed a wide range of novel attack techniques that build on the powerful attacker model that enclaves must resist.

Controlled channel attacks are such a class of powerful side channel attacks that use privileged system software capabilities to extract information from enclaves.

In this talk, we focus on a specific class of controlled channel attacks, more specifically those that rely on the use of interrupts.

We provide an overview of the attack techniques that have been developed, both for low-end and for high-end enclaves.

Next, we discuss appropriate mitigation techniques.

For enclaves on small microprocessors, hardware and compiler-based mitigations can provide strong protection.
For Intel SGX enclaves, Intel has recently announced an architectural extension that makes enclaves interrupt-aware, and this extension can be the basis for strong software countermeasures against interrupt-driven attacks.

*Intervenant