



Sécurité numérique et blockchain

Pour des infrastructures numériques distribuées et sécurisées

Les systèmes cyber-physiques doivent constamment évoluer afin de relever les défis de performance et d'agilité auxquels notre société moderne fait face.

Cette évolution se traduit par une digitalisation profonde et rapide, portée par de nouveaux composants matériels ou logiciels, connectés massivement et souvent distribués. Davantage exposés, ces composants sont désormais la cible privilégiée d'acteurs malveillants dont les connaissances, les techniques, les moyens et les motivations ne cessent de croître. Dans ce contexte, la maîtrise de la menace et sa prévention sont nécessaires mais largement insuffisantes.

Un changement de paradigme est indispensable, promouvant le déploiement de systèmes robustes, résilients et de confiance, et ce dès la conception (i.e., *by design*).



● ENJEUX

La sécurité doit être pensée de manière globale, couvrant à la fois le matériel, le logiciel et les données, et ce tant sur les volets préventifs que réactifs. Les enjeux sont multiples : protection des données sensibles ou personnelles, cryptographie post-quantique, résilience des mécanismes de détection d'intrusion, etc.

Par ailleurs, l'humain est un élément déterminant dans l'efficacité des mesures de protection mises en place. Les enjeux de formation sont à conjuguer avec le besoin d'automatisation de la cybersécurité dans un contexte où les technologies émergentes, comme l'intelligence artificielle et les registres distribués occupent une place de plus en plus importante.

● POSITIONNEMENT DE L'INSTITUT

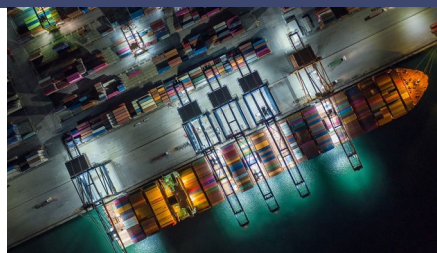
L'IRT SystemX s'intéresse aux défis de la cybersécurité et de la gestion des registres distribués (i.e. blockchain) en proposant des solutions à l'état de l'art et en développant des projets de R&D plus amont avec ses partenaires. Des approches innovantes, basées en particulier sur l'apprentissage automatique, permettent de réduire les surfaces d'attaques. Des approches de cyber-résilience sont étudiées et testées à l'institut et des travaux sont menés sur les architectures, protocoles et passage à l'échelle des blockchains dans des thématiques applicatives diverses telles que la mobilité connectée, le maritime, l'énergie, etc.

● EXPERTISES

Gestion des identités, contrôle d'accès et mécanismes d'autorisation, détection d'intrusion, cryptographie appliquée, analyse des risques cyber, *cyber threat intelligence*, blockchain, *smart contract*, protection de la vie privée.



Projets illustratifs



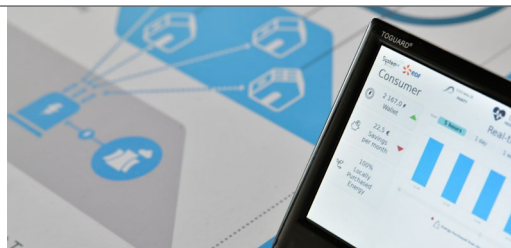
Projet PFS

Concevoir et évaluer de nouvelles architectures pour les Ports du Futur Sécurisés

- Description et analyse des architectures du port et du navire du futur
- Proposition d'un guide des bonnes pratiques pour la gouvernance de la sécurité maritime
- Développement et évaluation de la sécurité numérique par le biais d'un démonstrateur cyber-physique

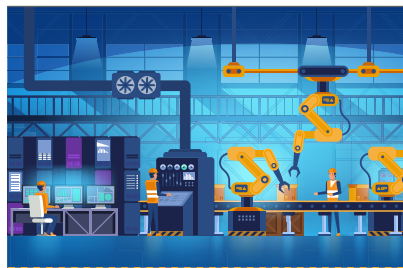
Projet BST Blockchain for Smart Transactions : faire la démonstration des usages et services facilités par l'adoption des blockchains

- Place de marché décentralisée gérée directement par ses participants
- Mécanismes de contrôle d'accès et de sécurisation des données à caractère sensible



Projet SECOIIA - H2020 Secure Collaborative Intelligent Industrial Assets : assurer la sécurisation des actifs cyber-physiques vulnérables

- Détection par inspection de paquets sur flux chiffrés et inspection du trafic/headers
- Contrôle d'accès à granularité fine
- Génération automatique de graphes d'attaque et remédiation



Recherches exploratoires

- Caractérisation de diverses attaques dans le *Code Based Cryptography*
- Détection de motifs d'intrusion dans des flux de données chiffrés
- Evaluation de la robustesse des modèles de détection d'intrusion à base d'intelligence artificielle face aux attaques par modèles adverses
- Convergences de la cybersécurité et de la *safety* dans les architectures de transport intelligent

Plateformes et démonstrateurs



CHESS

Environnement pour la modélisation et la simulation des systèmes cyber-physiques

- Catalogue d'attaques et générateurs de trafic
- Plateformes cyber-physiques :
 - pour l'industrie (CHESS5Industries)
 - pour l'automobile (CHESS4Automotive)



Feuille de route

DÉFIS SCIENTIFIQUES ET TECHNOLOGIQUES

VERROUS ASSOCIÉS

Protection des services et des données

- Gestion dynamique des identités
- Confiance pour les traitements sécurisés
- Projection des données et de la vie privée des usagers

Détection d'attaques et réduction de la fenêtre d'exposition

- Evaluation des systèmes de détection d'intrusion (IDS)
- Amélioration de la détection d'attaques et mise en œuvre d'IDS métier
- Hybridation des approches de détection (signature, IA, connaissances métier)
- Détection d'intrusion sur flux chiffrés
- Identification de la menace hybride (interne et externe)

Analyse de la menace et réaction aux attaques

- Identification et quantification de la menace
- Résilience numérique
- Gestion sécurisée des correctifs
- Hybridation de la sécurité et de la *safety*

Accompagner la montée en maturité des blockchains

- Fondements des blockchains (performances, sécurité et consommation énergétique)
- Fédération et intégration des blockchains (interopérabilité)
- Sécurité des *smart contracts*
- Gouvernance des blockchains

Cible des publications de l'IRT SystemX dans ce domaine (collection HAL)

● JOURNAUX

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

● CONFÉRENCES

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), ICN2S, 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)



Sécurité numérique et blockchain

PARTENAIRES ACADÉMIQUES

université
PARIS-SACLAY



INSTITUT
POLYTECHNIQUE
DE PARIS



GROUPEMENTS DE RECHERCHE ET SOCIÉTÉS SAVANTES



PARTENAIRES INDUSTRIELS



À PROPOS DE L'IRT SYSTEMX

SystemX est un institut de recherche technologique (IRT) expert en analyse, modélisation, simulation et aide à la décision pour les systèmes complexes. Seul IRT dédié à l'ingénierie numérique des systèmes, il coordonne des projets de recherche partenariale, réunissant académiques et industriels dans une perspective multi-filière. Ensemble, ils s'appliquent à lever des verrous scientifiques et technologiques majeurs de 4 secteurs applicatifs prioritaires : Mobilité et Transport

autonome, Industrie du futur, Défense et Sécurité, Environnement et Développement durable.

Au travers de projets orientés cas d'usage, les ingénieurs-chercheurs de SystemX répondent aux grands enjeux de notre temps, sociétaux et technologiques, et contribuent ainsi à l'accélération de la transformation numérique des industries, des services et des territoires.

Basé sur le plateau de Paris-Saclay et à Lyon, SystemX a été créé en 2012 dans le cadre du programme des investissements d'avenir.

DANS LES ÉQUIPES

16
ingénieurs-chercheurs

6 thèses
dont
5 soutenues

(septembre 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



@IRTSystemX



IRT SystemX

