IDEA GROUP PUBLISHING **ITB12243**

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, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter XXI

A Comparison of Authentication, Authorization and Auditing in Windows and Linux

Art Taylor, Rider University, USA

Lauren Eder, Rider University, USA

Abstract

With the rise of the Internet, computer systems appear to be more vulnerable than ever from security attacks. Much attention has been focused on the role of the network in security attacks, but it is ultimately the computer operating system that is compromised as a result of these attacks. The computer operating system represents the last line of defense in our security chain. This final layer of defense and its core defense mechanisms of authentication, authorization, and auditing deserve closer scrutiny and review. This chapter will provide an exploratory, descriptive, and evaluative discussion of these security features in the widely used Windows and Linux operating systems.

The Last Line of Defense: The Operating System

The number of computer security incidents reported from various forms of attacks has increased significantly since the introduction of the Internet (CERT, 2005; Staniford, Paxson, & Weaver, 2002). Though it is clear that the introduction of the Internet coupled with the decreased cost of networking has helped to pave the way for attackers, the end result of most malicious attacks is the alteration of the host operating system. This alteration is often with the intent of propagating the malicious program and continuing the attack (virus, Trojan horse) or potentially damaging, stealing, or altering some content on the host machine (Yegneswaran, Barford, & Ullrich, 2003). While this type of attack may be aided by the ubiquitous network and security weaknesses therein, the attack could not be successful without ultimately compromising the host operating system. These threats cannot be addressed without concentrating on the security weaknesses in the operating system (Loscocco et al., 1998). Security weaknesses in host operating systems are, therefore, a major concern for the IT practitioner. If unwanted modification of the host system can be prevented, then the attack may be thwarted despite any weaknesses in the network that allows the attacker to contact the host machine.

There has been a distinction drawn in research between application security and operating system security. It has become increasingly clear, however, that such as distinction is academic and that, in practice, malicious programs and the individuals who create them make no such distinction. Malware such as Code Red exploited weaknesses in both application security and operating system security (Staniford, Paxson, & Weaver, 2002). What is required is an end-to-end solution, one that considers not only the distributed nature of the current computing environment and the network, but also the close relationship between the application program and the operating system (Howell & Kotz, 2000; Saltzer, Reed, & Clark, 1981; Thompson, 1984).

This chapter will examine the principles of security for the host operating system in a descriptive and exploratory manner. By understanding the security controls available at the operating system level and the security weaknesses in those systems, it is possible to understand how to better prevent attacks on these systems.

Operating systems and their underlying security mechanisms are clearly a varied landscape which, over time, can be quite fluid. For purposes of this discussion, the focus will be on two server operating systems: Microsoft Windows Server 2003 and Red Hat Linux ES Version 3. (These server operating systems are increasingly being deployed on desktops so this discussion also has some relevance for the desktop computing environment.) Rather than refer to specific versions of these operating systems, this chapter will use the terms Windows and Linux to refer to Windows Server 2003 and Red Hat Linux ES Version 3, respectively.