Proposition de recherche doctorale

Systèmes coopératifs décentralisés de supervision et de contremesures

Mots clés :

- **Directeur de thèse** : AHMED SERHROUCHNI
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire Traitement et Communication de l'Information
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Contexte global de l'étude et état de l'art : La sécurité des infrastructures de coeur de réseaux est devenue un enjeu international à la fois pour les opérateurs et les utilisateurs de ces réseaux (qu'ils soient particuliers, entreprises privées ou administrations étatiques). En particulier, ces infrastructures doivent se prémunir des attaques distribuées de dénis de service (DDoS), qui s'appuient sur la capacité des attaquants à prendre le contrôle d'un grand nombre de machines zombies (botnets). Ce sont ces dernières qui réalisent les dénis de service quand elles en reçoivent l'ordre via un canal contrôlé par l'attaquant. Aujourd'hui, chaque opérateur met en place des systèmes de détection et de protection visant à limiter l'impact de ce type d'attaques pour ses infrastructures et ses clients. Ces systèmes routent généralement le trafic de dénis de service vers un trou noir. Des effets de bord peuvent se traduire par l'indisponibilité de quelques applications pour des utilisateurs légitimes. Le projet Européen DEMONS, dont le démarrage est prévu pour le Septembre 2010, propose d'améliorer les systèmes de détection et de protection actuels en s'appuyant sur un système collaboratif interopérateurs. Ce système comporte trois couches d'abstraction : 1- la couche de mesures, caractérisée par des sondes dont l'objectif est à la fois de détecter des attaques et si possible de mettre en place des contre-mesures 2- la couche de coordination, permettant le contrôle et la communication de ces sondes 3- la couche applicative, permettant de mettre en place les logiques et politiques de détection et de contre-mesures Ce projet soulève un certain nombre de problématiques, portant notamment sur: les algorithmes nécessaires pour être en mesure de détecter des attaques de type DDOS au sein d'un trafic légitime très important – et ceci en se positionnant près de la source de l'attaque et non de la cible. la conception d'algorithmes distribués, tirant profit d'un réseau de sonde collaboratif tout en préservant les concepts de confidentialité des données L'étude et la conception de systèmes de réaction distribués (automatisés ou manuels), tirant profit du même réseau de sondes pour améliorer et optimiser les contre-mesures en minimisant les effets de bord pour le trafic légitime Les travaux de recherche de la thèse s'intègrent aux contributions Orange Labs à ce projet. Positionnement du sujet vis-à-vis de la stratégie d'Orange et de l'OR L'élaboration de nouveaux moyens de défense active contre les menaces d'attaques sur des infrastructures et plates-formes distribuées vont nous permettre de maintenir et enrichir nos compétences et notre expertise dans ce domaine et de bénéficier des recherches en amont sur le sujet. Par ailleurs, l'OR sécurité porte la participation d'Orange Labs au projet Européen DEMONS (FP7).

Résumé du projet de recherche (Langue 2)

Objectifs de la thèse/ Résultats attendus/ Défis scientifiques/techniques à relever. Objectifs de la thèse Contribuer au développement des connaissances et de l'expertise d'Orange Labs nécessaires à la construction de solutions permettant de protéger nos réseaux et ceux de nos clients contre les attaques cybercriminelles. Résultats Attendus Elle intègrera notamment les aspects suivants: - Etat de l'art sur le fonctionnement des botnets (propagation, contrôle, auto-protection) et sur les attaques associées ; - Etat de l'art des systèmes de supervision et de contre-réaction ; - Analyse des scénarios et des besoins dans un contexte inter-domaines au sens réseau. - Conception d'algorithmes visant à une détection comportementale des botnets - Conception d'algorithmes de corrélation mettant à profit des points de mesures distribués - Etudes de contre-réactions visant à filtrer, cloisonner ou désactiver ces botnets Nous souhaitons au travers de ces travaux acquérir une meilleure compréhension sur les risques directs et indirects que posent ces botnets pour les clients de l'opérateur (i.e. vol d'identité, vol de données bancaires, impact sur la QoS liés à l'activité du bot) et pour son infrastructure (i.e. les effets du trafic DDOS sur le coeur de réseau, l'impact sur les serveurs DNS et les relais SMTP de l'opérateur).

Informations complémentaires (Langue 1)

Contributions secondaires si prévues (participation à des projets collaboratifs) Le travail de recherche réalisé dans le cadre de cette thèse inclut des contributions au projet européen DEMONS (DEcentralized, cooperative, and privacy-preserving MONitoring for trustworthinesS). Ce projet a pour but de développer une solution de supervision et de contre-mesures distribuée (sondes distribuées dans le réseau des opérateurs) et coopérative entre opérateurs partenaires. Cet outil doit également être applicable au sein d'un même opérateur entre des plates-formes de services ou des infrastructures équivalentes.

Informations complémentaires (Langue 2)

none