Proposition de recherche doctorale

Study of attack mitigation techniques in cross-domain environments using privacy-aware monitoring

Mots clés :

- **Directeur de thèse** : Hervé Debar
- **Co-encadrant(s)** :
- **Unité de recherche** : Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

{{SUJET ATTRIBUE NE PAS CANDIDATER}} --- This PhD proposal addresses the domain of information systems and networks security, and more specifically operational network security. The objective of operational network and system security is to monitor information systems and networks, looking for evidence of attacks. The PhD will address three activities related to privacy-aware monitoring and threat mitigation : -* The work will investigate novel cooperative distributed detection algorithms aimed at recognizing global events - most prominently DDoS and botnet operations, but also ongoing malware infections and spam campaigns originated by botnets over email, Internet Telephony and Instant Messaging - based on a the exchange of partial information as available after aggregation and privacy protection. In other words, the detection algorithms traditionally designed to work with complete information from a local observation point will be evolved and complemented with global but incomplete information from other domains, in a combination of local and global processing. Moreover, the interplay between local and global processing must be dynamic and closed-loop: the output of global cooperative processing can provide input for and steer the local processing, e.g. by requiring a tighter analysis of certain traffic components recognized as suspicious, or instructing the local probes to adapt the local processing parameters to the global traffic status. -* The work will move beyond the IP-centric approach (where only IP-headers and IP-flows are analyzed) and explore novel cross-layer detection methods, where also application-layer data are extracted and analyzed in combination to network-level data. In this way the task of botnet and spam detection can benefit from the availability of application-level semantic and more complete end-to-end information between the remote users. In this regard the project will provide proof-of-concept detection modules focused on a selected set of applications, to be identified in the first phase of the project. -* The work will finally design and implement novel strategies for cross-operator cooperative mitigation and reaction that take advantage from the global view provided by the project's platform. The challenge here is to develop strategies that can co-exist with individual operators' policies and deployed legacy systems, allowing each operator to maintain full control over the information (e.g. alerts) received by and exported to other domains.

Résumé du projet de recherche (Langue 2)

The key aspects of this research are twofold: -* {privacy-aware} monitoring strongly constraints the elements that can be observed for diagnosing security threats. Solving this challenge relies on the capability to store synthetic information about attacks, and on the use of privacy-preserving technologies developed by the partners in projects such as PRIME and PRIMELIFE -* {cross-domain} detection and mitigation. The PhD subject is fundamentally interested in ensuring that global attacks bypass not only national boundaries, but also AS boundaries or telecommunications operators realms. Thus, the challenge is to ensure distribution and delegation of detection and/or mitigation capabilities.