IDEA GROUP PUBLISHING **ITB13040**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter VII

Tracing Cyber Crimes with a Privacy-Enabled Forensic Profiling System

Pallavi Kahai, Cisco Systems, USA

Kamesh Namuduri, Wichita State University, USA

Ravi Pendse, Wichita State University, USA

Abstract

Security incidents that threaten the normal functioning of the organization are on the rise. In order to resist network attacks most organizations employ security measures. However, there are two sides of the problem at hand. First, it is important to secure the networks against new vulnerabilities. Second, collection of evidence without intruding on the privacy, in the event of an attack, is also necessary. The lack of robust attribution mechanism precludes the apprehension of cyber criminals. The implementation of security features and forensic analysis should be such that the privacy is preserved. We propose a forensic profiling system which accommodates real-time evidence collection as a network feature and uses a mechanism to keep the privacy intact.

Motivation

The Computer Crime and Security Survey 2003 conducted by Computer Security Institute (CSI) in association with the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad concluded that the theft of proprietary information was responsible for most of the financial losses, with the average reported loss of about $2.7 million per incident. Denial of service attacks alone were responsible for more than $65 million in total losses among the organizations that participated in the survey. The survey indicated that the threat to large corporations and government agencies originates from both inside and outside their electronic boundaries: 78% of the respondents quoted the internet as the source of attack and 36% attributed the attacks to internal systems. Viruses and worms can penetrate through thousands of computers through duplication and acquire information such as a company's e-mail directory or an individual's banking information. Among the organizations surveyed, 251 were able to quantify the losses as over $200 million. There has been an upward trend in the number of cyber crimes and also in their nature in 2004. In Massachusetts, organized crime groups hacked into the State Registry of Motor Vehicles databases paving the way for identity theft. A new trend noticeable in 2004 was "phishing", the use of spam impersonating a bank wherein an individual can be conned to provide confidential information.

Clearly, cyber crimes and other information security breaches are rampant and diverse. Most organizations employ methods such as encryption technologies, network monitoring tools, firewalls and intrusion detection, and response mechanisms to secure their networks. Configuring security features does not guarantee that the information system is absolutely foolproof. Evidence collection, "trace and trap" mechanism, and identification of the attacker are as important as intrusion detection. While there are several intrusion detection mechanisms available today, present technology lacks the tools and techniques for identification and IP traceback. Apprehending and prosecuting cyber criminals is complicated because of the intercontinental nature of the cyber space. Negotiations across jurisdictional boundaries, both corporate and national, are questionable because of the considerable variance between the regulations and policies of different government and corporations. This is generally because of the non-uniform legislative measures concerning privacy in different countries. Millions of computer systems around the world were affected by the May 2000 Love Bug virus initiated by a resident of the Philippines, which crippled email systems from the British Parliament to the Pentagon to networks in Asia. The virus caused billions of dollars of damage, mostly due to lost work time. Investigation was hampered by the lack of a Philippines law that specifically addresses computer crimes. The warrant was finally sought under the Access Devices Regulation Act of 1998. The law was written chiefly to target credit card fraud but also covered the use of any unauthorized access device in order to obtain goods or services. Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities and the potential for copycat crimes. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can therefore, defy the conventional jurisdictional domains.