Journal of International Technology and Information Management

Volume 15 | Issue 2 Article 3

2006

Enterprise Integrated Security Platform: A Comparison of Remote Access And Extranet Virtual Private Networks

Emmanuel U. Opara
Prairie View A&M University

Jack T. Marchewka
Northern Illinois University

Enterprise Integrated Security Platform: A Comparison of Remote Access And Extranet Virtual Private Networks

Emmanuel U. Opara
Prairie View A&M University

Jack T. Marchewka
Northern Illinois University

ABSTRACT

The Internet has created unprecedented opportunities for both organizations and individuals. However, these opportunities also have created a double-edge sword as organizations attempt to connect trading partners, customers, and remote users while providing adequate security measures that are flexible and cost-effective. This paper explores why secured socket layer (SSL) may be better tool for secured remote access and extranets by comparing it to internet protocol security virtual private networks (IPSec-based VPNs).

INTRODUCTION

The Internet has advanced to where networked systems and software agents are highly depended upon to support the exchange of information between individuals and organizations (Andress, 2000). Network security has become and will remain a primary concern as many enterprise users access corporate resources from cyber cafes, airport kiosks, or even home personal computers (PCs) that information technology (IT) departments often cannot control adequately (Lechner & Hummel, 2002; Nahnybida, 2003; Rubenkinf, 2002; Skoudis, 2005; Sundaram, 2000). In addition, secure network activity is also critical as many firms have extended their network infrastructure to their trading partners, remote customers, suppliers, and consultants. For example, Johnson and Johnson, one of the largest healthcare organizations with more than 200 separate companies located in 54 countries, views one of its biggest e-commerce challenges as providing business partners with access to its network while maintaining a high-level of security (Messmer, 2005). The company must balance the threat of introducing viruses and worms once its business partners are given access to the organization's network. Protecting enterprise data residing in relational databases is a primary goal of information security professionals as they strive to meet the objectives of confidentiality, integrity, and availability of data (Rutrell, 2001).

Although IT can be used to support an organization's goals and provide a competitive advantage, security threats and risks can lead to missed business opportunities or even disaster (Gartenburg, 2005). For example, a report published by Forrester Research, suggests that only 30 percent of the 22,907 Europeans polled said they have confidence that adequate security exists for keeping credit and debit card information used to make online transactions safe. On the other hand, approximately two-fifths of the Internet users polled do not use online banking and have no intention to do so because of security concerns. In fact, Forrester also reported that many Europeans believe online banking is less secure than paying by credit card in a store or restaurant. A similar study in the U.S. reported that about 3 million Internet users have discontinued using online banking services, with approximately one-third citing security issues as their main concern (Blau, 2005). Another study conducted by a Harris interactive poll, reported that more than 80 percent of the adults surveyed said that security and access to online data are their key concerns when using online services (Prokop & Machlis, 2005).

Given the onset of security breaches throughout the world, this may be quite understandable. For example, the British bank, HSBC Bank PLC, recently contacted more than 180,000 of its customers warning them that their credit card information may have been stolen due to a security breach at a U.S. retailer (Pruitt, 2005). However, security concerns are not only limited to the financial services industry. Cyber-criminals are increasingly taking advantage of vulnerable security measures and stealing valuable customer data. Often these criminals add insult to injury by extorting these businesses to buy back their customer lists (Prokop & Machlis, 2005).

The purpose of this paper is to explore how organizations can manage and support complex virtual private networks (VPNs) by comparing Internet Protocol Security Virtual Private Networks (IPsec VPNs) with secured sockets layers Virtual Private Networks (SSL VPNs). The objective in comparing these two VPN protocols is to understand better how remote users can be given secure and easy to use access to applications and resources on organizational networks, while minimizing risks from unmanaged access points. This should be of interest to both academics and practitioners. For academics, this study provides a basis of comparison of two technical approaches that can be used a foundation for future research concerning network security and protocols. For practitioners, this study can provide practical insight as to the technical and managerial decisions that can impact the IT strategy and, in turn, influence an organization's opportunities and risk.

NETWORK SECURITY

A study conducted by Ernst & Young reports that investments in IT security do not appear to provide adequate returns (Prokop & Machlis, 2005). Although organizations are spending an unprecedented amount of money on antivirus software, intrusion detection, and anti-spam products, many organizations still face security threats because of insufficient staff training, malicious attacks, and a lack of guidance from senior management. Modern organizations require a secure environment to meet its business objectives even though the value of IS security investments remain a challenge (Coulson, Zhu, Miyuan, & Rohm, 2005).

Although appropriate security measures may be difficult to show on the bottom line, many organizations are viewing security measures as a "reduction of risk on investment" (Vijayan, 2005). The growth of the World Wide Web (WWW) has enabled the extensive integration of network-level security technologies such as secured sockets layers (SSL), Internet Protocol Security (IPSec), and firewall filtering that attempt to create a secure perimeter around an enterprise network. Enterprise network administrators and Web professionals are generally aware of SSL certificates and the role they play in Internet security platforms (Berinato, 2000). As one study has shown, this secured perimeter is fast becoming permeable as more businesses seek to cut costs and improve their revenues by securely sharing applications with internal business units, external partners, and customers (Nerney, 2003).

Today, effective security is a business necessity since it protects the integrity of an enterprise system and supports corporate and organizational strategies. The basic principles of systems security include authentication, authorization, and auditing (Nahnybida, 2003). These features are required for all computing models such as client/server, Web Services, and grid/utility computing.

SSL, which is a transport-centric authentication technique, is not sufficient by itself to assure data integrity and confidentiality across multiple platforms (Drury, 2000). Since Simple Object Access Protocol (SOAP) messages can migrate across multiple arrays of a communication links, the security context is normally compromised or lost as SOAP messages are routed between end-points (Daudelin, 2000; Olson, 2000).

Authentication by itself alone, does not provide adequate security for the threat protection level of the security conundrum. For example, Denial of service ([DOS) attacks, information leakage, and malicious activities can all arise regardless of authentication strength (Savage, 2000).

However, some levels of systems and information security mechanisms have been commonly used to protect organizational IT resources. William (2000), noted that SSL is easier to implement and provides a more flexible security model; however, IPSec-based virtual private networks (VPNs) are the technology traditionally used to secure extranets.

Moreover, many organizations support their full-time remote workers with available technological resources. These workers supplement their office operations by working from a PC at home or while on the road. Other support activities include ad-hoc remote access users and remote employees. This group generally requires clientless and broadband access to corporate network resources in real-time (Powell, 2004).

Although many organizations take steps to protect their intellectual properties within an open source marketplace, enterprise systems can still be breached when attempting to connect users to corporate resources.

Enterprise systems in the past have relied on the use of the traditional IPSec-based VPNs and VPNs for site-to-site and branch-to-branch communications (Rutrell 2001 and Rubenking 2002). However, this protocol was not designed for remote access and extranet connections. When enterprise systems are in the remote access market, IPSec satisfies the basic requirements when there are a limited number of tunnels to create. When there are thousands of remote users at different locations, distributing, and managing the required client software can be cumbersome and costly thereby often leading to a compromised security system (Vijayan, 2000)

Another major concern of IT security includes confidentiality, integrity, non-repudiation, and data integration. Confidentiality concerns the protection of sensitive information, while integrity assures that transactions are not altered. Moreover, non-repudiation focuses on providing evidence that transactions have occurred, and integration relates to the ability to integrate with various company functions such as marketing, sales, finance, etc rather than through a piecemeal or isolated approach.

A COMPARISON OF IPSec VPNs and SSL VPNs

In the past, the Internet Protocol Security Virtual Private Networks (IPsec VPNs) for extranets was a key solution for securing a network gateway because it provided site-to site remote access through an encryption tunnel (Decarmo 2000). However, an improved newly designed virtual private network called secured socket layer (SSL)-based VPNs has emerged as the leading security gateway for remote access and extranet VPNs (Rob & Opara, 2003).

Earlier studies found evidence that a number of organizations attempted to develop enterprise security solutions for automating system-to-system collaborations, within or across respected trusted organizational domains as a means to enhance productivity and reduce operation costs (Brunker, 2000; William, 2000; Yeh & Wang, 2001). More recently, studies by Skoudis (2005), Powell (2004), Nerney (2003), and Nahnybida (2003), have paid considerable attention as to how an eXtensible Markup Language (XML) security gateway can provide a communication conduit among heterogeneous computing environments that are often used in the development and hosting of system applications.

Weber (2001) suggests that SSL based VPNs will be replacing IPSec based VPNs for the remote access protocol. IPSec based VPNs will handle the function of site-to-site VPNs communications (Manes, 2001). In addition, Rob & Opara (2003) as well as Yeh & Hwang (2001) suggest that as the SSL-based VPNs market grows, a number of traditional IPSec-based VPN vendors will blur the lines by integrating SSL-based VPN technology in the same equipment as IPSec technology. The reasoning is that SSL-based VPNs and IPSec-based VPNS are designed to solve different problems for different clients. Combining SSL-based VPN technology into an IPSec protocol may not add any value to the process since there are no overlapping technologies or components that can be leveraged between the two.

According to Markoff (2002), SSL-based VPNs are gaining popularity in the security secured access market due to their proven record of clientless access, security apparatus, and the ease of manageable control functions. This technology has continued to lead the way in solving customers' remote access and extranet VPN-based problems by adding new features that incorporate field experiences in large and complex environments (Shen, 2005).

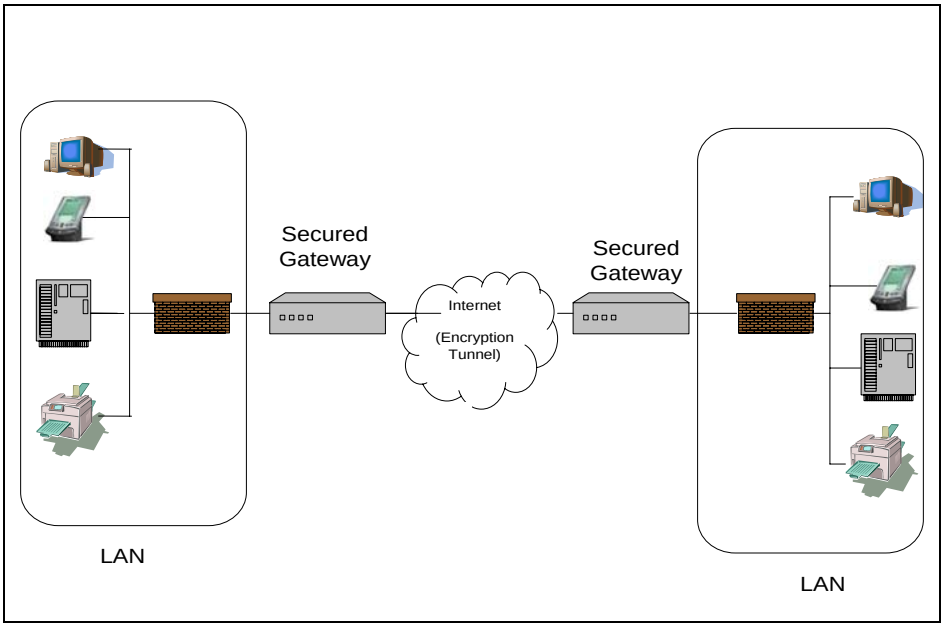
Other studies suggest that a lack of a standardardization between different IPSec vendors can create problems for the IT department whose responsibility includes setting up of a VNP technology that involves integrating different vendors or suppliers (Shen 2005). The effect could be that complex interoperability and integration problems could delay the process of getting new clients on board quickly (Piazza 2003). Powell (2004), Rubenking (2002), and Weber (2001) noted that SSL has emerged as the leading protocol in the remote access VNP environment. Moreover, Mulligan & Gordon (2002), further suggested that SSL-based VPNs are gaining more attention and that corporate implementation and usage is on the rise.

Vijayan (2000), Palmer (2001), Markoff (2002), and Skoudis (2005) suggest that business-to-business (B2B) enterprises that implement XML Web services security will benefit by transforming their business processes through which various enterprise collaborate with each other.

IPSec based VPNs at Work

IPSec is the de-facto standard for site-to-site VPN communications. This technology provides site-to-site remote access across an encryption tunnel as shown in Figure 1. Moreover, an IPSec-based VNP creates a tunnel over the Internet to connect users outside a corporate gateway to internal corporate resources. This type of system requires a high degree of compatibility between hardware and software. Usually a single vendor provides the necessary hardware or software for both ends of the encryption tunnel. Furthermore, with IPSec, the corporate IT groups dictate the technology used on both ends of the tunnel. As shown in Figure 1, the extranet capabilities of an IPSec-based VNP technology is limited because only a small number of firms can dictate the type of technologies their business clients or partners can use for their business.

Figure 1: IPSec based VPN.

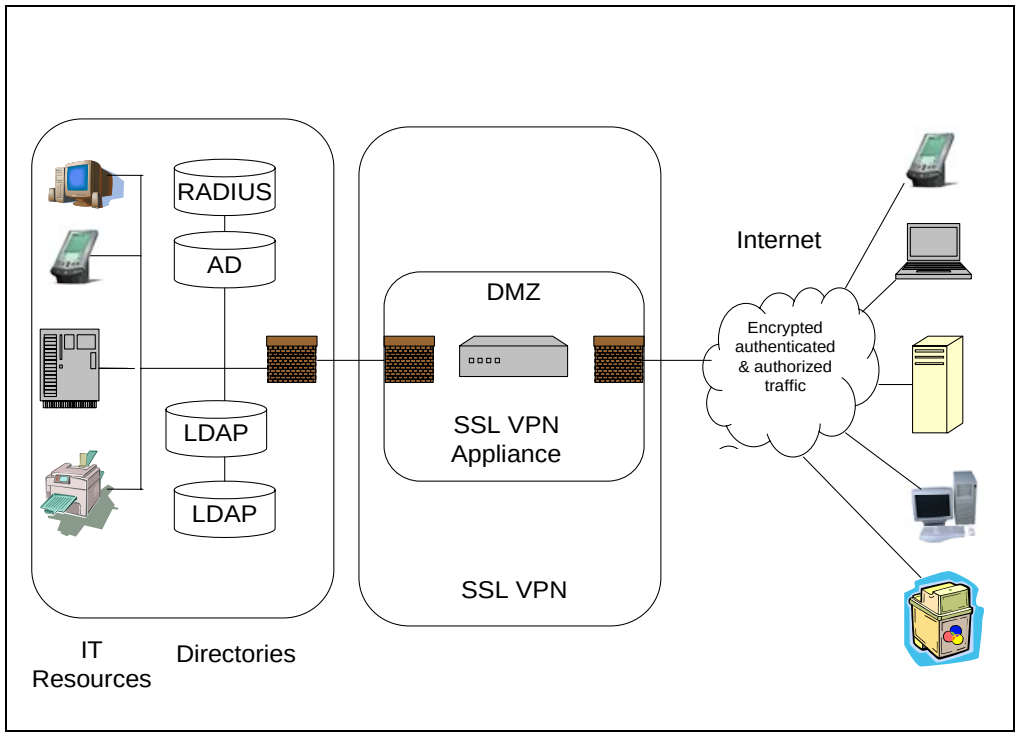


Adapted from Randall, Nichols, & Lekkas (2002)

SSL-based VPNs at Work

SSL is standard used in most browsers such as Internet Explorer and Netscape. It is network independent. This protocol is used for managing the security of a message transmission on the World Wide Web. It was designed to enhance productivity since it works on both wired and wireless platforms. These platforms include airport Kiosks, personal data assistants (PDAs), home PCs, and any unmanaged access point. SSL encryption occurs at the low and high levels. More specifically, low-level encryption occurs at either 40 or 56 bits while high-level SSL encryption occurs at a full 128 bits (Skoudis, 2005). This is widely believed to be the strongest SSL encryption for Web servers (Krim, 2003). Moreover, 128 bits encryption offers 2^{88} times as many possible combinations as 40-bit encryption. SSL is considered a higher–layer security protocol that sits closer to the application layer (Drury, 2000). This system requires a public key to encrypt data that is transferred over the SSL connection. As illustrated in Figure 2, the process works well when a client connects to the SSL VPN periphery, becomes validated, and gains access to the applications and resources for which access was granted. To ensure that there is no direct connectivity to the network, access is by proxy and occurs only at the application layer.

Figure 2: SSL-based VPN.



Adapted from Pfleeger (2003**)**

Table 1 provides a summary comparison of SSL VPN model to the IPSec VPN model.

Table 1: A Summary Comparing SSL VPN and IPSec VPN

IPSec VPNs	SSL VPNs
▪ Network-layer centric ▪ Designed to establish connection and protect private data streams between trusted networks. ▪ Suited for point-to-point access ▪ Assumes the end point is secured and authorizes users unless otherwise restricted. ▪ Uses tunneling and encryption to secure data transfer over the Internet between a private network and a trusted computer ▪ Relatively inexpensive technology to manage ▪ Pre-installed client software must be running on the user's machine. ▪ Not all IPSec VPN solutions can provide secured access through NAT and firewalls.	▪ Application-layer centric ▪ Designed to address the weaknesses of IPSec for remote access. ▪ Users have "anywhere" access to the network through any Internet browser ▪ Restricts end-users access unless authorized. ▪ Provides data encryption using the RCA or DES/Triple DES algorithms. ▪ Provides key management through the standard SSL key exchange method using the RSA algorithm with a bit length up to 1,024. ▪ Relatively manageable technology in the long run ▪ Uses most commonWeb browsers as the client by providing clientless access that increases the number of point's access is made. ▪ Can traverse NAT, firewalls and proxy servers. ▪ Network independent

Remote Access VPN Space Solutions

In addition, SSL-based VPN solutions can provide clientless access, as well as security and ease of management to enterprise systems. SSL-based VPNs can alleviate the problem of installing and managing complex

IPSec clients because SSL is included in most standard browsers such as Internet Explorer and Netscape. Moreover, SSL-based VPNs use SSL and proxy technology to instigate authorized and secure access for end-users to HTTP, client/server, and file sharing resources (Schneier, 2003; Shen, 2005). Since one of the enterprise system goals is to prevent users from making direct connection into its secured network, the addition of proxy technology to SSL platform enhances organizational security. As summarized in Table 2, SSL-based VPNs convey user-level authentication, thereby ensuring that only authorized users have access to the company's specific resources as allowed by the security policy of the organization (Kaufman, Perlman, & Speciner, 2002).

Table 2: IP SEC VPN versus SSL VPN.

IP SEC VPN					**SSL VPN**		
Variables	***High***	***Medium***	***Low***		***High***	***Medium***	***Low***
Cost and maintenance	X						X
Flexibility		X			X		
Scalability			X		X		
Integration		X			X		
Trusted relationship between network	X				X		
Transparency			X		X		
Efficiency		X			X		
Set-up time,	X						X
Training	X						X
Risk	X						X

An SSL VPN incorporates an integrated system for clientless access to Web applications, client/server applications and enterprise file sharing features (DeCarmo, 2000). SSL VPNs are rated high among leading organizations in scalability, security and modularity because they provide system users with secure, flexible remote access as they surf the net. Flexibility features include browser-based access for Web applications and file sharing protocols, a Web delivered Java SSL VPN agent for secured client/server applications and a Web-deployed Windows client that provides complete secured access to network resources from corporate computers, unmanaged desktops, employee home PCs, airport kiosks, cyber cafes, PDAs and computers used by business partners (Kaufman, Perlman, & Speciner, 2002; Gartenberg, 2005).

An IPSec VPN is effective when deployed as a support protocol in platforms where organizational groups use laptops, PDAs, or desktop computers. Even after an IPSec VPN is deployed, system configuration and periodic updates are required to run applications effectively (Powell, 2004; Blau, 2005).

Since SSL VPN are Web-based, downloads are relatively easy, even on a low-bandwidth connection (Powell, 2004). Although IPSec VPNs integrate with the desktop and personal firewalls, they do not perform well with environmental changes. When users migrate from network to network in remote areas, new system configurations are often required. As a result, security risks and cost of operations may increase (Vijayan, 2005).

Managerial Implications and Enterprise Systems Requirement

Organizations often face the challenge of identifying business requirements as well as the technical requirements related to security issues and challenges. For example, SSL-VPN provides full layer 3 connectivity to a remote network, but a key requirement for this technology entails a standard web browser that supports Java or

Active X capabilities. Subsequently, an organization's management should attempt to exploit this technology to its fullest potential so as to take advantage of its "ubiquitous" access and other capabilities.

This study also proposes that IPsec and SSL VPN are both complementary and therefore enterprise system managers may find it in the organization's best interest to not standardize on any one specific VPN protocol type because it will risk constraining client access requirements and overall enterprise systems objectives.

Moreover, an organization choosing an IPsec-VPN or SSL-VPN needs to consider organizational goals and objectives because they are mission driven. Most businesses are best served by implementing both technologies; however, consideration for a given technology should enable the organization to strengthened its competitiveness and attain organizational objectives. This includes the need for flexibility and the concern for a VPN being networked-based or customer premises equipment (CPE)-based.

Enterprise Systems Requirements to Deploy IPsec VPN or SSL VPN Technology

According to Prokop and Machlis (2005), there are several conditions that should guide an enterprise systems manager in the decision to deploy IPsec technology. These include, but are not limited, to the following:

- When the need for rapid deployment is critical because an organization is adding new sites and/or expanding to new locations or markets.
- When cost is an important consideration since this technology can be deployed across an existing IP network, thereby eliminating the capital and operational expenses of building a new network.
- When there is a vital need for security (i.e., data encryption, systems authentication, data confidentiality and integrity, etc.).
- When there is need to reduce congestion at hub sites when the enterprise system is configured for "split tunneling".

Alternatively, Prokop and Machlis (2005) suggest that the following conditions may help an enterprise systems manager determine when to deploy SSL VPN technology. Again, these include, but are not limited, to the following:

- When connections originate from a Web browser
- When remote access requirements include access to limited system network resources.
- When Information Technology departments have limited or virtually no control over the remote systems or the client software.
- When an organization needs to provide limited access from unmanaged systems such as from home computers, or access from airports, library kiosks or Internet cafes.

Subsequently, IT managers can meet their site-to-site VPN business requirements with the technologies mentioned above or with a combination of IPSec and SSL technologies.

CONCLUSIONS

Traditional enterprise network boundaries are dissolving rapidly as businesses expand globally and open up networks and applications to clients and mobile employees (Schneier 2003). A majority of organizations are implementing SSL VPN security gateway for enhanced systems flexibility, ease of administration and security. Security administrators are striving to achieve scalability, end-user simplicity, and strong security for the system (Pfleeger 2003). The goal is to lower administrative and support costs, reduce risks from increasing numbers of unmanaged access point within the network and provide remote access to multiple and complex applications. This study suggests that a SSL VPN client is better able to provide authorized users with secure and anywhere access capabilities. Further, it suggests that this technology will be able to provide transparency and simplicity to the end-users. It is believed that soon the majority of enterprise systems and organizations will implement SSL-based solutions as the leading technology for remote access. However, IPSec technology will continue to be used by enterprise systems for site-to-site communications between branch offices.

REFERENCES

Andress, M. (2000). AppShield repels hack attacks-speeds e-business applications to market while weeping web servers safe. Info World, 22 (20), May 1, 45.

Berinato, St. (2000). A UL-Type seal for secruity?, Don't bet on it. eWeek, October 15. http://www.zdnet.com/filters/printer-friendly/0, 6061, 2640597-2, 00.html.

Blau, J. (2005). Europeans worry about online banking security. Computerworld. March 30. http://www.computerworld.com/printthis/2005/0,4814,100736,00.html.

Brunker, M. (2000). Vast online credit card theft revealed: And related stories. MSNBC News, March 17. http://www.msnbc.com/news/382561.asp# BODY.

Coulson, T., Zhu, Z., Miyuan, S., & Rohm, C.E.T. (2005). The price of security: The challenge of measuring business value investments in securing information systems. Communications of the IIMA. 5(4). 19-32.

Daudelin, A. (2000) E-security advances for everyday banking, Bank Technology News 13(2), February 1, 21.

DeCarmo, L. (2000). Security protocols and performance. Dr. Dobb's Journal, 25(11), November, 40-48.

Drury, T. (2000). Safe and secure, Business First of Buffalo, 16(33), May 8, 21.

Gartenberg, M. (2005). Simple steps for raising the security bar at your company. Computerworld. March 30. http://www.computerworld.com/printthis/2005/0,4814,100589,00.html.

Harris, D. (2000). Security expert offers tips to stop web site defacement, Automotive News, 74(5865), March 13, 1

Hurwitz Report. (2000). Web application security: Protecting e-business from attack, Sanctum, Inc. http://www.sanctuminc.com/Security/more/index.html.

Kaufman, Perlman, & Speciner, (2002). Network Security: Private Communication in a Public World (2nd ed). Upper Saddle River, NJ: Prentice Hall, [ISBN: 0-13-046019-2]

Krim, J. (2003). WiFi is open, free and vulnerable to hackers: Safeguarding wireless networks too much trouble for many users, The Washington Post, July 27, A1.

Lechner, U. & Hummel, J. (2002). Business models and system architectures of virtual communities: From a sociological phenomenon to peer-to-peer architectures. International Journal of Electronic Commerce, 6(3), Spring, 41-52.

Manes, S. (2001). Security, Microsoft style: No safety net? PC World, 22(1), January, 25.

Markoff, J. (2002). Vulnerability Is discovered in security for smart cards. The New York Times, May 13. (http://www.nytimes.com/200205/13/technology/13SMAR.html)

Messmer, E. (2005). Johnson & Johnson tackles security pain. Computerworld. March 16. http://www.computerworld.com/printthis/2005/0,4814,101408,00.html.

Mulligan, P. & Gordon, S. (2002). The impact of information technology on customers and supplier relationships in the financial services. International Journal of Service Industry Management, 13(1), 29-46.

Nahnybida, S. (2003). Expectations unfulfilled on e-billing, e-payments. Bank Technology News, 16(10), October, 62-63.

Nerney, C. (2003). Get it right, Redmond. Internet News, May 12. (http://www.intenetnews.com/commentary/article.php/2205081

Olson, S. (2000). Protection from hackers available for e-tailers. Indianapolis Business Journal, 20(50). February 21, 5

Palmer, C. (2001). Ethical hacking. IBM Systems Journal, 40(3), 469-70

Pfleeger, C. P, (2003) Security in Computing *(3rd ed)*. Upper Saddle River, NJ: Prentice Hall, [ISBN: 0-13-337468-6]

Piazza, P. (2003). Phasing for trouble. Security Management, 47(12), December, 32-33.

Powell, T. (2004). Quick tips for web application security. Network World. 21(20), May 17, 50-51.

Prokop, M. & Machlis, S. (2005). Security highlights from around the world. Computerworld. May 06. http://www.computerworld.com/printthis/2005/0,4814,80400,00.html.

Pruit, S, (2005). British bank warns 180,000 over retailer's security breach. Computerworld. April 14. http://www.computerworld.com/printthis/2005/0,4814,101079,00.html.

Randall K., Nichols, & Lekkas, P.C. (2002) Wireless Security, (WS) McGraw-Hill Professional Books, January. [ISBN: 0-07-138038-8.]

Rob, M. & Opara, E. (2003). Online credit card processing models: Critical issues to consider by small merchants. Human Systems Management, 22(3), 133-142.

Rosencrance, L. (2004). Federal audit raises doubts about IRS security system. Computerworld, 38(36), September 6, 9.

Rubenking, N. (2002). Securing web services. PC Magazine, 21(17), October 1, lP01-04.

Rutrell, Y. (2001). Deep digital cover. Information Security, 4(10), October, 22.

Savage, M. (2000). Locking the doors-Denial of service attacks and viruses: Prime the market for security solutions and services. Computer Reseller News, September 25, 72.

Schneier, B. (2003). Beyond fear: Thinking sensibly about security in an uncertain world, **(**BF) Copernicus Books, 2003. [ISBN:0-387-02620-7]

Shen, X. (2005). Intellectual property and open source: A case study of Microsoft and linux in china. International Journal of IT Standards & Standardization Research, 3(1), January-June, 21-43

Skoudis, E. (2005). Five malicious code myths and how to protect yourself in 2005. SearchSecurity.com, January 4 http://searchsecurity.techtarget.com/tip/1,289483,sid14_gcu041736,00.html

Stonely, D. (2000). Hack job. The Business Journal, 18(2), May 5, 25.

Sundaram, A. (2000). An introduction to intrusion detection. Association for Computing Machinery. http//www.acm.org/crossroads/xrdds2-4/intrus.html

Verton D. (2004), Black ice: The invisible threat of cyber-terrorism, (ICE) Osborne, 2004 [ISBN:0-07-222787-7].

Vijayan, J. (2000). Possible s & p security holes reveal risks of e-commerce. Computerworld, 34(22), May, 29 6.

Vijayan, J. (2005). Strategic security. Computerworld. April 11. http://www.computerworld.com/printthis/2005/0,4814,100916,00.html.

Weber, T. (2001). Why you need to install a firewall-and why you shouldn't have to. *The Wall Street Journal,* July 30, B1.

Williams, C. (2000). Preparing your business for secure e-commerce. *Strategic Finance,* 82(3), September, 21.

Yeh, W.H. & Hwang, J.H. (2001). Hiding digital information using a novel system scheme. *Computers & Security,* 20(6), 533-538.