L.A.A.S. du C.N.R.S. - 7, Avenue du Colonel Roche - 31077 Toulouse Cédex 4 - ✆ 05.61.33.62.00

SUJET DE THESE 2016-2017

Equipe de Recherche :

Thèmes :

INFORMATIQUE CRITIQUE	☐
RESEAUX ET COMMUNICATIONS	☑
ROBOTIQUE	☐
DECISION ET OPTIMISATION	☐
HYPERFREQUENCES ET OPTIQUE DE L'ELECTROMAGNETISME AUX SYSTEMES	☐
NANOINGENIERIE ET INTEGRATION	☐
MICRONABIOTECHNOLOGIES	☐
GESTION DE L'ENERGIE	☐

Mot(s)-clé(s) : Sécurité proactive, Machine learning, détection d'anomalies, big data

Responsable du sujet : P. Owezarski e-mail : owe@laas.fr

Titre de la Thèse: Analyse du trafic réseau pour une sécurité proactive

Le grand dessein de l'Internet est de devenir un réseau multi-services garantissant des qualités de services (QoS), et ceci en toutes circonstances, y compris les plus difficiles. Parmi celles-ci se trouvent notamment les moments où une attaque de déni de service, simple ou distribuée, est perpétrée, et pendant lesquels le réseau devient incapable de fournir les services demandés. Cette extrême fragilité de l'Internet souligne le lien étroit qui existe entre sécurité informatique et QoS. Plus généralement, l'Internet présente cette même sensibilité face à tous types d'anomalies dans les caractéristiques de son trafic, qu'elles soient liées à des pannes, des comportements byzanthins de certains éléments du réseau, ou plus simplement à des augmentations fortes mais légitimes du trafic liées par exemple à la diffusion sur le réseau d'un événement populaire.
L'objectif de cette thèse est de proposer des solutions originales pour détecter les anomalies/attaques et les caractériser. L'idée consiste à concevoir une méthodologie d'analyse du trafic fonctionnant de façon autonome et en temps réel, et ce sans aucune connaissance préalable du trafic, à l'opposé des techniques actuelles qui reposent sur les compétences d'experts et qui sont donc lentes et coûteuses et laissent les systèmes informatiques sans protection face à de nouvelles attaques pendant de longues périodes. Cette contribution utilisera et adaptera des techniques récemment conçues pour le trafic Internet général qui reposent sur des techniques de "data mining", de "machine learning" non supervisé, et de théorie de l'information pour estimer l'anormalité et/ou la dangerosité des anomalies/attaques détectées. D'autre part, cette thèse devra proposer des techniques et méthodes d'analyse des causes sources pour les différentes anomalies/attaques qui permettront ainsi de proposer des techniques de gestion de la QoS et de la sécurité des réseaux et des systèmes informatiques qui résultent de l'analyse des risques identifiés et caractérisés et dont la mise en œuvre et le déploiement seront faits, autant que possible, automatiquement.