Chapter XXXIII
Plugging Security Holes in Online Environment

Sushil K. Sharma
Ball State University, USA

Jatinder N.D. Gupta
The University of Alabama at Huntsville, USA

Ajay K. Gupta
Gsecurity, Inc., USA

ABSTRACT

The ability to perform E-Commerce over the Internet has become the driver of the new digital economy. As it has opened up opportunities for businesses and consumers to conduct online transactions on a 24/7 basis, at the same time, it has also opened new opportunities for hackers to exploit the medium for nefarious cyber attacks. This paper discusses various potential security holes that exists in the e-commerce environment and suggests a framework to protect organizations from security breaches.

INTRODUCTION

The Internet, which currently connects more than 300 million computers and 500 million users, is vulnerable to security breaches as indicated in numerous instances in recent times (Internet Users Report, 2007). Online fraud threatens to undermine consumer confidence in online financial services. Beyond simple phishing schemes, significant new threats are posed by spyware, browser hijacking, keystroke logging, and remote administration tools (Shukla & Nah, 2005). The Internet has the capacity to reduce global barriers and is becoming a fast and viable medium for conducting global business. As traditional businesses continue their migration into e-commerce, security will become a central issue to be seriously addressed. Even as organizations are looking at ways to strengthen the security of their networks and services, hackers all around the world are continuously discovering new vulnerabilities and inventing malicious breaches. Organizations who offer e-commerce are quite concerned about security breaches as it lessens the confidence of consumers and businesses in the privacy and integrity of online transaction and therefore their willingness to conduct business online (Araujo & Araujo, 2003). Numerous vulnerability scanners and intrusion detection systems
Plugging Security Holes in Online Environment

have been developed and implemented but systems still seems to be susceptible to many attacks.

Attacks on computer systems are becoming much more sophisticated—and potentially devastating—than in the even recent past. A variety of security breaches take place in today’s world and are often not reported by organizations looking to safeguard their own interests. The Computer Security Institute report (2007) reports that the average annual loss reported by U.S. companies in the 2007 CSI Computer Crime and Security Survey more than doubled, from $168,000 in last year’s report to $350,424 in this year’s survey (Gordon, Loeb, Lucyshyn, & Richardson, 2006). The 2007 Global Security Survey (2007) for financial institutions by Deloitte indicates that e-commerce security attacks are increasing. GeoTrust, Inc. reports that significant new threats are posed by spyware, browser hijacking, keystroke logging, and remote administration tools for various types of online fraud (GeoTrust Report, 2007). The companies responding to these surveys indicated that information security spending by financial institutions continues to rise. Almost all respondents (98%) indicate increased security budgets, with 11 percent reporting an increase of over 15 percent over 2006. The report indicated that the security budgets increased from 14 percent in 2006 to 36 percent in 2007 (Deloitte Report, 2007). The Federal Financial Institutions Examination Council (FFIEC) also issued new guidance for new multi-factor authentication methods with identity verification best practices and consumer trust components for more effective and reliable means for authenticating end users (GeoTrust Report, 2007).

Despite the increased awareness, the recent frequency of security breaches seems to indicate that many companies have not adequately responded to the issue of data security within their organizations. New regulations and statutes are sure to get some attention, but the pressure to mitigate data security risks certainly increases. Interest in security is increasing and shareholders expect organizations to use proactive security measures to protect their value (Caralli & Wilson, 2004). Customers also expect the organizations with whom they conduct business online also expect a higher level of protection of their personal data. News reports of high-profile attacks on well-known Web sites do have an adverse impact on consumer confidence.

Organizations invest heavily in the latest firewalls, intrusion detection systems and other advanced security technologies, yet losses from security incidents continue to grow each year. As technologies advance, hackers also advance their tools, techniques and methods to break-in to and compromise networks (Dhillon & Torkzadeh, 2006). Up until a few years ago, phishing attacks (phony e-mails designed to entice users to give up personal information) were unheard of. Now they are relatively common and pharming (creating phony Web sites designed to extract personal information) has become one of the latest strategies employed by identity thieves (Gartner Report, 2005).

Security experts noted that the legions of infected computers are adding to the number of bot networks controlled by hackers. As such, organizations need to stay abreast of the latest protective measures and services to prevent and immediately respond to and recover from cyber attacks.

It is becoming imperative that networks must have self-defending capabilities to mitigate security threats before they affect operational continuity. Security measures deployed in any system should be commensurate with the risks on the system as well as the value of the system’s output and of the data the system holds and/or processes. However, the process to determine which security controls are appropriate and cost effective is quite often a complex and subjective matter (Caralli & Wilson, 2004). Technology is always changing and the need for adequate security over information technology systems is crucial not only to meet regulatory compliance, but to a specific business’ needs and the bottom line (Udo, 2001).

Making information available on interconnected networks allows for e-commerce and also creates the possibility for corporate espionage as corporations’ business critical and sensitive information is placed on systems that are remotely accessible. This paper identifies possible security holes in an online environment and suggests a framework to prevent organizations from security breaches. The first section of the chapter discusses the various kinds of vulnerabilities at various levels of the E-commerce infrastructure. The next section proposes a comprehensive framework for plugging security holes in an online environment. The paper finally concludes with some directions for future research in this area.

VULNERABILITY IN AN ONLINE ENVIRONMENT

To understand the vulnerabilities that may lead to a security breach, it is worthwhile first to understand