IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Inria

Automatisation de la réaction aux attaques :
Spécification des objectifs et mise en œuvre dynamique sur des réseaux programmables

Thèse : co-direction RESIST (INRIA Nancy Grand Est) – IMT-Atlantique (IRISA)
Jérome François, Fabien Autrel, Ahmed Bouabdallah, Guillaume Doyen

Contexte

L'évolution des réseaux et services tend toujours vers davantage de complexité, de rapidité tout en devant supporter des facteurs d'échelle toujours plus importants. Dans ce contexte, définir, mettre en œuvre et s'assurer de la conformité des fonctions de sécurité s'avère être une tâche toujours plus difficile et l'automatisation des fonctions de sécurité, et en particulier de la réaction aux attaques, s'avère être un challenge important pour les futures générations de réseaux et services (5G et 6G, Internet à très faible latence, réseaux industriels, bâtiments connectés, etc.). Dans ce contexte, la virtualisation des réseaux et l'usage massif de micro-services sont deux leviers technologiques qui doivent permettre de décomposer et recomposer les fonctions de sécurité à grain très fin. Cependant, le problème de la supervision et l'automatisation reste entier et est même exacerbé par la flexibilité fournie.

Le paradigme de réseau basé sur l'intention, « Intent-Based Networking » (IBN) [1] apporte une réponse possible à cette question. Ce paradigme permet aux opérateurs d'exprimer des objectifs de performance ou de sécurité de haut niveau et intelligibles (jusqu'à être exprimés en langage naturel) sans spécifier les moyens de les réaliser et ainsi laisser les composants de gestion effectuer leur mise en application sur les éléments gérés (équipements, services, applications).

Verrous scientifiques

Appliqué à la sécurité, le paradigme IBN apparaît comme prometteur, mais soulève de nombreuses questions de recherche qu'il est question d'explorer ici :

(1) comment traduire des objectifs exprimés, possiblement en langage naturel, dans un formalisme appréhendable par un système supervisé ? Il sera pour cela nécessaire de proposer dans un premier temps une sémantique formelle du langage d'expression des intentions et d'introduire une notion de raffinement de spécifications constituées d'intentions. Cela fournira l'ossature d'une méthodologie de déploiement correct par construction de politiques basées sur les intentions, par raffinement successifs de spécifications : à partir d'un ensemble d'intentions initiales les raffinements successifs conduisent à une politique concrète déployable directement sur les différents équipements de l'architecture ciblée ;

(2) comment vérifier formellement que la politique de sécurité déployée est bien conforme aux objectifs (*intents*) exprimés par l'opérateur ? En ayant défini préalablement la correction d'un raffinement d'intentions, il s'agira alors de montrer que chaque raffinement impliqué dans la chaîne ayant permis de transformer les intentions initiales en une politique concrète, est correct.

(3) garantir le bon fonctionnement de la politique de sécurité en s'assurant que les mécanismes déployés conservent à chaque instant et quels que soient les aléas induits par l'évolution du système les objectifs exprimés par l'administrateur. Parmi les exigences de sécurité spécifiées par l'administrateur qui constituent la politique de sécurité globale du système, la politique de réaction aux intrusions spécifie comment le système doit réagir face à une menace avérée car détectée. La détection d'une intrusion conduit à une mise à jour de la politique concrète et il est nécessaire d'une

part de vérifier que cette mise à jour respecte les objectifs (*intents*) du système et d'autre part la correction du déploiement de la mise à jour. Le levier mobilisé pour la mise en œuvre concrète de la politique de réaction aux intrusions exploitera pleinement les évolutions récentes de la programmabilité des équipements réseaux. En effet, l'utilisation de plan de données programmables dans les switchs réseaux permet en effet de délocaliser dans le réseau des traitements partiels des fonctions de sécurité alors que le traitement complexe de données peut être accompli par des micro-services de sécurité déployables à la volée. Ainsi, l'ensemble d'un réseau peut aussi être vu comme une ressource unique servant à détecter et contrer des attaques. Cela suppose toutefois la capacité à programmer ce dernier de manière unique, des mécanismes de distribution du processus/fonctions de sécurité et des protocoles de synchronisation. En particulier, les micro-services formeront un réseau d'overlay déployé dynamiquement et seront synchronisé via un réseau programmable. Cela permettra de définir des mécanismes de synchronisation opportunistes évitant de surcharger le réseau avec des messages de signalisation à part entière (dans un flux dédié). Plus précisément, ce mécanisme de synchronisation déterminera les paquets d'autres flux pour encapsuler l'information de synchronisation tout en ne considérant qu'une vue limitée (prochain saut) et non une vue globale, qui ne serait pas réaliste. D'un point de vue protocolaire, il sera proposé d'étendre les informations échangées par la télémétrie in-band. Plusieurs questions sont alors soulevées : quels messages sélectionner ? Doit-on changer ou non le routage éventuel de ces messages ? Doit-on dupliquer et forcer l'envoi du message sur plusieurs interfaces ? Quel taux de non transmission est acceptable par rapport à la performance du système de détection ou de réaction ? En supposant à l'avance le modèle de trafic, quelle performance de synchronisation est atteignable ?

Objectif

L'objectif général de cette thèse est de concevoir et développer une architecture globale de réponse aux attaques réseau qui permette d'exprimer des objectifs de sécurité à atteindre et maintenir, traduire ces objectifs en règles formant une politique de sécurité, tout en s'assurant de leur conformité, et enfin les déployer et les orchestrer par le biais d'une synchronisation opportuniste dans un environnement technologique hétérogène programmable et virtualisé.

Références

1. A. Clemm, L.Ciavaglia, L.Z. Granville and J.Tantsura. Intent-Based Networking - Concepts and Definitions. Internet-Draft. Internet Engineering Task Force. Dec. 2021.
2. J. P. Jeong, P. Lingga, J. Yang, and J. Kim, "Guidelines for Security Policy Translation in Interface to Network Security Functions," Internet Engineering Task Force, Internet-Draft draft-yang-i2nsf-security-policy- translation-11, Apr. 2022, work in Progress. [Online]. Available: https:// datatracker.ietf.org/doc/draft- yang- i2nsf- security- policy- translation/11/
3. G. Liu, W. Pei, Y. Tian, C. Liu, and S. Li, "A novel conflict detection method for ABAC security policies," Journal of Industrial Information Integration, vol. 22, p. 100200, 2021.
4. G.-J. Ahn and R. Sandhu, "The RSL99 language for role-based separa- tion of duty constraints," in Proceedings of the fourth ACM workshop on Role-based access control, 1999, pp. 43–54.
5. M. F. Hyder and M. A. Ismail, "INMTD: Intent-based moving target defense framework using software defined networks," Engineering, Technology & Applied Science Research, vol. 10, no. 1, pp. 5142–5147, 2020.
6. T. Szyrkowiec, M. Santuari, M. Chamania, D. Siracusa, A. Autenrieth, V. Lopez, J. Cho, and W. Kellerer, "Automatic intent-based secure service creation through a multilayer sdn network orchestration," Journal of Optical Communications and Networking, vol. 10, no. 4, pp. 289–297, 2018.
7. Bringhenti, D., Marchetto, G., Sisto, R., Spinoso, S., Valenza, F., & Yusupov, J. (2020). Improving the formal verification of reachability policies in virtualized networks. IEEE Transactions on Network and Service Management, 18(1), 713-728.

8. Bringhenti, D., Sisto, R., & Valenza, F. (2023). A novel abstraction for security configuration in virtual networks. Computer Networks, 228, 109745.
9. Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., ... & Walker, D. (2014). P4: Programming protocol-independent packet processors. ACM SIGCOMM Computer Communication Review, 44(3), 87-95.
10. Lu, D., Huang, D., Walenstein, A., & Medhi, D. (2017). A secure microservice framework for iot. 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), 9–18.
11. Zhang, N., Li, H., Hu, H., & Park, Y. (2017). Towards effective virtualization of intrusion detection systems. Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, 47–50.