Université de Rennes

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2024

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : Matisse **POLE DE RECHERCHE : Mathématique-Numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA

Equipe : SOTERN

Encadrement

Directeur de thèse : Mohamed-Aymen CHALOUF **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes (IUT Lannion)

HDR : □* oui □ non **Nb de thèses en cours** : 0

Mail : mohamed-aymen.chalouf@irisa.fr **Tél**. : 02 96 46 93 12

Co-directeur de thèse : Guillaume DOYEN **Unité de recherche** : IRISA

Employeur/Établissement d'origine : IMT Atlantique

HDR : □* oui □ non **Nb de thèses en cours** : 5

Mail : guillaume.doyen@irisa.fr **Tél.** : 0299127906

Co-encadrant de thèse : Pierre ALAIN **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes (IUT Lannion)

HDR : □ oui □* non **Nb de thèses en cours** : 0

Mail : pierre.alain@irisa.fr **Tél**. : 02 96 46 91 54

Sujet

Titre : Vers une auto-protection robuste, fiable et performante des systèmes connectés : une approche basée sur la blockchain et les microservices

Mots clés : Auto-protection, blockchain, microservices

Cotutelle internationale (oui/non) : Non **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif :

Contexte :

Les avancées technologiques permettent aujourd'hui aux utilisateurs d'être connectés partout et à tout moment. Ceci contribue à l'augmentation de la surface d'attaque à laquelle font face les systèmes connectés : intrusion, vol de données, déni de service, etc. Afin de 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 attaques, la gestion de la sécurité n'est plus compatible avec l'intervention d'un opérateur humain et il apparaît nécessaire de développer des approches autonomes permettant de détecter en temps réel les attaques et répondre automatiquement à ces dernières [1]. Dans un système d'auto-protection, la sécurité des équipements et des ressources est assurée par des entités de supervision sur la base des données remontées par les différents équipements. Deux approches sont possibles, d'une part la gestion de cette sécurité peut être confiée à une entité centrale avec un risque sur la compromission de cette entité le support du facteur d'échelle de cette solution. D'autre part, il est possible de répartir la gestion de la sécurité entre plusieurs nœuds avec l'utilisation d'une blockchain [2]. Ce type de système distribué peut cependant présenter des temps de réactions trop importants nécessitant de nouvelles solutions adaptées à ce cas d'usage particulier qu'est la réaction aux attaques.

État de l'art :

La technologie de blockchain est aujourd'hui utilisée dans la sécurisation de différents domaines et applications comme l'Internet des objets, le stockage des données de santé et la gestion des identités numériques [3]. La blockchain permet de stocker des données mais aussi du code sous forme de contrats intelligents (smart contracts) qui peuvent être exécutés par les

nœuds participant à la blockchain à la demande d'un client. Ainsi, les smarts contracts ont permis, entre autres, de décentraliser certains mécanismes de sécurité comme la gestion des identités [4], la gestion des certificats [5], le contrôle d'accès [6] et la détection d'intrusion [7]. Cette utilisation présente des avantages importants comme la suppression de point de défaillance unique (single point of failure), la baisse de l'exigence de la confiance que le client doit avoir dans les nœuds exécutant le code du contrat ou encore la garantie de l'inaltérabilité des données stockées dans les blocs. Une architecture d'auto-protection basée sur la blockchain permettrait donc un partage sécurisé des différentes données nécessaires à la détection des attaques, une traçabilité des différentes actions et une réaction rapide et automatisée aux attaques grâce aux smarts contracts. L'état de l'art a notamment montré que grâce aux smart contracts, la blockchain permet de sécuriser la gestion des configurations réseau [8] et 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 [9]-[10]. Par ailleurs, les performances des systèmes basés sur la blockchain dépendent principalement des performances de cette dernière et de sa capacité à obtenir un consensus dans un délai raisonnable. Le consensus est obtenu lorsqu'un ensemble de nœuds de la blockchain (entités de supervision de la sécurité dans notre cas) exécutent un smart contract et obtiennent un résultat identique. Ainsi, le temps de réaction d'un système d'auto-protection par blockchain va dépendre du type de consensus utilisé : preuve de travail, preuve d'enjeu, preuve d'autorité, etc. [11]. Pour améliorer les performances des systèmes basés sur la blockchain et des smart contracts, des travaux de recherche récents proposent de faire appel aux microservices pour l'exécution des smart contracts [12], [13]. Selon [14], fonder les traitements des blockchains sur le paradigme des microservices est une évolution naturelle compte tenu de la conception basée sur les microservices de tous les services et infrastructures réseau de nouvelle génération. Dans [15], Santos et al. affirment que l'usage des microservices permettrait de résoudre certains des problèmes de la blockchain comme la scalabilité, l'ordre d'exécution, etc. En effet, les architectures de type "BaaS: Blockchain as a Service" permettent d'exécuter en parallèle les smart contracts et d'obtenir un meilleur temps de réponse et une meilleure scalabilité. Néanmoins, ces performances dépendent fortement des technologies utilisées : virtualisation, conteneurisation, orchestration, etc. Par ailleurs, les unikernels représentent une alternative prometteuse du point de vue des performances [16]. Aussi, les unikernels permettent d'avoir des garanties supplémentaires au niveau de la sécurité d'exécution (isolation du système, gestion des ressources CPU, mémoire, etc.). Par exemple, Alp et al. [17] proposent d'exécuter les smart contracts par des unikernels déployés à l'avance (minimisant ainsi le surcoût lié à la création de la machine virtuelle), à la demande (limitant le gaspillage de ressources lorsque les unikernels ne sont pas utilisés). Néanmoins, les résultats obtenus montrent l'intérêt de l'utilisation des unikernels uniquement au-delà d'un seuil relatif aux nombres d'opérations spécifiques (~1000) ou selon une approche hybride.

Objectifs et principales contributions :

L'objectif principal de cette thèse est de proposer un système robuste, fiable et performant destiné à l'autoprotection des systèmes ouverts et connectés. La sécurité et la fiabilité du système proposé seront assurées grâce à l'utilisation de la blockchain. Ceci induit plusieurs défis liés notamment à la définition des rôles dans un système ouvert connecté et des smarts contracts qui permettront d'assurer l'exécution et le bon enchaînement des réactions aux attaques considérées (déni de service, exfiltration de données [15], etc.) tout en évitant les éventuels conflits entre les actions initiées par différentes entités. Concrètement, ceci permettrait de définir comment le système doit réagir (par exemple, mise à jour des configurations des serveurs et des éléments réseau comme les routeurs et pare-feu). Par ailleurs, les performances du système d'autoprotection basé sur la blockchain (blockchain-based) seront optimisées en exécutant les smart contracts par le biais des microservices. La majorité des travaux portant sur la blockchain et les microservices présentent simplement une preuve de concept [15]. Ainsi, un second défi lié au travail de cette thèse, sera de proposer un environnement réel de blockchain utilisant les microservices. Dans cet environnement, chaque nœud de la blockchain pourra disposer d'une grappe d'unikernels et d'un ordonnanceur dédié qui se chargera de la répartition des tâches (exécution de smart contracts) entre les unikernels disponibles. Il sera donc question de proposer un orchestrateur chargé de la gestion des ressources disponibles au niveau de la grappe d'unikernels dans l'objectif de, non seulement optimiser les performances de la plateforme proposée, mais aussi de gérer les priorités des actions. Ceci revient à définir un algorithme multi-objectifs avec un compromis entre la priorité et les autres critères de performances. Il conviendra également d'évaluer les performances de la solution globale proposée en matière de délai de réponse et de scalabilité. L'ensemble de ce travail permettra de valider les avantages de l'approche proposée en comparaison à d'autres approches de l'état de l'art (centralisée, blockchain-based classique, blockchain-based utilisant les machines virtuelles ou les conteneurs).

Approche méthodologique et qualité des résultats obtenus :

La méthodologie de travail de la thèse repose sur non seulement une approche pratique (développement d'une blockchain dont les smart contracts s'exécutent sur des unikernels) mais aussi une approche théorique (automatisation de la réaction aux attaques en évitant les conflits de configurations et formulation du problème visant à optimiser les performances et la rémunération). Les échéances de travail seront organisées comme suit :

- T0-T0+6 : état de l'art sur les systèmes d'auto-protection, la blockchain et l'usage des microservices et plus particulièrement les unikernels pour la blockchain ;
- T0+6-T0+18 : proposition et implémentation d'un système d'auto-protection (réaction aux attaques et éventuellement détection de ces attaques) en utilisant la blockchain et les smarts contracts ;

● T0+18-T0+26 : définition et implémentation d'un orchestrateur permettant l'exécution des smart contracts par des unikernels. Cet orchestrateur doit tenir compte de plusieurs critères (délais de réponses, rémunération, consommations de ressources, etc.) ;
● T0+26-T0+30 : validation de la solution proposée et évaluation de ses performances (comparaison avec une solution centralisée, une solution blockchain-based classique et des solutions blockchain-based utilisant la virtualisation et la conteneurisation) ;
● T0+30-T0+36 : rédaction du manuscrit de thèse. Les travaux réalisés dans le cadre de cette thèse feront l'objet d'articles qui seront soumis dans des journaux et conférences de renommée internationale dans le domaine de la cybersécurité des réseaux, par exemple "Computers & Security (COSE)" et "IEEE Transactions on Information Forensics and Security".

Références :

[1] 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/
[2] K. Wüst and A. Gervais, "Do you Need a Blockchain?," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 2018, pp. 45-54, doi: 10.1109/CVCBT.2018.00011.
[3] M. Arun Sekar Rajasekaran, Maria Azees, Fadi Al-Turjman, "A comprehensive survey on blockchain technology", Sustainable Energy Technologies and Assessments (Elsevier), Volume 52, Part A, 2022, 102039, ISSN 2213-1388, doi: https://doi.org/10.1016/j.seta.2022.102039.
[4] M. Tcholakian, K. Gorna, M. Laurent, H. Kaffel Ben Ayed, M. Naghmouchi, "Self-Sovereign Identity for Consented and Content-Based Access to Medical Records Using Blockchain", Security and Communication Networks, vol. 2023, Article ID 6025789, 2023. doi: https://doi.org/10.1155/2023/6025789.
[5] L. Mendiboure, M.A. Chalouf, F. Krief, "A scalable blockchain-based approach for authentication and access control in software defined vehicular networks", The 29th International Conference on Computer Communications and Networks, ICCCN 2020, Honolulu, Hawai, USA, August 2020, IEEE, pp. 1-11. doi: 10.1109/ICCCN49398.2020.9209661.
[6] T. Sylla, L. Mendiboure, M.A. Chalouf, F. Krief, "Blockchain-Based Context-Aware Authorisation Management as a Service in IoT", Sensors 21, no. 22, 7656, November 2021.
[7] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," in IEEE Access, vol. 6, pp. 10179-10188, 2018, doi: 10.1109/ACCESS.2018.2799854.
[8] I. D. Alvarenga, G. A. F. Rebello and O. C. M. B. Duarte, "Securing configuration management and migration of virtual network functions using blockchain," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 2018, pp. 1-9, doi: 10.1109/NOMS.2018.8406249.
[9] 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.
[10] 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/spy2.9
[11] Jie Xu, Cong Wang, and Xiaohua Jia. 2023. A survey of blockchain consensus protocols. Comput. Surveys (2023).
[12] E. Bandara, et al., "SaaS - Microservices-Based Scalable Smart Contract Architecture", In: Thampi, S.M., Wang, G., Rawat, D.B., Ko, R., Fan, CI. (eds) Security in Computing and Communications (SSCC 2020), Communications in Computer and Information Science, vol 1364, 2021, Springer, Singapore, https://doi.org/10.1007/978-981-16-0422-5_16
[13] S. Wang, X. Zhang, W. Yu, K. Hu and J. Zhu, "Smart Contract Microservitization", 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020, pp. 1569-1574, doi: 10.1109/COMPSAC48688.2020.00-31.
[14] D. Krishnaswamy et al., "A Microservices-Based Virtualized Blockchain Framework for Emerging 5G Data Networks", 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GCWkshps45667.2019.9024409.
[15] R. Santos, P. Soares, E. Rodrigues, P.H.M. Maia, A. Silveira, "How blockchain and microservices are being used together: a systematic mapping study", WETSEB '22: Proceedings of the 5th International Workshop on Emerging Trends in Software Engineering for BlockchainMay 2022, pp. 39–46, doi: https://doi.org/10.1145/3528226.3528371
[16] T. Goethals, M. Sebrechts, A. Atrey, et al., " Unikernels vs containers: An in-depth benchmarking study in the context of microservice applications", In : 2018 IEEE 8th International Symposium on cloud and service computing (SC2). IEEE, 2018. p. 1-8.
[17] E.C. Alp, C. Băsescu, P. Tennage, N. Kocher, G. Bosson, and B. Ford, "Efficient Deterministic Execution of Smart Contracts", in EPFL 2022. Online: http://infoscience.epfl.ch/record/292907