INFORMATION SHEET

Digital security and blockchain

Towards secure, distributed digital infrastructures

In order to meet performance and agility challenges faced by our modern society, cyber-physical systems must constantly evolve.

This evolution can be seen in the rapid and profound digitalisation of systems, driven by new hardware and software components that are massively connected and often distributed. These components, being more exposed, have become the preferred target of malicious actors whose knowledge, techniques, means and motivations are constantly growing. In this context, threat control and prevention are necessary but not always sufficient.

A paradigm shift is needed, to promote the deployment of robust, resilient and trusted systems from the design stage (i.e., by design).

CHALLENGES

Security must be thought of comprehensively, covering hardware, software and data, both in terms of prevention and reaction. There are many challenges: protection of sensitive or personal data, post-quantum cryptography, resilience of intrusion detection mechanisms, etc. Moreover, the human element is a determining factor in the effectiveness of the protection measures in place. Training requirements must be combined with the need to automate cybersecurity in a context where emerging technologies, such as artificial intelligence and distributed registers, are becoming increasingly important.

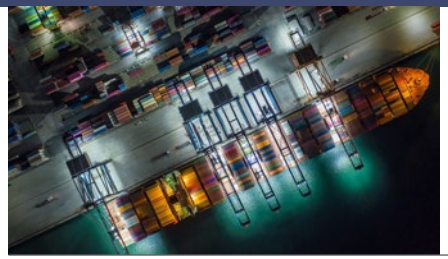
POSITIONING OF THE INSTITUTE

IRT SystemX addresses the challenges of cybersecurity and the management of distributed registers (i.e. blockchain) by proposing state-of-the-art solutions and developing upstream R&D projects with its partners. Machine learning-based innovative approaches are used to reduce attack surfaces. Cyber resilience approaches are studied and tested at the institute and work is carried out on blockchain architectures, protocols and scaling in various application areas such as connected mobility, maritime, energy, etc.

EXPERTISE

Identity management, access control and authorisation mechanisms, intrusion detection, applied cryptography, cyber risk analysis, cyber threat intelligence, blockchain, smart contract, privacy protection.

Projects in this field



PFS project

Designing and evaluating new architectures for Secure Ports of the Future

- Description and analysis of the port and ship of the future architectures
- Proposal of a best practice guide for maritime security governance
- Development and evaluation of digital security through a cyber-physical demonstrator

BST projet

Blockchain for Smart Transactions: demonstrating the uses and services facilitated by the adoption of blockchains

- Decentralised marketplace managed directly by its participants
- Access control and security mechanisms for sensitive data

SECOIIA Project - H2020

Secure Collaborative Intelligent Industrial Assets: securing vulnerable cyber-physical assets

- Detection by packet inspection on encrypted flows and traffic/ header inspection
- Fine-grained access control
- Automatic attack graph generation and remediation

Exploratory research

- Characterisation of various attacks in Code Based Cryptography
- Detection of intrusion patterns in encrypted data streams
- Evaluation of the robustness of artificial intelligence-based intrusion detection models against adversarial pattern attacks
- Convergence of cybersecurity and safety in intelligent transport architectures

Roadmap

SCIENTIFIC AND TECHNOLOGICAL CHALLENGES	RELATED RESEARCH FIELDS
Protection of services and data	• Dynamic identity management • Trust for secure processing • Projection of user data and privacy
Detection of attacks and reduction of the exposure window	• Evaluation of intrusion detection systems (IDS) • Improved attack detection and implementation of business IDS • Hybridization of detection approaches (signature, AI, business knowledge) • Intrusion detection on encrypted flows
Threat analysis and and reaction to attacks	• Identification of the hybrid threat (internal and external) • Threat identification and quantification • Digital resilience • Secure patch management • Hybridization of security and safety
Accompanying the rise in maturity of blockchains	• Foundations of blockchains (performance, security and energy consumption) • Federation and integration of blockchains (interoperability) • Security of smart contracts • Governance of blockchains

Platforms and demonstrators

CHESS

Environment for modelling and simulation of cyber-physical systems

- Catalogue of attacks and traffic generators
- Cyber-physical platforms: - for industry (CHESS5Industries) - for automotive (CHESS4Automotive)

Target of IRT SystemX publications in this field (HAL collection)

● JOURNALS

International Journal On Advances in Security, International Journal On Advances in Telecommunications, Ad-hoc networks

● CONFERENCES

ICISSP (International Conference on Information Systems Security and Privacy), ICIMP (Information Management and Processing), EUROCRYPT (International Conference on the Theory and Applications of Cryptographic Techniques), ICSC (International Conference on Systems and Control), IEEE CCNC (Consumer Communications & Networking Conference), ICNSS, CRISIS (International Conference on Risks and Security of Internet and Systems), IEEE VTC (Vehicular Technology Conference), SAFECOMP (International Conference on Computer Safety, Reliability and Security), IEEE S&B (Security and Privacy on the Blockchain), IFIP NTMS (International Conference on New Technologies, Mobility and Security), IEEE UEMCON (Annual Ubiquitous Computing, Electronics & Mobile Communication Conference), FPS (International Symposium on Foundations & Practice of Security), AsiaCrypt (Annual International Conference on the Theory and Application of Cryptology and Information Security), ACM CCS (ACM Conference on Computer and Communications Security), DBSec (Conference on Data and Application Security and Privacy), ACM SACMAT (Symposium on Access Control Models and Technologies)

Digital security and blockchain

ACADEMIC PARTNERS

RESEARCH GROUPS AND SCHOLARLY ORGANIZATIONS

INDUSTRIAL PARTNERS

ABOUT IRT SYSTEMX

SystemX is a technological research institute (IRT) with expertise in the fields of analysis, modelling, simulation and decision support for complex systems. As the only IRT dedicated to digital systems engineering, it coordinates partnership research projects, bringing together academics and industry in a multi-sector perspective. Together, they work to solve major scientific and technological problems in four priority application sectors: Mobility and Autonomous Transport, Industry of the Future, Defence and Security, Environment and Sustainable Development.

Through use-case oriented projects, SystemX's research engineers respond to the major societal and technological challenges of our time, and thus contribute to the acceleration of the digital transformation of industries, services and territories.

Located at the Paris-Saclay plateau and in Lyon, SystemX was created in 2012 as part of the future investment programme.

IN THE TEAMS

16 engineer-researchers

6 PhD project
5 of which have been defended

(September 2021)

CONTACTS

Responsable d'équipe
Reda Yaich
Reda.yaich@irt-systemx.fr

Responsable d'équipe
Nicolas Heulot
nicolas.heulot@irt-systemx.fr

Responsable d'axe scientifique
Makhlouf Hadji
Makhlouf.hadji@irt-systemx.fr

www.irt-systemx.fr/en/

@IRTSystemX

IRT SystemX