Nom – Prénom	BADONNEL Rémi
Laboratoire de rattachement	LORIA
Intitulé du diplôme HDR	INFORMATIQUE
Titre de l'HDR	Anglais : Managing Security for the Cyber-Space : From Smart Monitoring to Automated Configuration Français : Gestion de la Sécurité pour le Cyber-Espace : du Monitorage Intelligent à la Configuration Automatique

Abstract (français) – maximum 15 lignes

L'Internet est devenu une formidable plateforme d'intégration capable d'interconnecter efficacement des milliards d'entités, de simples capteurs à de grands centres de données. Cette plateforme fournit un accès à de multiples ressources (telles que machines virtuelles et objets connectés), à partir desquelles il est possible de construire et d'opérer des systèmes complexes et à valeur ajoutée. Ces systèmes sont cependant exposés à une grande variété d'attaques. Dans ce contexte, l'objectif de mes travaux de recherche porte sur une meilleure gestion de la sécurité pour le cyber-espace, à travers l'élaboration de nouvelles solutions de monitorage et de configuration pour ces systèmes. Un premier axe de ce travail se focalise sur l'investigation de méthodes de monitorage capables de répondre aux exigences de réseaux à faibles ressources. Un second axe porte sur l'amélioration de la détection et du traitement des vulnérabilités, qui peuvent survenir lorsque des changements sont réalisés sur la configuration de tels systèmes. Un troisième axe concerne la configuration automatique de ressources virtuelles pour la gestion de la sécurité. En particulier, nous proposons une approche de programmabilité de la sécurité pour les infrastructures cloud, et introduisons des techniques de construction automatique et de vérification de chaînes de sécurité pour les réseaux logiciels. Enfin, plusieurs perspectives de recherche relatives à la sécurité autonome sont mises en évidence concernant l'usage de méthodes ensemblistes, la composition de services, et la vérification de techniques d'intelligence artificielle.

Abstract (anglais) – maximum 15 lignes (pas obligatoire)

The Internet has become a great integration platform capable of efficiently interconnecting billions of entities, from simple sensors to large datacenters. This platform provides access to multiple resources (such as virtual machines and connected objects), from which the building and operation of complex and value-added networked systems is enabled. These systems are however exposed to a large variety of security attacks that are also gaining in sophistication and coordination. In that context, the objective of my research work is to support security management for the cyber-space, with the elaboration of new monitoring and configuration solutions for these systems. A first axis of this work focuses on designing smart monitoring methods to cope with low-resource networks. A second axis aims at improving the assessment and remediation of vulnerabilities that may occur when changes are performed on system configurations. A third axis is centered on automating the configuration of virtualized resources to support security management. In particular, we propose a software-defined security approach for configuring cloud infrastructures, and we introduce automated building and verification techniques for facilitating the orchestration of security chains in software-defined networks. Finally, several research perspectives on security automation are pointed out with respect to ensemble methods, composite services and verified artificial intelligence.