Le premier bulletin de la Chaire Cybersécurité des Infrastructures Critiques

Bienvenue à la premiere édition du bulletin de la Chaire Cybersécurité des Infrastructures Critiques. Dans ce qui sera des bulletins réguliers, nous rendons compte des activités et des réalisations de la Chaire.

Introduction à la Chaire

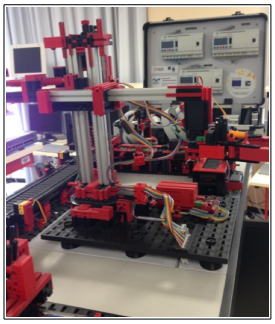
Cybersécurité des Infrastructures Critiques

La chaire a pour objectif de développer des solutions, validées théoriquement et expérimentalement, pour protéger et défendre ces infrastrutures face aux cyber attaques. La Chaire Cyber CNI de l'Institut Mines Télécom est portée par IMT Atlantique, et avec les écoles partenaires Telecom ParisTech et Telecom SudParis. Elle est soutenue par Airbus Defence and Space, Amossys, BNP Paribas, EDF, Nokia, Orange, La Poste, Société Générale et la Région Bretagne. Elle est reconnue dans le cadre du Pôle d'Excellence Cyber.

RECHERCHE

Axes de recherche de la Chaire

Métriques, Analytiques, Résilience et Gestion des données



Ces quatre thèmes définissent les axes de recherche de la chaire, avec les questions suivantes. Comment mesurer l'impact d'une menace et l'efficacité des contrôles ? Comment traiter les menaces tout en assurant la continuité des services ? Comment collecter de grands volumes d'événements de sécurité ? Comment analyser et corréler ces grands volumes d'événements pour identifier des menaces de sécurité ? Nous travaillons également sur des axes transversaux. Ils incluent les aspects psychologiques et métier dans les solutions de sécurité proposées. Les travaux s'appuient sur des plateformes de recherche (voir ci-contre une de nos plateformes système de contrôle industriel).

Social

chairecyber-cni.org #Cybersécurité http://chairecyber-cni.org

CONTENU

ACTUALITÉ DE LA CHAIRE

Journée SEE Cybersécurité de l'IoT à IMT Altantique, Rennes

European Cyber Week : Cybersécurité de l'internet des objets

Frederic Cuppens, **Rennes**

01/12/2017 L'Internet des objets (IoT) fait appel à des technologies avancées en matière d'architectures de systèmes, de réseaux de communications, de protocoles, de traitement et de stockage des données. Son enjeu économique est considérable et son développement intéresse tous les secteurs d'activité : grand public, industrie, services notamment d'intérêt public (énergie, traitement de l'eau ou transport). Toutefois, dans tous ces domaines, la cybersécurité est une préoccupation fondamentale car L'IoT, du fait de sa connexion au monde IP, de son étendue géographique et de son évolutivité, présente des vulnérabilités spécifiques.

La conférence organisée par la SEE et IMT Atlantique dans le cadre de la European-Cyberweek 2017, fait le point sur les travaux menés dans le cadre du cercle des entreprises de la SEE suite à la parution de l'étude IoT 2018 (voir ci-dessous).

La conférence s'est attachée à présenter les derniers développements dans le domaine de la cybersécurité de l'Internet des objets, notamment à partir des premiers retours d'expérience du terrain, en France et à l'étranger, des évolutions de la technique, des normes et des certifications de matériels. Après une table ronde sur sa prise en compte dans l'internet des objets, des recommandations ont été proposées aux participants. ■

THESE DE DOCTORAT CNI

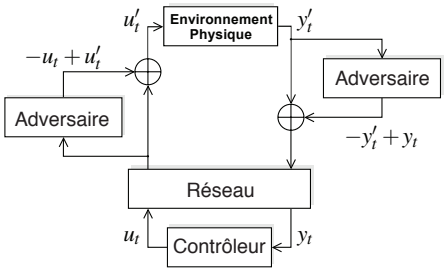
Thèse sur la sécurité des systèmes cyber-physiques industriels

Soutenue à Télécom SudParis par Jose Rubio-Hernan le 18 juillet 2017.

Télécom SudParis, **Evry**

Les recherches actuelles sur la sécurité des systèmes cyber-physiques est axée sur des adversaires cybers ou des adversaires physiques, mais ne considèrent pas la combinaison des deux. La thèse aborde cette problématique, et propose des contributions pour la détection d'attaques contre des systèmes cyber-physiques. Un système cyber-physique est, généralement, un système de contrôle industriel mis à niveau avec de nouveaux systèmes informatiques et de communication. Ces nouvelles capacités permettent d'améliorer l'interconnexion de ces systèmes.

La thèse réexamine aussi la sécurité d'un système de détection proposé par Mo et Sinopoli (2009) et Mo et al. (2015). Dans leur approche, l'utilisation des filtres de Kalman et des régulateurs linéaires quadratiques est complétée par un signal de marquage pour la détection d'attaques contre l'intégrité des systèmes cyber-physiques.



Dans un premier temps, la thèse montre que l'approche de Mo et Sinopoli ne détecte que des adversaires naïfs, qui ont seulement la possibilité d'écouter et d'enregistrer les informations du système, mais qui ne cherchent pas à acquérir des connaissances sur le modèle du système lui-même. En effet, le détecteur ne parvient pas à protéger le système contre des adversaires cyber-physiques, c'est-à-dire, des adversaires qui en plus d'écouter et d'enregistrer les informations d'un système, sont également en mesure de déduire le modèle du système pour échapper à la détection.

Thése de Doctorat conjointe à Telecom SudParis et l'Université Pierre et Marie Curie, encadrée par le professeur Joaquin Garcia-Alfaro.

Ensuite, la thèse propose une amélioration basée sur des signaux d'authentification à marquage multiple. La nouvelle version du détecteur est capable de protéger le système contre les adversaires cyber-physiques définis dans le travail. ■

ACTUALITÉ DE LA CHAIRE

La chaire Cyber CNI invite les chaires cyber bretonnes

12ième conférence sur les risques et la sécurité des systèmes d'information

Nora et Frederic Cuppens, **Rennes**

19-21/09/2017 La chaire Cybersécurité des Infrastructures et le Laboratoire de Hautes Sécurité ont organisé à Dinard, du 19 au 21 septembre, la douzième édition de la conférence CRISIS sur les risques et la sécurité des systèmes d'information. Cette conférence offre un forum remarquable aux acteurs de la cybersécurité de l'industrie, du monde académique et des institutions gouvernementales pour se rencontrer, échanger de nouvelles idées et présenter les avancées récentes sur les menaces et les vulnérabilités de l'Internet ainsi que les solutions de sécurité pour y faire face. Les sujets traités par cette conférence concernent l'analyse des risques, les attaques contre les systèmes et les réseaux, les modèles et les mécanismes de sécurité ainsi que les technologies pour protéger la vie privée et améliorer la résilience des systèmes.

Lors de cette conférence, une session technique ainsi qu'une table-ronde ont été organisées par la chaire Cyber CNI sur le thème "Comment accélérer le renforcement de la cybersécurité ?". Cette table-ronde, animée par Stéphane Grunenwald, lieutenant-colonel à l'Ecole des Transmissions, a permis aux 4 chaires cyber bretonnes d'échanger leur point de vue : Chaire de Cyberdéfense et Cybersécurité de Saint-Cyr-Sogeti-Thales, Chaire Cyberdéfense des Systèmes Navals, Chaire Analyse de la Menace et Chaire Cyber CNI. Au cours de cette table-ronde, Paul Lajoie-Mazenc (EDF) Gérard Le Comte (Société Générale) et Simon Foley sont intervenus pour la chaire Cyber CNI. Gérard Le Comte a également présenté une conférence invitée intitulée "A journey in banking information security". Le proceedings de la conférence CRISIS 2017 (Cuppens et. al., éditeurs) sera publié par Springer Verlag *Lecture Notes in Computer Science*. ■

ACTUALITÉ DE LA CHAIRE

Prix du meilleur papier au GAMESEC 2017

Z. Ismail et J. Leneutre, *A Game Theoretical Model for Optimal Distribution of Network Security Resources, International Conference on Conference on Decision and Game Theory for Security.*

Telecom ParisTech, **Paris**

Ziad Ismail recevant le prix du meilleur article à GAMESEC 2017.

Ziad Ismail, post-doctorant et Jean Leneutre, enseignant chercheur, ont obtenu la récompense du meilleur article à *GAMESEC (Conference on Decision and Game Theory for Security)* qui s'est tenue à Vienne en Autriche en octobre 2017. Cet article a été co-écrit avec Christophe Kiennert (post-doctorant à Telecom SudParis) et Lin Chen (Maître de Conférences au LRI, Université Paris Saclay).

Les travaux récompensés ont été initiés dans le cadre du projet MSSTB (Modélisation de Stratégies de Sécurité et de Tableaux de Bord) du programme Investissement d'Avenir financé par la Caisse des Dépôts et Consignations, en collaboration avec Airbus Defence & Space CyberSecurity et Cogisys, et ont été développés et finalisés dans le cadre de la chaire Cyber CNI.

La conférence GAMESEC créée en 2010 a pour objectif de réunir des chercheurs académiques et industriels afin de présenter des résultats récents appliquant la théorie de la décision et la théorie des jeux à des problématiques de sécurité.

L'objectif global des travaux récompensés est de fournir une méthode permettant d'optimiser la distribution des ressources de sécurité étant donné un budget de défense limité. Pour cela, l'article définit une classe générique de jeux de sécurité, appelés Resource Constrained Network Security (RCNS), et propose des résultats concernant les solutions de ces jeux dans le cas général. L'article applique ces résultats au cas particulier du problème d'allocation optimale des ressources de détection d'intrusion dans un réseau en prenant en compte les interdépendances des vulnérabilités des différents équipements. Ces résultats sont ensuite validés de manière numérique sur une étude de cas. Ces travaux s'incrivent dans la thématique de la chaire Cyber CNI visant à proposer des approches quantitatives pour la gestion des risques de sécurité des infrastructures critiques. ■

RECHERCHE

L'expérience humaine au cœur des travaux de la chaire Cyber CNI

Étudier l'expérience humaine dans des centres d'opérations de sécurité.

Vivien Rooney, **Rennes**

Un centre d'opérationnel de la sécurité (SOC, Security Operating Center) est vital pour la protection des systèmes critiques. Le fonctionnement efficace d'un SOC doit reposer non seulement sur la technologie et les outils, mais aussi sur ses personnels, dont les compétences permettent d'utiliser ces outils de la meilleure manière possible, à mesure que l'information est analysée et que les solutions sont mises en œuvre.

La Chaire Cybersécurité de l'IMT innove dans le domaine de la cybersécurité, en utilisant la recherche en psychologie appliquée pour comprendre le fonctionnement des SOC. Un psychologue de la Chaire interviewe le personnel travaillant dans les SOC afin d'identifier l'expérience utilisateur (UX) du travail dans le SOC : l'analyse est donc axée sur les personnes et vise à mieux comprendre l'expérience humaine de la technologie et des processus opérationnels connexes. Ainsi, plutôt que de considérer, par exemple, uniquement la facilité d'utilisation des outils de sécurité, la recherche considère d'autres aspects de l'expérience humaine individuelle, tels que le sensoriel et l'intellectuel.

L'objectif de cette recherche interdisciplinaire est de développer une compréhension psychologique de l'expérience de travail dans un SOC, en vue d'appliquer ces connaissances pour améliorer la manière dont les SOC peuvent fonctionner. ■

Les brèves

Alexandre Kabil remporte le défi Ma thèse 3.0

30/11/2017 Alexandre Kabil et Edwin Bourget, doctorants de la Chaire Cyber CNI, ont présenté leur sujet de thèse en 3 minutes au Défi Ma thèse 3.0 de la European Cyberweek organisé par la Réserve Citoyenne de Cyberdéfense en partenariat avec Orange Cyber Défense et Nokia. Félicitations à Alexandre qui a remporté le premier prix pour sa presentation *"CyberCOP 3D : visualisation 3D interactive et collaborative de l'état de sécurité d'un système informatique"*, une thèse dirigée par Thierry Duval et Nora Cuppens.

Cybersécurité : la science est entrée en guerre

20/11/2017 *"Le type de cibles est en train de changer et l'impact potentiel de ces attaques d'un nouveau genre bien plus important"* analyse de Frédéric Cuppens dans Les Echos sur la nécessité de concevoir des systèmes cyber résilients capables de résister à ces nouvelles cyber attaques.

Colloque scientifique IMT sur la cybersécurié

10/11/2017 Frédéric Cuppens et Hervé Debar ont organisé le colloque scientifique IMT sur le thème *Entrons-nous dans une nouvelle ère de la cybersécurité ?* Simon Foley a présenté la chaire Cybersécurité des Infrastructures Critiques et Joaquin Garcia Alfaro a parlé de ses travaux sur la détection des attaques contre les systèmes cyber-physiques industriels réalisés dans le cadre de la chaire.

RECHERCHE

Sélection de Publications Récentes

[1] S. Foley, "Getting security objectives wrong : A cautionary tale of an industrial control system," in *International Security Protocols Workshop*, 2017, pp. 18–37. [Online]. Available : Link

[2] Z. Ismail *et al.*, "A game theoretical model for optimal distribution of network security resources," in *GameSec 2017*, 2017. [Online]. Available : Link

[3] V. Rooney and S. Foley, "What users want : adapting qualitative research methods to security requirements elicitation." in *Workshop on Security and Privacy Requirements in Software Engineering*, 2017, pp. 229–249. [Online]. Available : Link

[4] J. Rubio-Hernan, "Detection of attacks against cyber-physical industrial systems," Ph.D. dissertation, Télécom SudParis, 2017.

[5] J. Rubio-Hernan, L. De Cicco, and J. Garcia-Alfaro, "Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems," *Trans. Emerging Telecommunications Technologies*, vol. 32(09), 2017. [Online]. Available : Link

[6] ——, "On the use of watermark-based schemes to detect cyber-physical attacks," *EURASIP Journal on Information Security*, vol. 2017, no. 1, p. 8, 2017. [Online]. Available : Link

■