Development of new techniques for Security Information Management (SIM) based on service dependencies and attack impact models

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. The main goal of the PhD thesis is the research and development of novel techniques for intrusion detection and alert correlation, addressing cross-layer detection, quantitative risk analysis, decision support and threat remediation.

Résumé du projet de recherche (Langue 2)

The following topics will be addressed during the PhD: - Multi-level abstraction: The combined use of multi-level abstraction techniques and event dictionaries will make it possible to identify the architectural support which would be needed at each level (microprocessor, network, operating system, middleware, and application) to improve the performance of SIEM technology, so to make it effective in a Service Infrastructure context. - Cross-layer correlation: The work will allow sophisticated cross-layer correlation, which will make it possible to implement timely and accurate diagnostic features in an effective way. The objective is to ensure that threats against the business logic are detected in an effective way, even if lower-layer trace analysis does not lead to alert generation. - Threat analysis: the work will address attack modelling/simulation, threat analysis and risk evaluation based on combination of analytical modelling and generating multi-level attack graphs as well as fine-grained simulation (dynamical imitation of attack actions mixing packet-based simulation and emulation). This will be carried out using previously-generated dependencies models and a simulation platform provided by another project partner. - Counter-measures: The work will leverage the collected and correlated data to select appropriate responses, based on the quantitative evaluation and comparison of the attack and countermeasures impact, and then will deploy the selected reactions in the infrastructure.

Informations complémentaires (Langue 1)

This PhD is executed in the context of the FP7 "MASSIF" project.