IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB7359

Chapter XII

Managing Security in Modern Enterprise Networks

S. Raj Rajagopalan
Telcordia Technologies, USA

Security is one of the most pressing and expensive problems in the management of modern enterprise networks. The objective of this chapter is to persuade the reader to consider security from an entirely new perspective from the traditional one. We argue here that the current view of security management needs to be modified and propose a new business-friendly view that treats security as a process that is an integral part of network management and operations. For completeness, this article reviews some of the current security technologies and methodologies and examines which problems have been satisfactorily addressed and which still need a lot of research, development and operationalization. We finish with a brief overview of a current research project on automatic management of network security, which the author is involved in and addresses some of these issues.

INTRODUCTION

Security is about managing risk. Risk exists only if there is (1) an asset worth protecting; (2) one or more weaknesses allowing those assets to be attacked; and (3) an entity motivated to carry out such an attack. This chapter addresses each of these three components of risk for any enterprise network. In the modern network environment, it has become necessary for security to go past being a purely technical issue and become a vital component of a business case for any new network product or application. Our new understanding of the evolving business environment allows us to frame security issues in terms of the stakeholders, market forces, and industry

This chapter appears in the book, Enterprise Networking: Multilayer Switching and Applications by Vasilis Theoharakis and Dimitrios Serpanos.

practices rather than the traditional view of just network operations and cryptography. This chapter discusses, for example, how to address security as a regulatory topic, which may actually involve more severe business consequences than dealing with a technical attack. We provide an overview of the different aspects of security that can form the basis for a security architecture. The implicit assumption is that attackers will probe for the easiest access method without regard to architectural or design esthetics, so achieving security is necessarily a multifaceted activity. Security, like quality, is an ongoing activity; it is neither all-at-once nor all-or-nothing and thus, the generic recommendations for any CIO would be to have short-term, intermediate-term, and long-term efforts to continuously update and upgrade security functionality. We also provide an example of future-looking security technology that the author has been involved in for the past few years.

WHY IS SECURITY MORE IMPORTANT TODAY?

Recent trends indicate an increase in security incidents in all computer networks. These increases range from simple misconfiguration errors that cause temporary loss of access to massive global denial-of-service attacks like the ones that were seen on prominent web portals in 2000. Understanding these threats and vulnerabilities is the first step in reducing and managing risk through a program of prevention, detection, and response, which includes not only technical countermeasures but also policies, awareness, and operational and business processes shared among all the entities that are affected by these attacks.

What are these vulnerabilities and why is it worse today than in past years? In today's networks, vulnerability is increased because of the enormous number of different networks and subsystems that are interconnected. A casual inspection of an average enterprise network invariably shows many applications from the realm of paper memos such as corporate purchasing, vouchers, and customer accounts that have been given web interfaces to increase productivity. This interconnectivity has amplified the danger from the attacks that were already widely acknowledged. In addition to this general trend, specific phenomena have also contributed to the new vulnerabilities. Because network intelligence and signaling capabilities have been extended out to the network edges, end entities may be able to achieve a higher degree of control by replacing or modifying their network interfaces. A prominent example of this phenomenon is the Java applet which, in its various incarnations, allows remote programs a remarkable degree of control over host computers. This is not the only manifestation of this phenomenon: routers, switches, and other network infrastructure routinely provide access for remote administrators to change configurations using simple interfaces such as telnet and http. As more network equipment becomes programmable and configurable, the corresponding danger of loss of resources from well-meaning, but naive participants (not to speak of rogue