Application of visual analytics techniques for network traces analysis and alert correlation

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)

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. More specifically, intrusion detection systems have been designed to analyze traces generated by the system under monitoring, such as logs, network packets or operating system calls, and seek evidence of malicious activity in these traces. Security information and/or event management systems (SIEM) are tasked with receiving, correlating and analyzing the alerts generated by intrusion detection sensors and other log producers, to make available a global view of the security status of the monitored system, and support the system administrator in making the right decisions for the continuous operation of his system. IDS sensors and SIEM platforms have historically generated and manipulated huge amounts of information. The main goal of the PhD topic is the research and development of novel visual analytics technologies for the understanding, identification and prediction of very complex patterns of particular or abnormal activities in various application areas dealing with network information security. It will involve analysis and mining of large amounts of heterogeneous data and the introduction of novel interaction and information visualization technologies. The ultimate goal is, by building upon the expertise of two distinct communities, to provide more efficient solutions to fight the cyber-crime

Résumé du projet de recherche (Langue 2)

The PhD will study the application of visual analytics techniques to two different data streams, one at the sensor level and one at the SIM level. Visual analytics expertise will be provided by other partners in the project, the contribution of Telecom SudParis targeting specifically the network security domain. The objective of the PhD is to define new tools that can be applied to raw traces (network traces in the context of this project) for the detection of network anomalies and that can be applied to large volumes of alert information to extract attack patterns and to evaluate the risks associated with these attack patterns.

Informations complémentaires (Langue 1)

This PhD is proposed within the FP7 Vis-sense project.