Chapter IX

Internet and E-Business Security

Keng Siau
University of Nebraska - Lincoln, USA

Kent Whitacre
Mutual of Omaha, USA

Survey: Internet improves lives, but raises privacy fears [CNN, February 23, 2000]
Insufficient computer security threatens doing business on-line [CNN, February 24, 2000]
‘I Love You’ virus sweeps the US [CNN, May 5, 2000]

The Internet is one of the miracles happening in this century. Starting from a project known to a few hundred people, the Internet is now a global network and the hottest hype in the world. Its growth, however, has been slowed by the concern over Internet security. Internet security has been blamed as the stumbling block preventing the widespread acceptance of electronic business. Is Internet security really a problem? If so, what are the technologies available to alleviate this problem? How should management evaluate the existing technologies? This chapter looks at the issues surrounding e-business security. The chapter first discusses Internet security and then proposes a framework to help management evaluate existing security technologies.

THE INTERNET/E-BUSINESS ERA

In 1997, Taaffe wrote that electronic commerce over the Internet was expected to grow from “$2.6 billion to more than $220 billion by 2001…much of the growth during the next two years to be spurred by business-to-business commerce.” Recently, BusinessWeek
(2000) claimed that e-business transaction was estimated to be $450 billion in 2000. Whatever the exact dollar amount, the fact is that e-business is huge and it is growing. To continue with this exponential growth of e-commerce, the security issue of the Internet must be addressed and the security threat alleviated. Security is a prerequisite for e-business (Keen et al. 2000, Turban et al. 2000, Fingar et al. 2000, Kaufman et al. 1995, Ford & Baum 1997).

Internet usage has been growing at an amazing rate. From a research project that was known to a few researchers, it is now used by millions of users worldwide. Simply speaking, the Internet is a collection of networks and routers that use TCP/IP (Transmission Control Protocol/Internet Protocol) to function as a single, large network (Comer 1999). It has been known as the network of all networks (Comer 1997). The reason for the rapid expansion of the original Internet, ARPANET, has been the various technological advances in personal computers, telecommunications and economies of scale in the computer world.

In addition to Internet, Intranet and Extranet are also getting much attention and growing in importance. Intranets are networks based on Internet standards and exist within an organization for the benefit of its employees. An Extranet is a private wide area network (WAN) using Internet protocols. An example would be a manufacturer that uses an Extranet to exchange information with its suppliers. The information could consist of raw material needs, production schedules, etc. Manufacturers using Just-In-Time manufacturing need constant communication with their suppliers in order to ensure that the raw materials arrive timely and at the correct site. An Extranet can be a value-added benefit that helps strengthen the relationship between buyer and seller. Organizations will rely on Extranets as their main communication system when dealing with buyers and suppliers; thus providing a vital link in an organization’s value chain.

INTERNET SECURITY: IS IT REALLY AN ISSUE?

One of the greatest strengths of the Internet is also one of its greatest weaknesses: anybody with a computer and a modem can gain access to the Internet. This has lead to horror stories about “hackers” breaking into the Department of Defense computer systems, hackers stealing credit card numbers and other well publicized incidents. Two good examples are the Melissa and “I Love You” viruses that created havoc throughout the world. Experts estimated that 60-80 percent of U.S. companies were infected by “I Love You” (CNN, May 5, 2000).

The security threat is aggravated by the fact that the Internet is a global network. A few recent incidents clearly demonstrate that hackers can be from any country in the world—sometimes beyond the reach of the legal arm. Legal infrastructures are country and state dependent. What is illegal in one country may be legal in another. It is, therefore, difficult to use a regional legal tenant to address a global security threat. The legal infrastructures are lagging behind the advancement of the Internet by at least a decade.

One of the barriers to e-business is on-line transaction fraud. Although there is a low amount of fraud compared to other techniques of transfer as the table illustrates (Sharon and Mitch 1997), the psychological fear of consumers when using the Internet is a major stumbling block to the growth of e-business.

There have been two kinds of fraud perpetrated over the Internet: outright theft and theft by deception. An example of outright theft would be a hacker stealing a credit card
Related Content

Wireless Hacking
(2019). *Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention* (pp. 244-257).
[www.igi-global.com/chapter/wireless-hacking/218421?camid=4v1a](www.igi-global.com/chapter/wireless-hacking/218421?camid=4v1a)

A State-of-the-Art Review of Data Stream Anonymization Schemes
[www.igi-global.com/chapter/a-state-of-the-art-review-of-data-stream-anonymization-schemes/114368?camid=4v1a](www.igi-global.com/chapter/a-state-of-the-art-review-of-data-stream-anonymization-schemes/114368?camid=4v1a)

Towards Usable Application-Oriented Access Controls: Qualitative Results from a Usability Study of SELinux, AppArmor and FBAC-LSM
[www.igi-global.com/article/towards-usable-application-oriented-access/64346?camid=4v1a](www.igi-global.com/article/towards-usable-application-oriented-access/64346?camid=4v1a)

Secure Group Message Transfer Stegosystem
[www.igi-global.com/article/secure-group-message-transfer-stegosystem/153529?camid=4v1a](www.igi-global.com/article/secure-group-message-transfer-stegosystem/153529?camid=4v1a)