Cryptographic Hardware from Untrusted Components

Vasilios Mavroudis
v.mavroudis@cs.ucl.ac.uk
University College London

Cryptographic devices used in critical applications assume that all hardware components always operate according to their specifications. However, this is not always true as components may contain intentional or unintentional errors (e.g., bugs, hardware trojans, backdoors). We designed and built the first hardware security module that maintains its security properties in the presence of multiple malicious and faulty components.

Motivation

The semiconductor industry is fully globalized, and integrated circuits (ICs) are commonly defined, designed and fabricated in different premises across the world. This reduces production costs, but also exposes ICs to supply chain attacks, where insiders introduce malicious circuitry into the final products. As a result, the security of critical systems that rely on such ICs for cryptographic operations is jeopardized. Existing detection and prevention techniques are brittle, as new threats are able to circumvent them quickly or come with unrealistically high manufacturing costs and complexity. At the same time, post-fabrication testing techniques fail to detect even unintentional manufacturing errors resulting in faulty components making it to the market.

A Real Example

The newly discovered ROCA vulnerability highlights the fact that no matter how rigorous the testing and examination of the hardware ICs is, it will never provide 100% guarantee of their security. The attack affected cryptographic smartcards, security tokens and other secure hardware chips manufactured by Infineon Technologies AG from as early as 2012. From a technical perspective, it resulted in weak RSA key pairs (both 1024 and 2048 bits-long) that allowed an attacker to compute their private part. Major vendors including Microsoft, Google, HP, Lenovo, Fujitsu already released software updates and mitigation guidelines.

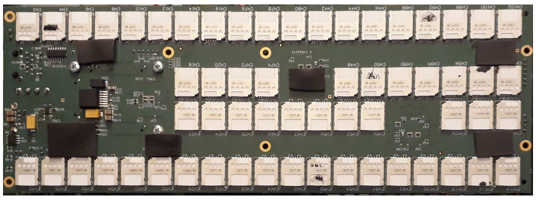
Our Solution

This work follows a new mitigation approach and introduces a novel high-level architecture (named *Myst*) that enables cryptographic devices to maintain their security properties in the presence of malicious hardware components. Unlike prior mitigation efforts that attempted to detect or prevent all possible errors, our work is based on the premise that no component comes with 100% correctness guarantee. Instead, Myst combines established privacy enhancing technologies (PETs), with mature fault-tolerant system architectures to distribute trust between multiple components originating from non-crossing supply chains. This reduce the likelihood of compromises as it ensures that unless an adversary manages to breach *all* these supply chains, the device remains secure.

Our architecture is directly applicable to many critical systems with high-security needs that use secure crypto-processors to carry out sensitive tasks (e.g., key generation and storage, digital signing) or to maintain a protective layer against cyber-attacks and security breaches. For instance, banking infrastructure, military equipment and even space stations utilize crypto-processors embedded into Hardware Security Modules, Cryptographic Accelerators and Trusted Platform Modules.

HSM Prototype

To evaluate the practicality of our architecture, we built a hardware security module (HSM) capable of generating keys, decrypting ciphertexts, and issuing digital signatures.



Side A of our hardware security module prototype, featuring 120 crypto-processors.

Our prototype features 120 highly tamper-resistant ICs, and comes with a very good throughput/cost ratio. Namely, for 120 smartcards the maximum throughput was 315ops/sec for ciphertext Decryption and 77ops/sec for Signing. Our experiments, show that performance increases linearly to the number of ICs, thus making the architecture highly-scalable. Most importantly, this is the first work proving in practice that error and trojan-resilient hardware is feasible at a negligible performance cost.

Consortium

The architecture and the prototype were developed by researchers from the Information Security Group, University College London, the CRoCS laboratory, Masaryk University and Enigma Bridge. The academic paper will be presented at the ACM Conference on Computer and Communications Security (ACM CCS '17). The research and development is supported by the European Commission through the H2020 DS-2014-653497 PANORAMIX project and the European Research Council via the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 307937, and the Czech Science Foundation under project GA16-08565S.

For more information please visit:
BackdoorTolerance.org