



Move securely within the cyberworld


**itrust consulting s.à r.l.**

55, rue Gabriel Lippmann

L-6947 Niederanven

 Carlo Harpes – Managing Director

 +352 621 451 945

 info@itrust.lu

Niederanven, 28 June 2018

### **Steve Muller d'itrust consulting se voit décerner un doctorat avec mention 'Excellent' pour son travail sur le monitoring des risques et la détection d'intrusion pour les systèmes de contrôle industriel**

Le 26 juin, Steve Muller d'itrust consulting a soutenu sa thèse de doctorat en informatique sur le monitoring des risques et la détection d'intrusion pour les Systèmes de Contrôle Industriel (SCI) à l'Université du Luxembourg.

Steve a présenté une description complète de nouvelles techniques et algorithmes de gestion des risques pour surveiller le risque d'une organisation en temps réel, y compris un système de détection d'intrusion appliqué aux SCI. Il a découvert un algorithme efficace (en temps polynomial) pour calculer les probabilités d'attaques dans des graphes de dépendance arbitrairement complexes. Cela permet de calculer la probabilité de scénarios de risque interdépendants, en tenant compte de la probabilité qu'un scénario soit la conséquence d'un autre.

Il a également optimisé considérablement le temps de calcul des algorithmes par séparation et évaluation existants qui trouvent l'ensemble optimal de contre-mesures – en termes de retour sur investissement en sécurité (ROSI) - dans les arbres d'attaque et de défense. De tels arbres permettent aux évaluateurs du risque d'estimer le risque actuel dans un contexte où les contre-mesures sont mises en œuvre avec des performances variables, et constituent donc une approche complémentaire aux graphes de dépendance.

Pour traduire les alertes provenant de systèmes de détection d'intrusion et d'agents similaires en notions de risque, Steve les a décrites comme une série temporelle basée sur des fonctions exponentielles. Ainsi, seules l'amplitude et la demi-vie estimées doivent être transmises à la plateforme de surveillance. Il a conçu et développé une interface (API) qui agrège le risque d'alertes multiples. Après avoir remplacé les paramètres statiques du graphe de dépendance par les facteurs de risque dynamiques obtenus à partir des différentes alertes, il peut prédire le niveau de risque actuel et futur, tant dans la configuration actuelle que dans une situation simulée avec de nouvelles contre-mesures en place. Ses algorithmes peuvent alors guider l'opérateur d'un système de contrôle industriel à travers l'activation de contre-mesures appropriées lorsque des alertes se produisent.

Dans une implémentation prototype, il a remplacé les valeurs statiques de l'outil d'évaluation des risques 'TRICK Service' par des formules qui impliquent les paramètres de risque remontés à l'API en temps réel, transformant ainsi l'évaluation statique en un outil de surveillance en temps réel appelé 'TRICK Cockpit'.

Dans la partie finale de sa thèse, Steve a étudié comment des paramètres de risque peuvent être extraits d'outils de sécurité, tels que les systèmes de détection d'intrusion (où il a utilisé la détection d'anomalies, qui est complémentaire aux techniques basées sur les signatures), les analyseurs syntaxiques de logs pare-feu et les outils de gestion de correctifs.

Yves Le Traon, directeur de thèse: « Le comité confère à Steve le grade de 'Docteur' avec la mention la plus élevée possible 'Excellent' pour sa capacité à trouver des solutions nouvelles et efficaces face aux défis. »

Carlo Harpes, Gérant d'itrust consulting: « Steve Muller a développé des techniques de gestion des risques qui, bien que pouvant être utilisées indépendamment dans n'importe quelle méthodologie de gestion des risques, ont été intégrées dans l'outil TRICK Service d'itrust consulting, pavant ainsi le chemin vers TRICK Cockpit, un outil de suivi des risques en temps réel. Elles ont déjà été appliquées au bénéfice de nos clients actuels, tels que Luxmetering, et amélioreront la qualité des estimations des activités futures d'évaluation et de surveillance des risques, non seulement pour les SCI, mais aussi pour tous les systèmes TIC (Technologie de l'Information et de la Communication) complexes. »

Ces travaux ont été financés par une allocation de recherche AFR du Fonds National de Recherche luxembourgeois FNR. L'hébergement et la gestion ont été assurés par itrust consulting dans le cadre d'un partenariat public-privé avec Uni.lu et IMT Atlantique Bretagne-Pays de la Loire en France. Cette gestion et ce soutien ont été cofinancés par le projet de recherche national SGL Cockpit, le projet TRESPASS sur la gestion des risques et les arbres d'attaque et de défense financé par l'UE, et le projet ATENA sur la cybersécurité des infrastructures critiques, également financé par l'UE. La partie académique a été supervisée par les Professeurs Yves Le Traon et Jean-Marie Bonnin de l'Université du Luxembourg et d'IMT Atlantique Bretagne-Pays de la Loire respectivement, qui ont décerné conjointement le doctorat.

### **À propos d'itrust consulting**

itrust consulting, une PME luxembourgeoise spécialisée dans la sécurité de l'information, aide ses clients des secteurs public et privé à protéger leurs données contre la divulgation, la manipulation, et l'indisponibilité. Ses services consistent entre autres à établir, implémenter et auditer des systèmes de gestion de la sécurité de l'information, à évaluer et traiter les risques à l'aide de son outil TRICK Service, à mettre à disposition ses experts en sécurité en cas de besoin (SECaaS, la sécurité en tant que service), à pirater sur demande de nos clients leurs infrastructures et à gérer des incidents de cybersécurité (malware.lu CERT), ou encore à concevoir et opérer des solutions de sécurité pour les TIC. Ces services bénéficient hautement de projets de recherche cofinancés par des instances nationales et européennes.

### **À propos du SnT**

Le SnT (*Interdisciplinary Centre for Security, Reliability and Trust*) est un centre de recherche de l'Université du Luxembourg. Grâce à son programme de partenariat, les chercheurs du SnT, en collaboration avec des partenaires de l'industrie et du secteur public, relèvent les défis actuels des TIC. Le programme encourage le développement d'idées innovantes, faisant du Luxembourg un centre européen d'excellence et d'innovation dans le domaine des systèmes et services TIC sûrs, fiables et dignes de confiance.

### **À propos d'IMT Atlantique**

IMT Atlantique Bretagne-Pays de la Loire est une grande école spécialisée dans les technologies numériques, l'énergie et l'environnement. Le Département Systèmes réseaux, Cybersécurité et Droit

du numérique (SRCD) est situé sur le campus de Rennes de l'IMT Atlantique. Ses domaines d'activité couvrent tous les aspects de l'enseignement et de la recherche en :

- systèmes réseaux, y compris les technologies pour les réseaux fixes et mobiles et l'Internet des Objets. En outre, les systèmes complexes qui permettent de construire et de sécuriser les systèmes qui soutiennent l'énergie, l'industrie, les villes et le transport intelligent ;
- la cybersécurité, en renforçant la sécurité des systèmes complexes, des industries du futur et des infrastructures critiques ;
- le droit et l'économie de la technologie numérique, notamment au niveau européen et international.

### **À propos de SGL-Cockpit**

SGL-Cockpit vise à concevoir, développer et tester les outils et méthodologies nécessaires pour surveiller les aspects de cybersécurité du Smart Grid Luxembourg (SGL 2.0). Il est financé par le Ministère de l'Économie luxembourgeois. Le projet est géré par itrust consulting, et les autres partenaires sont CREOS et l'Université du Luxembourg.

### **À propos de TRESPASS**

TRESPASS (*Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security*) est un projet européen FP7 avec 17 partenaires de neuf pays européens. Son objectif est de développer des méthodes et des outils de prédiction, d'évaluation et de hiérarchisation des scénarios d'attaque sur l'infrastructure informatique d'une entreprise. Le projet développera des méta-modèles de risques intégrés physiques, numériques et d'ingénierie sociale, recueillera des connaissances empiriques sur les attaques socio-techniques et développera des méthodes quantitatives pour évaluer le risque de ces attaques. Ces modèles et techniques seront intégrés dans des méthodes d'évaluation des risques et mis en œuvre dans un "navigateur d'attaque" pour soutenir la prise de décision en matière de sécurité. <http://www.trespas-project.eu/>

### **À propos d'ATENA**

ATENA (*Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures*) est un projet européen financé par le programme Horizon 2020 'Digital Security: Cybersecurity, Privacy and Trust, H2020-DS-2015'. Le projet ATENA vise à atteindre un niveau donnée de sécurité et de résilience des infrastructure critiques considérées, tout en préservant leur gestion efficace et flexible. En s'appuyant sur les résultats des activités de recherche européennes précédentes, en particulier les projets européens CockpitCI et MICIE, ATENA améliorera ces résultats de manière remarquable en exploitant les caractéristiques avancées des algorithmes et des composants TIC, et les portera au niveau de la maturité industrielle opérationnelle ; à cet égard, les résultats ATENA seront adaptés et validés dans une sélection de cas d'utilisation. <https://www.atena-h2020.eu/>