Chapter XXXII
Large-Scale Monitoring of Critical Digital Infrastructures

André Årnes
Norwegian University of Science and Technology, Norway

ABSTRACT

Network monitoring is becoming increasingly important, both as a security measure for corporations and organizations, and in an infrastructure protection perspective for nation-states. Governments are not only increasing their monitoring efforts, but also introducing requirements for data retention in order to be able to access traffic data for the investigation of serious crimes, including terrorism. In Europe, a resolution on data retention was passed in December 2005 (The European Parliament, 2005). However, as the level of complexity and connectivity in information systems increases, effective monitoring of computer networks is getting harder. Systems for efficient threat identification and assessment are needed in order to handle high-speed traffic and monitor data in an appropriate manner. We discuss attacks relating to critical infrastructure, specifically on the Internet. The term critical infrastructure refers to both systems in the digital domain and systems that interface with critical infrastructure in the physical world. Examples of a digital critical infrastructure are the DNS (domain name service) and the routing infrastructure on the Internet. Examples of systems that interface with the physical world are control systems for power grids and telecommunications systems. In 1988, the first Internet worm (called the Morris worm) disabled thousands of hosts and made the Internet almost unusable. In 2002, the DNS root servers were attacked by a distributed denial-of-service (DDoS) attack specifically directed at these servers, threatening to disrupt the entire Internet.[1] As our critical infrastructure, including telecommunication systems and power grids, becomes more connected and dependent on digital systems, we risk the same types of attacks being used as weapons in information warfare or cyber terrorism. Any digital system or infrastructure has a number of vulnerabilities with corresponding threats. These threats can potentially exploit vulnerabilities, causing unwanted incidents. In the case of critical infrastructures, the consequences of such vulnerabilities being exploited can become catastrophic. In this chapter, we discuss methods relating to the monitoring, detection, and identification of such attacks through the use of monitoring systems. We refer to the data-capturing device or software as a sensor. The main threats considered in this chapter are information warfare and cyber terrorism. These threats can lead to several different scenarios, such as coordinated computer attacks, worm attacks, DDoS attacks, and large scale scanning and mapping efforts. In this context, the primary task of network monitoring is to detect and identify unwanted incidents associated with threats in order to initiate appropriate precautionary measures and responses.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

NETWORK MONITORING AND INTRUSION DETECTION

In this chapter, we will look at different aspects of network monitoring. Network monitoring is the field of capturing traffic data on a network in order to perform corresponding analysis. We consider the areas of threat monitoring, intrusion detection, and security monitoring to be covered by the term network monitoring. Threat monitoring is a term currently used by, for example, the Internet Storm Center. The term was used by NIST in a publication regarding the monitoring of internal and external threats to a computer system (Anderson, 1980). Intrusion detection is the specialized field of detecting attempts to attack and compromise computer systems. Early work on intrusion detection systems (IDS) was published by D. E. Denning (1987). The practice of intrusion detection is discussed in several books, such as *Network Intrusion Detection* (Northcutt, 2002). Stefan Axelsson published a survey and taxonomy for IDS in 2000 (Axelsson, 2000). The term security monitoring was used by Bishop (1989), which provided a formal description of a security monitoring system with logging and auditing as its main components. Richard Bejtlichs book *Network Security Monitoring Beyond Intrusion Detection* (Bejtlich, 2004) defines the term network security monitoring as a process consisting of the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions.

There are currently several organizations on the Internet that monitor and publish security relevant trends and events. Most notably, the Computer Emergency Response Team (CERT)[1], established in 1988, alerts users to potential threats on the Internet, and the Internet Storm Center[2], established in 2001, provides trend reports and warnings for its users. The Cooperative Association for Internet Data Analysis (Caida)[3] is another organization that provides tools for and publishes analysis results based on Internet monitoring. The European Union is currently funding a specific support project, Lobster for large-scale monitoring of the backbone Internet infrastructure. The project is currently in its implementation phase, and it is intended to provide a network monitoring platform for performance and security measurements in research and operational use.

Recent research on intrusion detection has, to a high degree, focused on scalability and performance for large-scale and high-speed monitoring. To address larger networks and increased scalability requirements, distributed intrusion detection has been discussed in several research papers (Snapp et al., 1991; Staniford-Chen et al., 1996). A variation on this is the agent-based IDS (Balasubramaniyan, Garcia-Fernandez, Isacoff, Spafford, & Zamboni, 1998; Carver, Hill, Surdu, & Pooch, 2000; Helmer, Wong, Honavar, Miller, & Wang, 2003). IDMEF is a recent standard for an intrusion detection message exchange proposed to facilitate standardized messaging between sensors and analysis systems (Debar, Curry, & Feinstein, 2005). It is used in distributed intrusion detection systems such as Prelude and STAT.

Threat and intrusion detection is generally on data analysis, being either a type of signature or pattern detection, or a statistical analysis. In intrusion detection, these are referred to as misuse detection and anomaly detection respectively. Misuse detection generates alerts based on known signatures of suspected security incidents, whereas anomaly detection generates alerts based on deviations from known or assumed normal traffic or use pattern. Another type of statistical analysis is data mining, as discussed in Jesus Menas book *Investigative Data Mining for Security and Criminal Detection* (Mena, 2003). Data mining can also be combined with intrusion detection (Barbara, 2002; Lee & Stolfo, 1998). See Marchette (2001) for a discussion on statistical analysis in computer intrusion detection and network monitoring.

Two central research topics in network monitoring and intrusion detection are detection of DDoS and worm detection. Such attacks can be efficient weapons in an information warfare or cyber terrorism scenario. The detection of zero-day worms is a problem that has provided inspiration for several research projects (Akritidis, Anagnostakis, & Markatos, 2005; Zou, Gong, Towsley, & Gao, 2005), and the Wormblog[4] is a resource for sharing updated information about worms

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/large-scale-monitoring-critical-digital/7464

Related Content

Spam, Spim, and Illegal Advertisement
Dionysios V. Politisand Konstantinos P. Theodoridis (2007). *Cyber Warfare and Cyber Terrorism (pp. 146-153).*
www.irma-international.org/chapter/spam-spim-illegal-advertisement/7451

Fake Identities in Social Cyberspace: From Escapism to Terrorism
Lev Toporand Moran Pollack (2022). *International Journal of Cyber Warfare and Terrorism (pp. 1-17).*
www.irma-international.org/article/fake-identities-social-cyberspace/295867

Security Monitoring of the Cyber Space
Claude Fachkha (2015). *Cybersecurity Policies and Strategies for Cyberwarfare Prevention (pp. 62-83).*
www.irma-international.org/chapter/security-monitoring-of-the-cyber-space/133927

SCADA Systems Cyber Security for Critical Infrastructures: Case Studies in Multiple Sectors
Suhaila Ismail, Elena Sitnikovaand Jill Slay (2016). *International Journal of Cyber Warfare and Terrorism (pp. 79-95).*
www.irma-international.org/article/scada-systems-cyber-security-for-critical-infrastructures/159886

Examinations of Email Fraud Susceptibility: Perspectives From Academic Research and Industry Practice
Helen S. Jonesand John Towse (2018). *Psychological and Behavioral Examinations in Cyber Security (pp. 80-97).*
www.irma-international.org/chapter/examinations-of-email-fraud-susceptibility/199883