Chaire Cybersécurité des Infrastructures Critiques (CyberCNI.fr)

le nom et l'acronyme du projet ;

Chaire Cybersécurité des Infrastructures Critiques (CyberCNI.fr)

l'identité et l'affiliation du porteur·euse ;

Titulaire : Marc-Oliver Pahl, IMT Atlantique, Rennes (marc-oliver.pahl@imt-atlantique.fr)

le consortium

- acteurs collectivités territoriales
  - Region Bretagne
  - Pôle d'Excellence Cyber
- contrat industriel
  - Airbus Cybersecuritée
  - Amossys
  - BNP Paribas
  - EDF
  - SNCF

l'instrument de financement ;

Les thèses sont indirectement financé par des industriels par un don à la fondation Mines Télécom.

les dates de début et de fin de projet ;

2/ 2022 – 2/ 2025

la plage de TRL associée aux innovations.

Les résultats de la recherche sont typiquement dane des TRL2 - TRL4. La chaire opère un testbed grand avec les partenaires qui est utilisé pour la validation.

Condition de recevabilité

Le projet est soutenu par :

- acteurs collectivités territoriales
  - Region Bretagne
  - Pôle d'Excellence Cyber
- contrat industriel
  - Airbus Cybersecuritée
  - Amossys
  - BNP Paribas
  - EDF
  - SNCF

Figure 1: Some members of the chaire cyberCNI.fr at a presentation at EDF in fall 2021.

La chaire Cybersécurité des Infrastructures Critiques (cyberCNI.fr) est la plus importante chaire de recherche en cybersécurité au sein du groupe IMT avec actuellement six partenaires industriels et trois partenaires régionaux / publics. La chaire accueille 13 doctorants, 5 post-docs, 2 ingénieurs, et compte 15 professeurs associés. Voir Figure 1. La chaire est une chaire industrielle qui est généralement financée par des cycles de 3 ans. La troisième phase de financement commence au printemps 2022.
Dans cette présentation, nous allons introduire le programme scientifique de la troisième phase. Notre objectif est de favoriser la collaboration au sein de la communauté de recherche française, en faisant du RESSI la première adresse pour cela.

Introduction

Les cyberattaques sont plus que jamais d'actualité en 2022. Les récentes attaques par ransomware ont notamment montré à quel point les infrastructures critiques sont vulnérables aujourd'hui. La softwarisation et la connectivité croissantes des systèmes distribués des technologies de l'information (IT) et des technologies d'exploitation (OT) rendent indispensables la sécurité par la conception, la détection continue des anomalies, les défenses semi-automatiques et entièrement automatisées, et l'intégration de l'utilisateur dans la boucle pour divers aspects, notamment la configuration, la connaissance de la situation et l'analyse des risques.

La phase 3 de la chaire Cybersecurity for Critical Networked Infrastructures (Cyber CNI) de l'Institut Mines Telecom se concentre sur ces aspects. Les doctorants, postdocs, ingénieurs, professeurs et tous les autres membres de la chaire continueront à consacrer leur énergie à l'amélioration de la cybersécurité et, avec elle, de la résilience des infrastructures critiques.

La chaire envisage ses activités de recherche dans les deux sens : recherche et enseignement pour soutenir et communiquer la recherche. Cela inclut des événements de diffusion plus larges tels que la série mensuelle de conférences talk.cybercni.fr et les écoles doctorales Future-IoT.org. Avec la participation à des événements tels que le FIC ou le CEW, ces activités favorisent la collaboration en matière de recherche. Par conséquent, cette

présentation couvre les deux avec un accent sur les activités de recherche prévues dans la phase 3.

Méthodologies

Dans la phase 3, le concept de gestion bien établi avec son interaction étroite entre les partenaires industriels et le personnel de la chaire, en premier lieu ses doctorants, se poursuivra.

Les événements de mise à jour de la recherche du printemps et de l'automne offriront aux entreprises l'occasion de diffuser les fruits de la collaboration avec la chaire, car leur mode hybride continuera d'offrir un accès facile à toutes les personnes intéressées au sein des entreprises. Les rencontres sur site chez les partenaires continueront à permettre d'approfondir l'échange avec les équipes locales, permettant également d'intéresser de nouvelles personnes à s'engager comme collaborateur de thèse. Avec son caractère de présentation de tous les sujets et de leur avancement, cet événement continuera également sa fonction de guide pour les partenaires industriels afin de s'attacher dynamiquement à différentes thèses si les intérêts et les besoins changent.

Les cycles de mise à jour mensuels avec les étudiants pour tous les représentants de l'industrie intéressés continueront à garantir un suivi et un encadrement étroits des thèses de doctorat. Cela permettra également une collaboration étroite, par exemple en échangeant des données ou en pilotant des algorithmes développés ou testés.

Les publications continueront à renforcer la position de la chaire dans la communauté des chercheurs. L'amélioration de l'image de marque augmentera la visibilité de la chaire lors des événements scientifiques.

L'école doctorale (https://school.future-iot.org) fournira une base unique pour une visibilité internationale. Il en va de même pour la série de conférences sur la cybersécurité (https://talk.cybercni.fr). Le site web (https://cyberCNI.fr) continuera à servir de vitrine pour rendre visible le travail de la chaire et de ses partenaires à un large public. La stratégie médiatique avec de fréquentes interviews et la participation à des événements servent le même objectif. Il en va de même pour les présences à des événements tels que le Forum international de la cybersécurité (FIC) et la Semaine européenne du cyberespace (ECW).

Le banc d'essai cyberCNI permettra une nouvelle qualité d'expérimentation, de validation et de compréhension. Il est ouvert aux partenaires, permettant un échange étroit et un travail conjoint entre les partenaires et la chaire.

Axes de recherche

La phase 3 de la chaire est organisée en quatre axes. Voir Figure 2. Ces axes sont 1) la sécurité par la conception, 2) la surveillance et l'analyse des données, 3) la défense (semi-) automatisée, 4) l'humain dans la boucle. Ces axes sont reliés par des activités telles que les différentes techniques de gestion de la sécurité, la connaissance de la situation ou l'analyse

des risques.

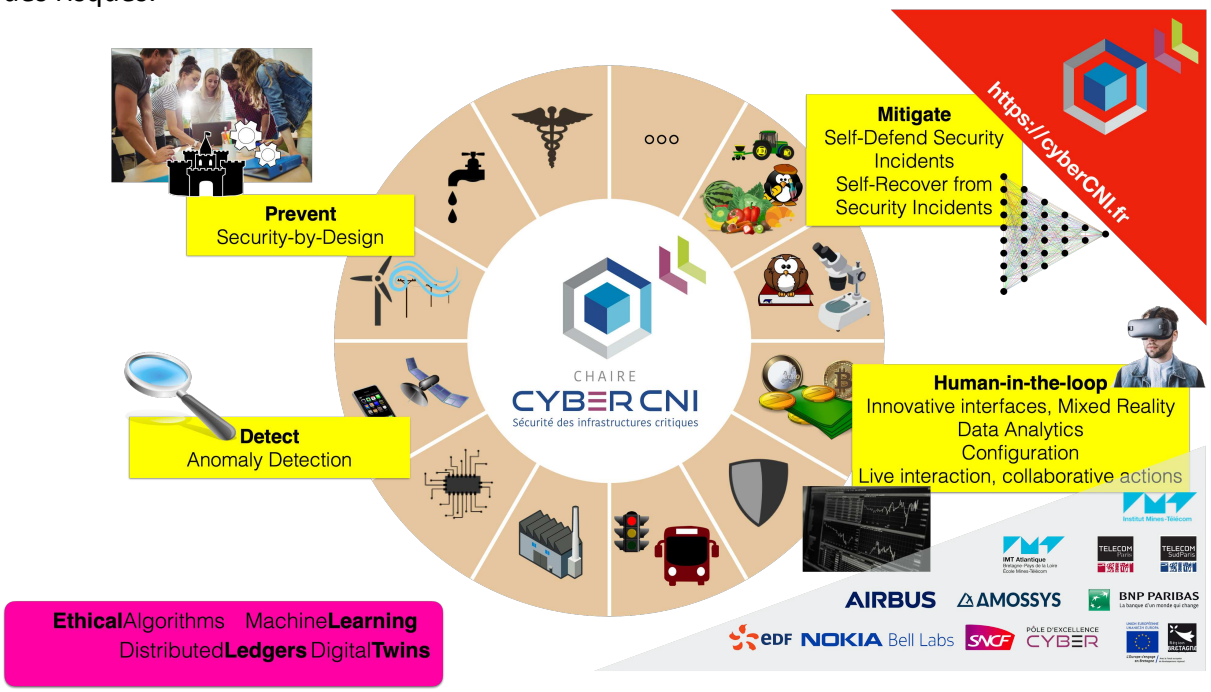

Figure 2: The research axes of the third phase of the chaire cyberCNI.fr.

Les thèmes de recherche prévus sont les suivants :

- P3-1- Modular Digital Twin-based cyber resilience (IMT Atlantique)
    - Modélisation des systèmes et des attaques afin d'obtenir des informations, de permettre de meilleures analyses et d'atténuer les cyberattaques.
- P3-2- Simulation and Deceptive Infrastructures for investing attack and mitigation mechanisms (IMT Atlantique)
    - Conception et mise en œuvre d'une infrastructure de déception et d'expérimentation reproductible pour recueillir des informations sur les attaques dans le monde réel, et pour étudier et valider les techniques de détection et de traitement des incidents de cybersécurité.
- P3-3- CodeLedger- tracking the provenance of critical open-source components (Télécom Paris)
    - Rendre l'interaction des composants logiciels plus sûre en gérant les dépendances.
- P3-4- How DLT can improve trust in the use of Al for cybersecurity (Télécom Sudparis)
    - Utilisation de grands livres distribués pour améliorer la confiance dans l'IA pour la cybersécurité.
- P3-5- Multi-Modal Collaborative Cybersecurity Operation Center (IMT Atlantique)
    - Interfaces collaboratives multimodales innovantes pour comprendre les systèmes et leur comportement ainsi que les algorithmes qui sous-tendent leur cybersécurité, comme l'explication des aspects de l'IA utilisée.
- P3-6- Improving resilience through securing software in IT and OT (PostDoc) (IMT Atlantique)
    - Sécuriser le côté logiciel des infrastructures critiques tout au long de la vie d'un logiciel, de sa conception à son déclassement.

Tous les travaux ont une interaction étroite. Les interfaces (P3-1) seront utilisées dans et utiliseront les données, les cas d'utilisation et l'expérimentation des autres projets. Le banc d'essai cyber-physique (P3-2), avec sa tromperie, son pot de miel et son expérimentation reproductible, fournit des informations précieuses et des possibilités de validation pour les autres projets. Les jumeaux numériques (P3-3) offrent de nouvelles possibilités d'analyse des risques et de développement de la défense en combinaison avec les autres projets. La connaissance des dépendances au sein et entre les composants logiciels (P3-4) fournit des données et des cas d'utilisation pertinents pour les autres projets. Une confiance accrue dans les technologies de cybersécurité (P3-5) améliore les composants développés dans les autres projets. Avec son rôle central, le projet PostDoc lié au cycle de vie des logiciels permettra non seulement de pousser plus loin la recherche sur les défis concrets dans ce domaine, mais il apporte également un potentiel pour stimuler les autres projets.

Un élément central, point de connexion entre les travaux intertnaux, et lien vers les collaborations externes est le testbed cyberCNI.fr qui est utilisé pour l'expérimentation et la validation des résultats de recherche obtenus. Voir Figure 3.

La présentation détaillera les travaux des doctorants et postdocs et les mettra en contexte de tous les travaux en cours à la chaire. Cela fournira une bonne vue d'ensemble et de nombreux points de connexion pour les autres chercheurs.

Figure 3: Parts of the cyberCNI.fr testbed infrastructurte.

References

Les références récentes suivantes donnent un aperçu du contexte des travaux prévus.

1. Barbeau, M., Cuppens, F., Cuppens, N., Dagnas, R., & Garcia-Alfaro, J. (2020). Metrics to enhance the resilience of cyber-physical systems. *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 1167–1172. https://doi.org/10.1109/TrustCom50675.2020.00156

2. Barbeau, M., Cuppens, F., Cuppens, N., Dagnas, R., & Garcia-Alfaro, J. (2021). Resilience Estimation of Cyber-Physical Systems via Quantitative Metrics. *IEEE Access*, *9*, 46462–46475. https://doi.org/10.1109/ACCESS.2021.3066108
3. Bender, M., Kirdan, E., Pahl, M.-O., & Carle, G. (2021). Open-Source MQTT Evaluation. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–4.
4. Bkakria, A., Cuppens, N., & Cuppens, F. (2020b). Pattern Matching on Encrypted Data. *IACR Cryptol*, 1–28.
5. Bkakria, A., Tasidou, A., Cuppens-Boulahia, N., Cuppens, F., Bouattour, F., & Ben Fredj, F. (2019). Optimal Distribution of Privacy Budget in Differential Privacy. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11391 LNCS*, 222–236. https://doi.org/10.1007/978-3-030-12143-3_18
6. Bourget, E., Cuppens, F., & Cuppens-Boulahia, N. (2020a). PROS2E, a Probabilistic Representation of Safety and Security Events for Diagnosis. *CPSS 2020 - Proceedings of the 6th ACM Cyber-Physical System Security Workshop, Co-Located with AsiaCCS 2020*, 30–41. https://doi.org/10.1145/3384941.3409590
7. Clédel, T., Cuppens, N., & Cuppens, F. (2019a). Managing the overestimation of resilience. *ACM International Conference Proceeding Series*. Published. https://doi.org/10.1145/3339252.3340333
8. Clédel, T., Cuppens, N., Cuppens, F., & Dagnas, R. (2020). Resilience properties and metrics: how far have we gone? *Journal of Surveillance, Security and Safety*, 119–139. https://doi.org/10.20517/jsss.2020.08
9. Delcombel, N., Kabil, A., Duval, T., & Pahl, M.-O. (2021). *CyberCopter: a 3D helical visualisation for periodic signals of cyber attacks*. VR4Sec: 1st International Workshop on Security for XR and XR for Security.
10. Dernaika, F., Cuppens-Boulahia, N., Cuppens, F., & Raynaud, O. (2019). Semantic mediation for a posteriori log analysis. *ACM International Conference Proceeding Series*. Published. https://doi.org/10.1145/3339252.3340104
11. Dernaika, F., Cuppens-Boulahia, N., Cuppens, F., & Raynaud, O. (2021). A Posteriori Analysis of Policy Temporal Compliance. *Risks and Security of Internet and Systems: 15th International Conference, CRiSIS 2020, Paris, France, November 4–6, 2020, Revised Selected Papers 15*, 133–148.
12. Dernaika, F., Cuppens-Boulahia, N., Cuppens, F., & Raynaud, O. (2020). Accountability in the A Posteriori Access Control: A Requirement and a Mechanism. *International Conference on the Quality of Information and Communications Technology*, 332–342.
13. Kabil, A., Duval, T., & Cuppens, N. (2020a). Alert characterization by non-expert users in a cybersecurity virtual environment: A usability study. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12242 LNCS*, 82–101. https://doi.org/10.1007/978-3-030-58465-8_6
14. Kabil, A., Duval, T., Cuppens, N., Comte, G. L., Halgand, Y., & Ponchel, C. (2019a). Why should we use 3D Collaborative Virtual Environments for Cyber Security? *2018 IEEE 4th VR International Workshop on 3D Collaborative Virtual Environments, 3DCVE 2018*, 3–5. https://doi.org/10.1109/3DCVE.2018.8637109
15. Kabil, A., Duval, T., & Pahl, M.-O. (2021). *Training and Data Analysis use cases for Cybersecurity through Mixed Reality Applications*. VR4Sec: 1st International Workshop on Security for XR and XR for Security.
16. Khan, I., & xavier François-Aubet. (2019). *Deep Learning-aided Resource Orchestration for Vehicular Safety Communication C-ITS Decentralized Congestion Control (DCC)*. *April*.
17. Lubben, C., Pahl, M. O., & Khan, M. I. (2020). Using Deep Learning to Replace Domain Knowledge. *Proceedings - IEEE Symposium on Computers and Communications*, *2020-July*. https://doi.org/10.1109/ISCC50000.2020.9219567
18. Moussaileb, R., Cuppens, N., Lanet, J. L., & Le Bouder, H. (2020). Ransomware Network Traffic Analysis for Pre-encryption Alert. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12056 LNCS*, 20–38. https://doi.org/10.1007/978-3-030-45371-8_2
19. Moussaileb, R., Navas, R. E., Cuppens, N., Moussaileb, R., Navas, R. E., Cuppens, N., Moussaileb, R., Navas, R. E., & Cuppens, N. (2021). *Watch out ! Doxware on the way \ldots To cite this version : HAL Id : hal-03132748 Watch Out ! Doxware on The Way ...* Published.

20. Mühlbauer, N., Kirdan, E., Pahl, M. O., & Carle, G. (2020). Open-Source OPC UA Security and Scalability. *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, *2020-Septe*, 262–269. https://doi.org/10.1109/ETFA46521.2020.9212091
21. Mühlbauer, N., Kirdan, E., Pahl, M.-O., & Waedt, K. (2021). Feature-based Comparison of Open Source OPC-UA Implementations. *INFORMATIK 2020*. Published.
22. Navas, R. E., Cuppens, F., Boulahia Cuppens, N., Toutain, L., & Papadopoulos, G. Z. (2021). MTD, Where Art Thou? A Systematic Review of Moving Target Defense Techniques for IoT. *IEEE Internet of Things Journal*, *8*(10), 7818–7832. https://doi.org/10.1109/JIOT.2020.3040358
23. Navas, R. E., Cuppens, F., Cuppens, N. B., Toutain, L., & Papadopoulos, G. Z. (2021). Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming. *Computer Networks*, *187*, 107751.
24. Navas, R. E., Sandaker, H., Cuppens, F., Cuppens, N., Toutain, L., & Papadopoulos, G. Z. (2020). IANVS: A Moving Target Defense Framework for a Resilient Internet of Things. *Proceedings - IEEE Symposium on Computers and Communications*, *2020-July*. https://doi.org/10.1109/ISCC50000.2020.9219728
25. Pahl, M. O., & Donini, L. (2019). Giving IoT services an identity and changeable attributes. *2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019*, *section II*, 455–461.
26. Pahl, M. O., Liebald, S., & Wustrich, L. (2019). Machine-learning based IoT data caching. *2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019*, 9–12.
27. Pahl, M.-O. (2020, January 1). iLab@ Home: Hands-On Networking Classes without Lab Access. *Sigcomm 2020 Education*. Published.
28. Pahl, M.-O. (2019). Multi-Tenant IoT Service Management towards an IoT App Economy. *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 1–4.
29. Pahl, M.-O., Bauer, F., & Lüubben, C. (2021). Pipeline for Crowdsourced IoT Data-Modeling with AI-Supported Convergence. *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 702–706.
30. Pahl, M.-O., Kabil, A., Bourget, E., Gay, M., & Brun, P.-E. (2020). A Mixed-Interaction Critical Infrastructure Honeypot. *European Cyber Week CAESAR, 2020, Rennes, France*. Published.
31. Pahl, M.-O., & Liebald, S. (2019). Information-Centric IoT Middleware Overlay: VSL. *International Conference on Networked Systems 2019 (NetSys)*. Published. https://s2labs.org/download/publications/2019-03_NetSys_Designing_a_Data-Centric_Internet_of_Things.pdf%0Ahttps://www.netsys2019.org/proceedings/
32. Pahl, M.-O., Liebald, S., & Lübben, C. (2019). VSL: A Data-Centric Internet of Things Overlay. *International Conference on Networked Systems 2019 (NetSys)*, 1–3. https://s2labs.org/download/publications/2019-03_NetSys_Demo_VSL.pdf%0Ahttps://www.netsys2019.org/proceedings/
33. Paiho, S., Kiljander, J., Sarala, R., Siikavirta, H., Kilkki, O., Bajpai, A., Duchon, M., Pahl, M.-O., Wüstrich, L., Lübben, C., & others. (2021). Towards cross-commodity energy-sharing communities–A review of the market, regulatory, and technical situation. *Renewable and Sustainable Energy Reviews*, *151*, 111568.
34. Pays, B., Loire, D. E. L. A., Atlantique, I. M. T., & N, C. O. É. D. (2020). *T HÈSE Thomas C LÉDEL Cyber-résilience des infrastructures critiques Analyse préventive des défaillances d ' origine malveillante*. Published.
35. Piccoli, A, Pahl, M. O., & Wüstrich, L. (2020). Group Key Management in constrained IoT Settings. *Proceedings - IEEE Symposium on Computers and Communications*, *2020-July*. https://doi.org/10.1109/ISCC50000.2020.9219619
36. Piccoli, Alessandro, Pahl, M.-O., Fries, S., & Sel, T. (2020, January 1). Ensuring Consistency for Asynchronous Group-Key Management in the Industrial IoT. *International Conference on Network and Service Management (CNSM 2020)(CNSM 2020), Izmir, Turkey*. Published.
37. Segovia, M., Cavalli, A. R., Cuppens, N., Rubio-Hernan, J., & Garcia-Alfaro, J. (2020). Reflective attenuation of cyber-physical attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11980 LNCS*, 19–34. https://doi.org/10.1007/978-3-030-42048-2_2
38. Smine, M., Espes, D., Cuppens-Boulahia, N., & Cuppens, F. (2020). Network functions virtualization access control as a service. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12122 LNCS*(1), 100–117. https://doi.org/10.1007/978-3-030-49669-2_6

39. Smine, M., Espes, D., Cuppens-Boulahia, N., Cuppens, F., & Pahl, M.-O. (2021). A Priority-Based Domain Type Enforcement for Exception Management. *Foundations and Practice of Security: 13th International Symposium, FPS 2020, Montreal, QC, Canada, December 1–3, 2020, Revised Selected Papers*, *12637*, 65.
40. Wuestrich, L., Schröder, L., & Pahl, M.-O. (2021, May 1). Cyber-Physical Anomaly Detection for ICS. *IFIP/IEEE International Symposium on Integrated Network Management Co-Located with IM*. Published. http://xxxxx/213227.pdf
41. Wüstrich, L., Pahl, M. O., & Liebald, S. (2020a). Towards an Extensible IoT Security Taxonomy. *Proceedings - IEEE Symposium on Computers and Communications*, *2020-July*, 11–16. https://doi.org/10.1109/ISCC50000.2020.9219584
42. Wüstrich, L., Pahl, M.-O., & Liebald, S. (2020b, January 1). An extensible IoT Security Taxonomy. *IEEE ISCC 2020*. Published.