Université de Bretagne Occidentale

Ecole Doctorale

HABILITATION A DIRIGER DES RECHERCHES

Avis de soutenance

Monsieur ESPES DAVID

présentera ses travaux en vue de l'habilitation à diriger des recherches, sur le sujet suivant :

"Cybersécurité de l'industrie du Futur: vers une industrie plus résiliente"

Le mardi 29 juin 2021 à 14h

à l'UFR Sciences et Techniques - salle J009.

Le jury sera ainsi composé :

- M. BOUABDALLAH ABDELMADJID, Professeur des universités
UTC - COMPIEGNE
- M. CUPPENS FREDERIC, Professeur
IMT Atlantique - CESSON-SEVIGNE
- MME CUPPENS NORA, Professeure
IMT Atlantique - CESSON-SEVIGNE
- M. FESTOR OLIVIER, Professeur des universités
Université de Lorraine - VILLERS-LES-NANCY
- M. LE PARC PHILIPPE, Professeur des universités
Univ. de Bretagne Occidentale - BREST
- M. NANA TCHAMNDA LAURENT, Professeur des universités
Univ. de Bretagne Occidentale - BREST
- M. PUJOLLE GUY, Professeur des universités
Univ Paris VI - PARIS 15EME
- M. URIEN PASCAL, Professeur
Télécom Paris - PALAISEAU

A BREST, le 14 juin 2021
Le Président de l'Université de Bretagne Occidentale,

UNIVERSITE DE BRETAGNE OCCIDENTALE

M. GALLOU

DOCTORAT BRETAGNE LOIRE / MATHSTIC

Habilitation à Diriger des Recherches

Cybersécurité de l'Industrie du Futur : vers une industrie plus résiliente

David Espes

Résumé :

Grâce à l'utilisation de nouvelles technologies comme le Cloud, l'Internet des Objets Industriels, la convergence entre les technologies d'information et d'opération, l'industrie est en train de connaître une importante digitalisation qui bouleverse son fonctionnement.

Bien que cette digitalisation améliore sensiblement l'efficacité et la compétitivité de ces industries, elle accroît significativement leur surface d'attaque. La cybersécurité est devenue essentielle pour une industrie et doit prendre en compte l'intégration de ces nouvelles technologies.

Mes travaux de recherche adaptent et conçoivent des mécanismes de sécurité qui répondent à deux des quatres piliers d'une industrie du futur : 1) la convergence des technologies d'information et d'opération et 2) l'automatisation du cycle de vie des produits.

Pour sécuriser les technologies utilisées dans ces deux piliers, mes travaux ont porté sur trois thématiques :

1) La segmentation automatique des architectures réseaux d'une industrie : Pour simplifier la segmentation des systèmes, nous avons proposé une méthode de segmentation itérative qui regroupe les composants d'une industrie du futur dans une même zone en fonction de caractéristiques communes. Ces caractéristiques concernent le site sur lequel se situe le composant, le niveau fonctionnel (tel que défini par l'ISA 95) auquel il appartient, son processus métier, son risque de sécurité, son positionnement géographique dans l'atelier et enfin ses spécificités techniques. Une telle méthode automatise le processus de segmentation en limitant la charge opérationnelle de l'opérateur qui l'effectue.
2) La détection d'intrusion par anomalie : mes travaux ont porté sur la conception d'un système de détection d'intrusion à analyse comportementale. Deux objectifs particuliers ont été étudiés : concevoir spécifiquement un système de détection d'intrusion pour détecter les attaques complexes et persistantes (c. à-d., les attaques à signaux faibles) et réduire les faux-positifs retournés par ces dispositifs.
3) La gestion des politiques de contrôle de flux et leur déploiement : Mes travaux proposent des méthodes pour définir automatiquement la politique de contrôle de flux entre verticaux utilisés par l'industrie et à l'intérieur de chacun de ces verticaux (c'est-à-dire entre ressources virtualisées VNF qui composent ces verticaux). Le déploiement de ces règles de contrôle de flux est réalisé grâce à la conception d'un pare-feu à états qui respecte la philosophie SDN, c'est-à-dire qui sépare le plan de contrôle du plan de données. Ce pare-feu SDN, le premier de son genre, assure un contrôle de flux au plus près des utilisateurs et résout les contraintes imposées par la sécurité périmétrique en contrôlant les flux non seulement en périphérie mais également à l'intérieur de chaque zone du système.

Mes travaux ont principalement concerné la protection des infrastructures d'une industrie du futur et la détection des attaques qu'elle pouvait être l'objet. Dans un avenir proche, je souhaite orienter mes travaux sur la réponse à apporter en cas de cyber-attaque dans le but d'assurer une continuité dans le fonctionnement de ces systèmes. Cette réponse dynamique à une adversité, qui s'est produite malgré toutes les contremesures mises en place pour l'éviter, soulève de nouveaux challenges comme la prise en compte de l'interdépendance entre la sûreté de fonctionnement et la cybersécurité.