Abstract

Alberto Carelli
PhD Program in Computer and Control Engineering
XXXII Cycle

April 2020

The growing threat of advanced cyber-attacks is a major cause of concerns for Information-Technology (IT) systems. Cybersecurity implies guaranteeing the security of the cyberspace from threats, which might present in different forms. Among the different classes of system that employ IT systems, there are the Critical Infrastructures. Critical infrastructures describe all physical and cyber systems, assets and other elements on which the society of a nation relies upon to maintain national security, economic vitality, and public health and safety. Examples of critical infrastructures for a nation can be power plants and energy supply networks, water supply systems, healthcare and hospital structures, transportation infrastructures, etc.

Originally Critical Infrastructures were designed as isolated systems not connected to the internet. They were based on old legacy systems, lacking the security protocols that are now built in. In recent years there has been a proliferation of new digital technologies that are designed to provides beneficial features to the systems where they are embedded. However, also the integration of such technologies makes the systems more vulnerable from a cybersecurity point of view by expanding the attack surface. The lack or inadequacy of appropriate security mechanisms leads to malicious attacks. If successful, attacks to these classes of systems, may lead to physical disruption or business operations and intellectual property theft. This may result in extensive economic losses and expose health or social well-being of people to safety and security risks.

This thesis focuses on the study of protection mechanisms for Critical Infrastructures from new cyberattacks. Different classes of attacks are considered.

Microarchitectural side-channel attacks exploit the microarchitecture of a microprocessor for unintended leakage of sensitive information. Targeting the computational cores, which are at the base of the majority of cyber assets, makes Critical Infrastructures and industrial control systems potentially vulnerable. Particular attention must be paid to the implementation of countermeasures against this type of attacks, because they might interfere with other crucial aspects of the system, such as safety.

Critical Infrastructures employ new technologies, such as reconfigurable platforms to exploit additional flexibility and acceleration capabilities. Also FPGA-based systems are vulnerable to attacks targeting the design to be deployed

in-the-field. These attacks might target the confidentiality of the design or the injection of unintended features allowing the system to be controlled by malicious attackers or discover and exfiltrate sensitive information, such as intellectual property data. Although existing security measures already mitigate the attacks, they do not deal with a complex scenario where multiple different designers are involved.

Finally, a broader protection mechanism is provided through a hardware security module featuring secure key management and cryptographic functionalities. The robustness of the device is assessed through a physical and non-invasive side-channel attack aiming at the recovery of the stored encryption keys.