NADIA: eNhancing vulnerability Analysis and intrusion Detection using Itinerant Agents

Master Thesis

Pasquale Stirparo

March 2008

Submitted to
SecLab
Department of Computer and System Sciences (DSV)
Kungl Tekniska Högskolan(KTH)
Stockholm, Sweden

This thesis corresponds to 20 weeks of full-time work.

Abstract

The rapidly increasing size of networks and the widespread use of Internet in recent years resulted in a huge number of security threats. Several solutions emerged in the past, which provide security at host or network level. These traditional solutions, like antivirus, firewall, spy-ware, and authentication mechanisms, provide security to some extent, but they still face the challenge of inherent system flaws, OS bugs and social engineering attacks. Recently, some interesting solutions emerged like Intrusion Detection and Prevention systems, but these too have some problems, like detecting and responding in real-time, because they mostly require manual interventions by system administrators. It is believed to have succeeded in protecting the hosts to some extent by applying the reactive approach, such as antivirus, firewall and intrusion detection and response systems. However, critically analyzing this approach, it can be concluded that it has inherent flaws, since the number of penetrations, Internet crime cases, identity and financial data thefts, etc. are rising exponentially in recent years. The main reason is that current solutions use only reactive approach, i.e. protection system is activated only when some security breach occurs. Therefore, there is the need to develop a strategy using Mobile Agents in order to operate in reactive and, mainly, proactive manners, what requires providing security based on the principle of defence in depth, so that the ultimate goal of securing a system as a whole can be achieved. System is assumed to be secure if unauthorized access (penetrations) is not possible and system is safe against damages. This strategy includes four aspects: (a) autonomously detect vulnerabilities on different hosts (in a distributed network) before an attacker can exploit them; (b) when vulnerability is detected, automatically apply the related patch, if available; (c) protect hosts by detecting attempts of intrusions in real time; and finally (d) perform tasks related to security management.