Cybersecurity is a major challenge for digital trust

The rise of the Internet of Things (IoT) has sparked an explosion of innovative services, powered by a variety of heterogeneous connected devices and sophisticated data management.

CHRISTOPHE VILLEMAZET, DIRECTOR OF THE NANOELEC/PULSE PROGRAM

© P. Jayet/CEA

Yet, this digital revolution comes with a dark side: a surge in cyberattacks that is forcing public and institutional bodies to confront the risks of unchecked digital transformation.

New hardware and software vulnerabilities are being exposed at an alarming rate, as medical devices, vehicles, industrial, and urban infrastructure become increasingly interconnected and autonomous. These vulnerabilities, and the exploits that target them, are eroding public trust in connected services and products. The repercussions are vast, affecting corporate reputations, societal stability, economic growth, and individual privacy. Inadequate protection can even jeopardize the legal and social accountability of both public and private entities.

Moreover, cybersecurity is often relegated to an afterthought in digital product design, seen as a constraint that should not impede primary functions, whether health, mobility, or manufacturing, nor compromise cost, performance or ergonomics.

The Nanoelec/Pulse program rises to this challenge, seeking to harness electronic technologies to address this new reality. Our mission is to pioneer technologies that enable the development of connected products and services, fortified with enhanced security, robust data protection, and simplified cybersecurity strategies. We are committed to safeguarding the confidentiality, authenticity, and integrity of digital data, and ensuring privacy protection. Our focus lies in three critical domains: fortifying the cybersecurity of industrial systems, safeguarding healthcare products, and securing autonomous robotic systems and vehicles.

•••

AGENDA

In 2024, the teams involved in the Nanoelec/Pulse program achieved significant milestones in both post-quantum cryptography and the securing of embedded AI. We now possess a secure, open-source microprocessor core platform (RISC-V). Our teams are developing advanced modeling and evaluation capabilities for digital components in building management, crane control systems, and the secure implementation of blockchain on embedded systems.

This progress underscores our commitment to pushing the boundaries of cybersecurity and ensuring that our technological advances are both innovative and secure. As we continue to explore these frontiers, we remain dedicated to creating solutions that protect data integrity, enhance system reliability, and fortify the digital infrastructure of the future. •

PULSE AT A GLANCE

→ **Vision**
Due to the rise in cybercrime, Internet of Things (IoT) cybersecurity is a major challenge for digital trust. Strengthening and hardening critical embedded, increasingly interconnected and smarter systems is now vital

→ **Ambition**
New smart and intrinsically secure nanocomponents to reinforce the resistance of systems to future cyberattacks + improved security of smart embedded systems throughout their lifecycle (including AI algorithms) + safer deployment environments through digital ID, data sovereignty and secure interactions between smart systems

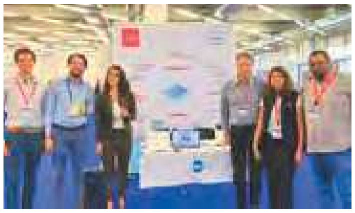
→ **Mission**
To develop and test new security features for components and systems in three fields of application: Industry 4.0, homecare and robotics

→ **Partners**
CEA, Grenoble INP-UGA, Inria, Schneider Electric, STMicroelectronics, UGA

AGENDA

Pulse at international events

The Nanoelec/Pulse program teams took part in the 2024 editions of the InCyber Forum (Lille, Oct. 31 – Nov. 4, 2024), European Cyber Week (Rennes, Nov. 18-21, 2024), RISC-V Summit Europe (Munich, June 24-28) and CSAW (Valence, Nov. 7 and 8) to present their work, notably concerning intrinsically secure application processors.



IRT Nanoelec 2025

Thomas Loubier, embedded systems cybersecurity research engineer in the Systems Department of CEA-Leti, testing the security of communication protocols at the physical and wireless interfaces, on CEA-Leti's SCIBE (Secure Communication Interface BEnch), developed with IRT Nanoelec.

© A.Havret/CEA 2024

IRT Nanoelec 2025

PhDs AT PULSE

Numerous students connected to the Nanoelec/Pulse program defended their theses in 2024.

Confidentiality of embedded machine learning models

The deployment of Deep Learning (DL) models on embedded platforms is becoming increasingly widespread.

These models are required to perform tasks and handle sometimes sensitive data, so they must be secure, notably for European regulatory projects. Raphaël Joud studied threats to the confidentiality of DL models through hardware attacks, more particularly side channel attacks. Based on these results, Raphaël then assessed various countermeasures aimed at reinforcing the confidentiality of embedded models[1].

Collision avoidance in robotics

Mobile robots and autonomous vehicles must navigate in complex, unstructured environments, such as urban spaces shared with humans.

Although simple and effective, object representations often fail to model these uncertain scenes. The approach adopted by Thomas Genevois[2] aims to facilitate the integration of dynamic occupancy grids for collision avoidance, thus improving the connectivity between perception and navigation. The solutions were tested on three different robots, including a robotic car, in real conditions.

Security of post-quantum cryptographic implementations

Side channel attacks are a threat to the security of post-quantum cryptography.

After identifying the vulnerabilities in these implementations, three attacks on the HQC scheme were analyzed. The countermeasures identified by Guillaume Goy[3] include masking and mixing of the data handled in order to protect sensitive operations. His work demonstrates the ineffectiveness of existing countermeasures and underlines the need to reinforce the security of post-quantum implementations.

AGENDA

Cameras to study the effects of overweight and obesity

Overweight and obesity are a major public health issue. Balance and walking problems are frequently observed in overweight or obese people, which can sometimes lead to falls. To measure the effects of overweight and obesity when dealing with an obstacle while walking, Matthias Chardon[4] analyzed a set of experimental data. This data included five space-time parameters for walking and three obstacle clearance parameters measured on each foot by means of a system of ten infrared cameras filming the gait and obstacle clearance of 43 young adults. Even if the initial results suggest that overweight has minimal impact on tripping when clearing an obstacle while walking, additional work should evaluate overweight individuals of different ages and with different health conditions.

[1] St Etienne University thesis, defended on January 18, 2024, prepared with the Centre Microélectronique de Provence - Site Georges Charpak (CMP-GC)

[2] Grenoble Alpes University thesis, defended on June 19, 2024, prepared with Inria

[3] Limoges University thesis, defended on June 24, 2024, prepared with the XLIM laboratory (UMR CNRS 7252)

[4] Grenoble-Alpes University thesis, defended on September 20, 2024, prepared with the Ageis laboratory

Insight into age-related changes in gait

Since walking has a crucial role in maintaining independence, changes in gait should be identified and prevented at an early stage.

Walking speed predicts many clinical outcomes in old age. However, a comprehensive assessment of how walking speed affects accelerometer-based quantitative and qualitative gait measurements in younger and older adults is lacking.

The objective of this thesis was to gain insight into the possible mechanisms underlying age-related changes in gait.

A better understanding of age-related changes in gait patterns is provided through digital monitoring of gait (walking speed, walking conditions) with accelerometers. Gait speed is considered as the most commonly and widely used measurement to assess the locomotor performance of older adults. Iris Hagoort[6] has contributed to clarify the different functional properties contributing to age-related changes.

One of the conclusions is that the relationship between walking speed and quantitative and qualitative gait measurements, as well as the effects of age on this relationship, depends on the type of gait measurement studied.

—

Safety-security convergence of industrial control systems

Nowadays, industrial control systems (ICS) incorporate information technologies and are interconnected with the outside world, such as the internet, thus exposing their infrastructures to cyberattacks.

Cyberattacks have become new threats for industrial system operators, more particularly for continuity of service, reliability and security. Mike Da Silva[5] presents a complete assessment of the cybersecurity threat to the security of industrial control systems. His method differs from the state of the art in its high level of automation and its ability to model complex ICSs.

—

Acceptance of digital technologies in rheumatology

Telemedicine can be used for remote consultation, diagnosis, treatment and monitoring of patients, thereby facilitating their access to healthcare.

By studying 12 automatic learning algorithms for predicting the willingness to use tele-medicine by patients suffering from rheumatic and musculo-skeletal disorders, Felix Mühlensiepen studied the social, economic and psychological determining factors influencing the acceptance and use of digital health technologies in rheumatology, both by the patients and by the health professionals. If the use of these technologies is generally well accepted by the patients and health professionals, there are nonetheless access barriers which could lead to a digital divide.

—

Simulating cyberattacks on industrial control systems

Reinforcing the cybersecurity culture in industry.

After a systematic review of all the anomaly detection methods based on the system calls described in the literature, the teams from CEA and Schneider Electric, within Nanoelec, set up a testing and attack platform representative of an industrial system. Its aim is to test security solutions and notably to generate datasets to train AI models to automatically detect intrusion. The test bench proposes the greatest diversity and attack coverage in the MITRE ATT&CK matrix on Programmable Logic Controller and industrial gateway type devices, by comparison with the other state-of-the-art test benches.

Restoration mechanisms were also implemented for each of the attacks in order to return the system to a normal operating state. The aim is to be able to execute all attacks and extract internal signals from the device without having to reprogram or restart the target after each attack. All these developments are scheduled to be released as open source in 2025.

The WonderPOT honeypot was expanded to make for easier deployment. The aim is to provide a solution capable of capturing IoT-oriented malware while remaining stealthy so as not to be detected as a decoy system.

—

[5] Grenoble-Alpes University thesis, defended on October 15, 2024, prepared with the LIG laboratory

[6] Grenoble-Alpes University and RIJKSUNIVERSITEIT GRONINGE thesis, defended on November 1, 2024, with the Ageis laboratory

[7] Grenoble-Alpes University thesis, defended on November 7, 2024, with the Ageis laboratory

AGENDA

Safe and autonomous smart hoisting system

A more autonomous overhead crane thanks to artificial intelligence.

Within the framework of Nanoelec, the teams from Schneider Electric and INRIA are developing a learning pipeline for artificial intelligence dedicated to the automatic control of load sway during autonomous movements of an overhead crane.

"The aim is to increase the autonomy of the overhead crane without compromising safety while reducing equipment maintenance and parameter setting times," says Charles Blondel, Head of R&D Dept. of the Industrial Automation Business Unit at Schneider Electric. *"Automation of hoisting systems requires the use of advanced sensors, such as scanners and cameras, as well as algorithms to interpret a whole range of data to generate reliable and safe decisions."*

Robotics is becoming increasingly present in plants, notably to improve productivity and safety when moving heavy loads. *"Autonomous Intelligent Vehicles (AIVs) or Autonomous Mobile Robots (AMRs) are now integrated into production lines, including with remote sensors around the infrastructure,"* explains Charles Blondel. It is possible to integrate this new Integrated Autonomous Crane System (IACS) without endangering the production line, surrounded by human employees. Following mathematical modelling of an overhead crane, the teams at Nanoelec defined an approach to the problem of crane control aiming to optimize the parameter settings of the existing controllers. An AI learning pipeline incorporating a simulator developed by Schneider Electric was then set up.

"We have generated datasets for simulations by varying the system parameters (acceleration, deceleration, maximum linear speed, overall time delay) across the range of control algorithm coefficients. A total of 32 distinct crane models were simulated," says Charles Blondel. *"The new approach, validated using a simplified model (3 degrees of freedom), enables automated deployment during the commissioning phase, ensures more consistent performance without human intervention, and delivers a 10% to 20% production increase on the SE bridge."*

SCHNEIDER ELECTRIC TEST BENCH FOR THE DEVELOPMENT OF A SAFE AND AUTONOMOUS SMART HOISTING SYSTEM

© Schneider Electric

8. With the collaboration of Grenoble INP - UGA and INRIA

AGENDA

NUMEROUS EXPERIMENTS ARE BEING CARRIED OUT IN EUROPE AND AROUND THE WORLD, MOSTLY AROUND LOCALIZED AND LIMITED AUTONOMOUS SHUTTLES

© pixabay.com

Validated perception solutions for autonomous vehicles

Multimodal perception systems for mobile robotics.

Within Nanoelec, Inria has been developing probabilistic perception and navigation systems for autonomous vehicles for years, enabling safe and explainable fusion and filtering of information and decision-making. The developed systems are particularly effective at dealing with multimodal data sources, coming from different types of embedded or deported sensors, making them particularely well-suited to complex dynamic environments. This core technological framework, in constant evolution, supports various transfer and associated research projects, empowering diferent indoor and outdoor autonomous mobile robots. Mainly focused this year on engineering issues, the work on the significant software and technology base has enabled much greater modularity and robustness, integrating into our solutions the latest developments in the mobile robotics community (ROS2, NAV2).

As explained by Lukas Rummelhard, research engineer at Inria working in the scope of Nanoelec, if the current improvement rate of data-driven AI systems might pave the way for large-scale deployment of autonomous vehicles in some environments, diffusion of such breakthrough technologies in many other use-cases may be hindered by a lack of sufficient relevant data and dedicated compute power, or validation and regulatory concerns.

Core to these developments, GPU optimization of methods and software have always been a key focus of effort to enable this probabilistic framework to be embedded. Such optimizations of data transfers have been the topic of a presentation at ROSConfr, by Hugo Bantignies, "The ROS2-type adaptation, a gateway to GPU hardware acceleration"[10].

Jean-Baptiste Horel (PhD at Inria) presented a Navigation-Based Evaluation Metric for Probabilistic Occupancy Grids at ITCS 2023[10]. *"We unveiled a new navigation-based metric for occupancy grid similarity evaluation. Our method addresses the limitations of existing metrics by evaluating the differences in pathfinding behavior between the ground truth and the inference occupancy grids,"* he states.

—

AGENDA

[9] **9.** Hugo Bantignies at ROSConFr - Nantes, June 19, 2024 "The ROS2-type adaptation, a gateway to GPU hardware acceleration".

[10] **10.** Horel, J.-B., Baruffa, R., Rummelhard, L., Renzaglia, A., & Laugier, C. (2023). A Navigation-Based Evaluation Metric for Probabilistic Occupancy Grids : Pathfinding Cost Mean Squared Error. ITCS 2023 - 26th IEEE International Conference on Intelligent Transportation Systems, 1-6. https://hal.science/hal-04211125

Digital identity management on a robotic system

Preventing identity theft.

Within Nanoelec/Pulse, the CEA teams are developing a demonstrator in response to the need to identify a person face-to-face via the anonymous trace of a record on a blockchain-type digital system. *"We are studying the question of digital identity in the industrial context and are producing the prototype of a connection interface for robotic system users,"* says Christine Hennebert, in charge of the project at CEA-Leti.

The goal is to guarantee user confidentiality on the digital system, while enabling the traceability of actions and the accountability of those involved to their employer or auditors. *"We are also developing solutions to prevent identity theft on the robotic system. The smart contracts technology is being used to implement an end-to-end confidentiality protocol between the user connection interface and the remote register, while respecting embedded system constraints."*

Blockchain hardware implementation

Following on from the “blockchain and digital identification” white paper, and in order to envisage the technology readiness level (TRL) of the demonstrators, Nanoelec is a member of the “Alliance Blockchain France” association. The Alliance Blockchain France recently joined the ACN (Alliance for digital trust) as GT4 “Blockchain”.
On the technical side, a third version of the testnet was deployed with a significant increase in maturity on the production and security side. A 4th version of the testnet is currently being prepared, to replace the consensus protocol at the heart of the blockchain.

© AdobeStock

An intrinsically secure processor

A modular design based on the Risc-V open standard.

After carefully identifying the vulnerabilities of the most common processors (microcontrollers, processors for IoT, personal computers and servers) in award-winning work in 2019[11], a team from CEA-Leti is continuing its work under the Nanoelec/Pulse program on 64-bit NaxRiscV, a Risc-V open standard processor[12]. *"By separately examining each logic level of the processor, we are looking to implement the "intrinsically secure processor" concept. The approach is in response to the worrying exponential increase in cyberattacks and the impossibility of guaranteeing a fault-free software code. It is then up to the intrinsically secure processor to prevent these vulnerabilities from being exploited,"* explains Olivier Savry, a researcher at CEA-Leti[13].

"The unique feature of this highly advanced processor is its modular design: we can thus study countermeasures proportionately to different levels of attack.

OLIVIER SAVRY,
CYBERSECURITY EXPERT
AT CEA-LETI

© Havret/CEA

[11] **11.** Olivier Savry, Thomas Hiscock, Mustapha El Majihi "Sécurité matérielle des systèmes", Dunod, 2019

[12] **12.** CIAMH : Confidentiality, Integrity and Authentication across the Memory Hierarchy, AIT LAHSSAINE Karim, SAVRY Olivier, RISC-V Summit Europe 2025

[13] **13.** Comprehensive Lockstep Verification for NaxRiscv SoC integrating RISCV DV, RVLS, and Questa/UVM, IGHILAHRIZ Billal, SAVRY Olivier, RISC-V Summit Europe 2025

AGENDA

Secure implementation of post-quantum cryptography

The NIST reaches a new milestone in post-quantum cryptography by selecting the HQC scheme to which IRT Nanoelec made significant contributions.

The international process to select the best post-quantum cryptography algorithms set up by the National Institute of Standards and Technology (NIST) has reached an important milestone with the selection of the HQC scheme with a view to standardization. This decision completes the first selection phase initiated in 2016 to define a new asymmetrical encryption standard able to withstand future quantum attacks.

Since 2020, the teams at IRT Nanoelec have been involved in studying HQC, addressing all the challenges represented by a new standard. Most of the work done consisted in a security analysis of HQC in the face of physical attacks. Most of the physical attacks published on HQC come from the work done by Nanoelec, underlining the expertise of its teams.

"We proposed a software implementation of HQC with the smallest memory footprint capable of embedding HQC on components with resource constraints," explains Antoine Loiseau, who is conducting research at CEA-Leti, within the framework of Nanoelec/Pulse. *"We also proposed a more advanced hardware architecture in terms of agility, making it possible to accelerate the main PQC schemes recently standardized."*

Post-quantum cryptography (PQC) will become the standard in the coming years and will replace the existing cryptography. The NIST in the United States, the ANSSI in France and the BSI in Germany have begun the technological and industrial cryptography transition.

The results of this research are published in open source so that the entire community can benefit from implementation of the performance on an embedded system.

WITHIN NANOELEC, RESEARCHERS FROM CEA HAVE PUBLISHED A FIRST LEVEL OF OPTIMIZATION FOR THE IMPLEMENTATION OF A COMMUNITY-ACCLAIMED STANDARDIZED POST-QUANTUM ALGORITHM (NIST COMPETITION), IN OPEN SOURCE

© A. Havret/CEA 2024