# Offre de stage en laboratoire entre mars et août 2023

# Auto-protection des systèmes par une approche blockchain : application à l'exfiltration de données

## Contexte

Les avancées technologiques permettent aujourd'hui aux utilisateurs d'être connectés partout et à tout moment. Ceci contribue à l'augmentation des menaces et attaques auxquelles font face les systèmes connectés : intrusion, vol de données, déni de service, etc. Pour résister à ces attaques, certains services de sécurité doivent être mis en place par le biais de divers protocoles et techniques comme la sécurité des communications et des accès ou encore la détection d'intrusion. Néanmoins, étant donné la complexité des systèmes supervisés et la nécessité de réagir de manière précise et rapide aux évènements anormaux détectés, la gestion opérationnelle de la sécurité n'est plus compatible avec l'intervention d'un opérateur humain et il apparaît nécessaire de développer des approches autonomes permettant une mise en œuvre automatique et dynamique des mécanismes de sécurité les plus adaptés [Hammad 18] ou de détecter en temps réel les attaques et répondre automatiquement à ces dernières [Zuk 22].

## Objectif

Un système d'autoprotection met en œuvre des entités de supervision autonomes capables d'assurer la sécurité des équipements et des ressources sur la base des données remontées par ces derniers. Toutefois, en tant que système distribué à part entière, il peut lui-même être la cible d'attaques, nécessitant d'être lui-même fondé sur des composants et communications sécurisés. Dans ce contexte, la technologie de blockchain, qui assure en outre le support du facteur d'échelle par la décentralisation de ses traitements et un accès temps réel et contrôlé aux données nécessaires, apparaît comme un substrat prometteur pour la conception d'architectures d'auto-protection. L'état de l'art a notamment montré que grâce aux contrats intelligents, la blockchain permet d'automatiser la mise en place de contre-mesures adéquates à des attaques de déni de service distribuées en permettant par exemple à plusieurs systèmes de partager et mettre à jour une liste de sources de menaces [Rodrigues 17] [Sagirlar 18] [Singh 19] [Abou El Houda 19].

## Travail à réaliser

Dans le cadre de ce stage, nous nous intéresserons à d'autres formes d'attaques, plus difficiles à détecter et stopper, telles que les attaques d'exfiltration de données exploitant le protocole DNS comme support à la tunnelisation [Nadler 19].

L'objectif sera de construire une première solution de sécurité autonome capable de détecter et stopper les attaques par exfiltration sur les flux DNS dans des grands systèmes.

Dans ce contexte, le travail demandé sera organisé comme suit :

- Etat de l'art sur les systèmes d'autoprotection, la technologie de blockchain et, entre autres, des attaques d'exfiltration de données avec DNS ;
- Sur la base de l'état de l'art, identification d'une approche de détection et de contre-mesures qui repose sur les contrats intelligents ;
- Implémentation et évaluation de la proposition dans un environnement Ethereum (réseau Ropsten) ou Hyperledger Fabric afin d'évaluer l'efficacité et les performances de la proposition.

### Compétences nécessaires

Le stage vise des candidatures de niveau M2 ou équivalent, comme la dernière année d'école d'ingénieurs. Des compétences générales en système, réseaux et sécurité sont attendues. Des connaissances sur la blockchain et/ou sur les attaques visant à exfiltrer des données seraient un plus appréciées.

### Conditions du stage

Le stage se déroule à l'IUT de Lannion (département Réseaux et Télécommunications) au sein de l'équipe SOTERN de l'IRISA. Le stagiaire aura accès à la plateforme du laboratoire et aux ressources nécessaires pour le travail (poste de travail, ressources bibliographiques, etc.).

La rémunération de stage se situe autour de 530€ par mois.

### Références


[Abou El Houda 19] Z. Abou El Houda, A. S. Hafid and L. Khoukhi, "Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract," in *IEEE Access*, vol. 7, pp. 98893-98907, 2019, doi: 10.1109/ACCESS.2019.2930715.

[Hammad 18] M. Hammad, J. Garcia and S. Malek, "Self-Protection of Android Systems from Inter-component Communication Attacks," 2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE), 2018, pp. 726-737, doi: 10.1145/3238147.3238207.

[Nadler 19] A. Nadler, A. Aminov, A. Shabtai. "Detection of malicious and low throughput data exfiltration over the DNS protocol", Computers & Security, Volume 80, 2019, Pages 36-53, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2018.09.006.

[Rodrigues 17] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," Lecture Notes in Computer Science, Vol. 10356 LNCS, pp. 16-29. Springer Verlag, 7 2017.

[Sagirlar 18] G. Sagirlar, B. Carminati and E. Ferrari, "AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things," 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), 2018, pp. 1-8, doi: 10.1109/CIC.2018.00-46.

[Singh 19] R. Singh, S. Tanwar, T.P. Sharma, "Utilization of blockchain for mitigating the distributed denial of service attacks," Security and privacy, Volume3, Issue3, Wiley, May/June 2020, https://doi.org/10.1002/spy2.96

[Zuk 22] Nir Zuk, Extended Security Intelligence and Automation Management, Palo Alto Networks, February 2022,
https://www.paloaltonetworks.com/blog/2022/02/extended-security-intelligence-and-automation-management/


## Encadrants


Mohamed Aymen Chalouf (mohamed-aymen.chalouf@irisa.fr)
Université Rennes 1, SOTERN-IRISA

Romaric Ludinard (romaric.ludinard@imt-atlantique.fr)
IMT Atlantique, SOTERN-IRISA

Guillaume Doyen (guillaume.doyen@irisa.fr)
IMT Atlantique, SOTERN-IRISA