leti
cea tech

CYBER SECURITY

Hardware security
and security by hardware

Leti, technology
research institute

Contact:
leti.contact@cea.fr

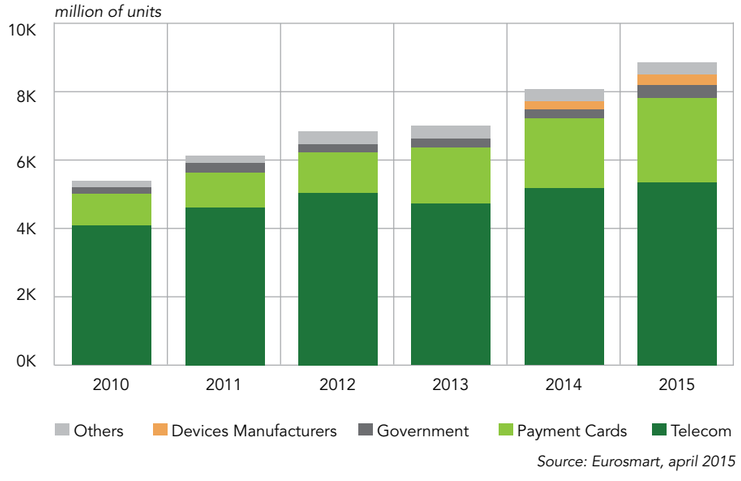
Tomorrow's challenges: **Security in a smarter & connected world**

Every day, everywhere, digital technology is part of our lives, our neighborhoods and our objects, generating new ways of living, working, interacting.
At the same time, we frequently hear about examples of **successful attacks** on the Internet of Things (sometimes called Internet of Threats), smart cars, smart homes, smart energy, e-health, payment, e-identity, etc. Technology's expansion has opened multiple opportunities for **hacking**, **identity-theft** and other **new digital intrusions** in our lives.

Security—and privacy—are critical in the digital world. Yet, security professionals are challenged to protect company and customer data as it proliferates across more devices, gets parked in more places and is accessed by more applications than ever before.

SECURE ELEMENTS SHIPMENTS FROM 2010 TO 2015

By year, the portion of contactless secure elements by sector among the total number of secure elements actually shipped or forecasted.



Source: Eurosmart, april 2015

SMART CITIES

The concept of a smart city is very topical, and many organizations around the world are working on intelligent solutions to make urban areas energy efficient, comfortable, environmentally friendly and safe. Cyber security in these smart cities must be part of the equation from the start.

ID, AUTHENTICATION

The increases in international travel, growing threats from terrorism and high levels of identity fraud mean that our travel documents, ID and healthcare documents must be very secure.
The world of financial services is changing fast and consumers expect increasingly personalized, convenient, yet secure options to pay, communicate and interact with their banks. With sensitive data residing everywhere, organizations becoming more mobile, and the breach epidemic growing, the need for advanced identity—and data—protection solutions has become even more critical.

CONNECTED CAR

Today's connected cars have a highly sensitive electronic environment, containing critical systems. Until recently security measures to safeguard this environment have been limited, partly because the systems were relatively isolated from the rest of the world. With increasing connectivity in the car, a Secure Network Platform is needed, giving manufacturers and drivers complete peace of mind.

IoT

The Internet of Things (IoT) is advancing rapidly. As it becomes more prevalent, the amount of data and connected devices that businesses have access to increases exponentially. While this has tremendous benefits for enterprises of all sizes, data and devices must also be protected, which poses a number of challenges.

LETI: OPTIMIZED SECURITY SOLUTIONS

LETI IS A RECOGNIZED GLOBAL LEADER
DEDICATED TO HIGH-PERFORMANCE, SECURE AND ENERGY EFFICIENT MINIATURIZATION TECHNOLOGIES

Leti's goal is to achieve **optimized security solutions to meet customer needs**, such as security level, power consumption, size/volume, cost... Research focuses on design, implementation and verification of secure and correct systems.

SECURITY AT DIFFERENT LEVELS

WIRELESS COMMUNICATION
Communication layers are potential open doors for the attackers: man in the middle, relay, eavesdropping have demonstrated their efficiency in various areas (automotive, smartcards, etc).

INTEGRATED CIRCUIT
Secured integrated circuits become the heart of secure systems with the implementation of secure storage and cryptographic primitives. Ensuring a high level of resistance over a relatively long time (5–10 years) is still a challenge as physical attacks evolves quickly (invasive attacks, side channel, fault injection). Thanks to its capabilities in advanced technologies and IC design, Leti offers original and efficient solutions.

SYSTEM
Security is complex. A single error in software can be an open door for a breach. Cryptography relies on the security of secrets (the key) and has to be used carefully to be error free. The Internet offers an entry door to most of the connected systems and a way for attackers to quickly exchange and distribute information about weaknesses of potential targets. Security by design, validated cryptographic protocols and end-to-end security are key elements of a secure system.

SECURE DEVICES
The security-by-design paradigm must be applied to all components of a system: electronics, embedded software architectures and implementation. Leti offers all its capabilities to help designers secure their components.

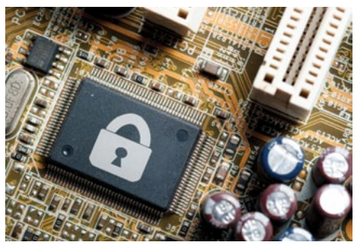
MAIN RESEARCH

Leti focuses on micro- and nanotechnologies, architectures, tools and design methodologies that secure computing systems efficiently and reliably. It has unique know-how and unique access to technologies (shielding, sensors, architectures, embedded software) to design ASICs and SOCs for security applications implementing the best trade off between security (resistance to attacks) and applications constraints (power, cost, performance).

CRYPTOGRAPHY
Securing the Internet of Things with tens of billions of connected objects and their associated low-power requirements is a real challenge. Classic cryptographic schemes have shown their limits both for symmetric protocols (problems with the keys management) and for asymmetric protocols (too heavy in multiple applications). Current research topics include: lightweight, identity based, quantum safe, cryptography intrinsically resistant to side channel…

SECURED COMMUNICATIONS
Security of communication is not only encryption. Multiple wireless interfaces and secure updates "over the air" are often open doors for attackers. In addition, attacks on the communication link (man in the middle, relay, denial of service) are critical. Current research topics include: specific mechanisms to protect the data during communication, physical-layer protection, secured protocols.

SECURITY ARCHITECTURES
Security has to be the heart of a system and successful attacks on any of its components must be taken into account in the design. Specific architectures have to be developed. These include using redundant protections, secured kernel (Root of Trust), integrity checking associated with security functions such as bootstrap (setting up an object, introducing it in a network), updates (uploading firmware or application software, updating a physical component) and recovery (capability to move back to a secure state after a successful attack). Current research topics include the development of such architectures for various applications such as industrial systems, cyber physical systems, automotive, etc.



EFFICIENT & SECURED IMPLEMENTATION
Using the best cryptography is not enough if the attacker has physical access to the circuit. Physical, side channel, fault injection attacks have to be countered by specific implementation. In addition, emerging markets such as the Internet Of Things, medical devices and home applications require a cost-and-power optimization. Current research topics include ultra low-power secure design, security by design, zero power protection…

LETI: SECURITY EVALUATION/ CERTIFICATION

LETI OFFERS A BROAD RANGE OF SERVICES,
TO PERFORM INDEPENDENT ANALYSIS, EVALUATIONS AND TESTING ON VARIOUS PRODUCTS OR SYSTEMS.

TEST & EVALUATION

- Searching for a risk analysis to identify the risks of an application?
- Searching for a vulnerability analysis to evaluate the resistance of the system architecture?
- Searching for competencies and test capabilities to evaluate either the resistance of components to physical attacks or the efficiency of a countermeasure?

Leti's challenges your product to discover your security weaknesses.

FUZZING PLATFORM
Testing devices interfaces

FAULT INJECTION
Glitches, light, laser, EM fault injection

SIDE CHANNEL PLATFORM
Timing, power, electromagnetic signal analysis

PHYSICAL ATTACKS PLATFORM
Access to internal data (probing)

NANO-CHARACTERIZATION PLATFORM
Silicon analysis and preparation

EVALUATION FOR CERTIFICATION

CESTI Leti is a security evaluation laboratory licensed by the French Certification Scheme and the major worldwide evaluation schemes (EMVCo, VISA, MASTERCARD, NXP-MIFARE). It is able to perform security evaluations targeting an official certification using up-to-date norms and standards (Common Criteria).

Specialized in the evaluation of top-level components (integrated circuits, smartcards, electronic devices, HSM), it masters all the evaluation components (site audits, design analysis, source-code audits, penetration testing), including the management of formal and semi-formal design (up to the Common Criteria EAL7 level).

CESTI Leti also develops new methodologies for specific areas, such as biometrics and automotive, with partners.

Common Criteria · EMVCo · MasterCard · VISA

ABOUT LETI

Leti is a technology research institute at CEA Tech and a recognized global leader in miniaturization technologies enabling smart, energy-efficient and secure solutions. Committed to innovation, its teams create differentiating solutions for Leti's industrial partners.

By pioneering new technologies, Leti enables innovative applicative solutions that ensure competitiveness in a wide range of markets. Leti tackles critical, current global issues such as the future of industry, clean and safe energies, health and wellness, safety & security…

Leti's multidisciplinary teams deliver solid micro and nano technologies expertise, leveraging world-class pre-industrialization facilities.

For 50 years, the institute has been building long-term relationships with its industrial partners providing tailor-made solutions and a clear intellectual property policy.

Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 rue des Martyrs | 38054 Grenoble Cedex 9 | France
www.leti.fr

INSTITUT CARNOT Leti