Communiqué de presse

Cybersécurité des infrastructures numériques : SystemX dévoile les résultats de son ambitieux projet de recherche EIC

Centré sur la cybersécurité des systèmes du futur, le projet EIC vient de s'achever. Il affichait pour ambition de développer, en collaboration avec l'ANSSI, une plateforme expérimentale de confiance pour évaluer le couplage de technologies de cybersécurité au travers de scénarios concrets (véhicule connecté, IoT, usine 4.0, smart grids, etc.). Il a permis de lever des verrous technologiques majeurs liés à l'identification des menaces et à l'évaluation de la robustesse des infrastructures numériques. Les perspectives de poursuite des travaux sur la plateforme CHESS sont multiples.

Palaiseau, le 18 mai 2020 – L'Institut de Recherche Technologique (IRT) SystemX a annoncé la clôture de son premier projet de R&D en cybersécurité lancé en 2015 : Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité (EIC). Ce projet ambitieux, d'une durée de 5 ans, s'inscrivait dans le plan « Cybersécurité » de la NFI (Nouvelle France Industrielle). Il a fédéré 7 partenaires industriels (Airbus, Airbus Defence & Space, Bertin IT, Engie, Gemalto, Prove&Run, Thales) et 2 partenaires académiques (CEA et Télécom SudParis / IMT) autour de la nécessité de développer un environnement expérimental et humain de premier plan, afin d'accueillir et tester par simulation hybride les systèmes du futur ultra-connectés, lors de scénarios avancés.

Le projet EIC en chiffres

Durée : 5 ans
ETP : 12
9 partenaires industriels et académiques

- Création d'une plateforme technologique : CHESS
- 4 cas d'usage étudiés : IoT, véhicules connectés, usine du futur, smart grids
- Plusieurs publications (dont un best paper, ICIMP 2018, Barcelone)
- 4 rapports (assurance risque cyber)
- 2 brochures (« Les Cyberattaques et leurs préjudices dans les entreprises »)

Les travaux de R&D menés dans le cadre du projet offrent plusieurs avancées scientifiques et technologiques majeures :

- une meilleure connaissance et une anticipation précoce des menaces de cybersécurité ;
- une évaluation consolidée de la robustesse des contre-mesures mises en œuvre dans des cas d'usage réalistes ;
- une réponse unique aux exigences de supervision des attaques au travers d'une gestion opérationnelle intégrée ;
- et une contribution inédite à la sensibilisation aux risques et à l'entraînement des équipes en charge de la sécurité numérique.

CHESS : plateforme de confiance, labellisée par l'ANSSI et le CoFIS

Les équipes du projet ont bâti une plateforme technologique de pointe, en collaboration avec l'ANSSI pour une durée de 10 ans. Labellisée par le Comité de la Filière Industrielle de la Sécurité (CoFIS), CHESS (Simulation et analyse pour l'évaluation de la cybersécurité des architectures de systèmes) offre un environnement matériel et logiciel complet à la fois pour :

- les fournisseurs de solutions de sécurité : évaluation du niveau de protection atteint par leur composant innovant dans différents contextes d'utilisation,
- les grands utilisateurs - opérateurs d'importance vitale, banques, constructeurs automobiles, opérateurs de transports - et intégrateurs de solutions : évaluation de leurs choix d'architecture et de solutions de sécurité, identification des meilleures alternatives, etc.

« *CHESS met à disposition un environnement complet « neutre » et protégé pour évaluer la cybersécurité des systèmes hyperconnectés, sur des cas d'usage qui concernent les domaines émergeants des objets connectés et de traitement des Big Data. Tout type d'environnement industriel peut y être modélisé pour l'exécution de scénarios variés. Elle permet à la fois de mener des projets de recherche collaboratifs ambitieux tels que EIC, mais peut également être utilisée en mode ad hoc par les industriels qui souhaitent évaluer la menace cyber de leurs innovations et la robustesse des contre-mesures qui s'imposent* », explique Philippe Wolf, chef de projet EIC.

Des scénarios complexes simulés sur CHESS

Des cas d'usages variés dans les domaines de **l'usine du futur, des véhicules connectés, des *smart grids* et de l'internet des objets** ont été étudiés sur la plateforme CHESS :

- Utilisation d'une infrastructure Blockchain afin de sécuriser les mises à jour d'objets connectés, de corriger leurs vulnérabilités et de se prémunir contre les piratages, comme par exemple sur des véhicules connectés.
- Illustration de la viabilité de l'utilisation de la cryptographie homomorphe pour renforcer de manière significative la sécurité de l'authentification biométrique
- Démonstration de la vulnérabilité des Smart Grids, notamment au niveau des données à caractère privé
- Analyse comportementale d'une baie industrielle de traitement de l'eau et de ses dysfonctionnements.

Missions de formation et de sensibilisation

SystemX a organisé, en collaboration avec l'ANSSI, **l'entraînement de l'équipe de France Cyber** pré-sélectionnée par l'ANSSI (candidatures libres « juniors »-moins de 20 ans et « seniors »-de 21 à 25 ans-) du 3 au 6 septembre 2019, afin de la préparer au Challenge européen de cybersécurité (ECSC) à Bucarest (octobre 2019). Au programme : des sessions de montée en compétences et de perfectionnement sur les techniques et méthodologies de découverte et d'exploitation de vulnérabilités et des exercices de mise en situation proche du réel au travers d'un jeu de « hacking éthique » de type CTF (Capture The Flag). La plateforme expérimentale CHESS a servi de terrain de jeu pour entraîner l'équipe France Cyber à déjouer des scénarios d'attaques complexes. Fort de cette première réussite, SystemX et l'ANSSI renouvellent leur collaboration pour le challenge 2020. Des sessions de sensibilisation et de formation sont également menées à la demande d'entreprises.

Le nombre de Cyber-attaque sous-estimé

SystemX a enquêté pendant près de trois ans **auprès d'entreprises, TPE et PME françaises, victimes de cyberattaques réussies pour quantifier l'impact réel des cyber-préjudices en France**. Cette étude inédite a permis de faire voler en éclats deux croyances communément admises : le nombre de cyberattaques réussies, de l'ordre de 2 à 5%, s'avère bien supérieur aux estimations habituellement rendues publiques, tandis que le coût moyen des cyberattaques se révèle en revanche beaucoup plus faible que supposé et s'évalue en milliers d'euros.

Et surtout, elle a permis de sensibiliser largement les petites structures aux cyber-risques et mesures élémentaires à mettre en œuvre.

Des études ont également été réalisées avec les assureurs pour mieux maîtriser le risque cyber sur l'ensemble de la chaîne de sa valeur (sous-traitance) et son transfert vers l'assurance. L'exercice s'est étalé sur 3 années jusqu'à la simulation financière d'un scénario cyber s'appliquant à la filière aéronautique qui a démontré que le coût global d'une catastrophe numérique n'était pas supportable dans la situation actuelle. Une dizaine de thèmes clés ont été proposés à l'ensemble de la filière pour agir sur les points faibles de demain.

Une thèse dédiée à la simulation d'attaques dans le domaine de la cyberdéfense

Dans le cadre du projet EIC, une thèse sur le thème « Simulation d'activité et d'attaques : application à la cyberdéfense » a été défendue par Pierre-Marie Bajan (IRT SystemX, Télécom SudParis). Son objectif : développer une nouvelle méthode de simulation en réseau pour créer un environnement d'évaluation des produits de sécurité et des services. L'ambition était d'exécuter des applicatifs industriels (navigateurs web, programmes industriels, etc.) dont seules les données échangées sont nécessaires à l'évaluation de ces produits et services, et ainsi de limiter la consommation de ressources. Les applicatifs industriels ont ainsi été remplacés par un programme capable de reproduire leurs données au bon format et applicable sur un environnement réseau plus léger.

Évaluation des systèmes de détection d'intrusion

La détection d'intrusion repère des activités malveillantes sur un hôte et/ou sur un environnement réseau. Il existe une variété de systèmes de détecteurs d'intrusion et le projet EIC s'est attaché à définir et expérimenter des méthodologies, des techniques et des outils d'évaluation facilitant la comparaison objective des différents types d'IDS (*Intrusion detection Systems*).

EIC ouvre la voie à d'autres perspectives dans de nombreux secteurs industriels

EIC a été le premier projet en cybersécurité lancé par l'IRT SystemX. D'autres projets en ont rapidement émergés, dans plusieurs domaines : dans le domaine du véhicule connecté : **le projet SCA** lancé en 2017 visant à répondre aux défis de « security & privacy » liés au déploiement du véhicule autonome et connecté, et **le projet CTI** dont l'objectif est de fédérer à travers une approche commune, les bonnes pratiques et solutions IT innovantes en matière de cybersécurité dans les domaines de l'automobile, du transport ferroviaire et de l'aéronautique.
Dans le domaine portuaire, **le projet PFS** (Ports du Futur Sécurisés) lancé en 2019 porte sur l'identification des fonctions maîtresses des ports maritimes, la définition d'une politique globale de sécurité et la création de démonstrateurs associés à ces métiers. Il s'appuie sur CHESS et teste des scénarios d'attaques et des réponses possibles. Le projet a pour objectif l'étude, le développement et la validation d'un ensemble de solutions (matérielles et logicielles) de sécurité numérique nécessaires à la protection des infrastructures portuaires actuelles et futures.

« Le projet EIC nous a permis de lever de nombreux verrous technologiques dans le domaine de la cybersécurité appliquée à l'industrie. Au-delà de ces projets, SystemX et ses partenaires du domaine développent de nouvelles opportunités d'innovation collaborative sur la cybersécurité des systèmes industrielles, incluant les objets connectés critiques, la sécurisation des données en tenant compte de leur DCIT (Disponibilité, Confidentialité, Intégrité, Traçabilité), et l'entraînement jusqu'à la gestion de crise » déclare Gilles Desoblin, responsable de la thématique cybersécurité, IRT SystemX.

À propos de l'IRT SystemX

SystemX est un institut de recherche technologique (IRT) expert en analyse, modélisation, simulation et aide à la décision appliqués aux 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, Lyon et Singapour, SystemX a lancé depuis sa création en 2012, 53 projets de recherche (dont 29 en cours), impliquant plus de 100 partenaires industriels et 55 laboratoires académiques, et compte actuellement 197 collaborateurs en équivalent temps plein (ETP) dont 134 ressources propres.
Pour en savoir plus : www.irt-system.fr | @IRTSystemX | LinkedIn | YouTube

Contacts presse
Marion Molina – Claire Flin
Tél. 06 29 11 52 08 / 06 95 41 95 90
marionmolinapro@gmail.com / clairefline@gmail.com