IT SOLUTIONS FOR NETWORK SECURITY

Mel Damodaran, Ph.D., University of Houston-Victoria, damodaranm@vic.uh.edu

ABSTRACT

Network security problems are varied and can variously affect the assets in a virtual marketing scenario. The solution to these problems has to be based on both technology and legislation. In this paper, we focus on those security threats with partial or full technological solution. We look at some of the new technologies that can change or have already changed the level of security in the global network, and some prospects for the future.

Keywords: Electronic Commerce security, network security, Internet security, security solutions

INTRODUCTION

In order for virtual marketing to succeed, customers must have confidence in the transmission of sensitive financial and personal information across networks to designated business organizations; digital enterprises must be certain in the knowledge that information collected over web storefronts is indeed valid; and furthermore, businesses must undertake additional precautions to ensure that databases with confidential information from their customers are not compromised by hackers or malicious employees. The solution to these problems has to be based on both technology and legislation. In this paper, we focus on the new technologies that can change or have already changed the level of security in the global network.

The paper first examines briefly our view of the assets that require protection in a virtual marketing scenario, the potential sources of threat, and the likely methods of attack. We then examine various types of security threats, including some "cutting edge" technology solutions, and explore how digital enterprises can be managed (and are being managed) more securely using these technology solutions.

ASSETS THAT REQUIRE PROTECTION IN A VIRTUAL MARKETING SCENARIO

The following are assets of e-commerce and other network based services, which require protection:

a) The personal data supplied by consumers need to be protected while in transit, while stored in company files and databases, and in future use. They must be protected against loss, damage, unwarranted changes and unwarranted third party disclosures.
b) The corporate databases of the organization offering goods and services by e-commerce must be protected as in a).
c) The applications and delivery platforms of the organization offering goods and services by e-commerce must be protected against all threats to its availability and integrity of its services.

d) Payment-related records and other records of value must be protected at a higher level than other customer data against fraud and privacy abuses.

POTENTIAL SOURCES OF THREAT

We can broadly classify sources of threat into the following two categories.

a) Outside individuals and organizations. This includes competitors in the market place, individuals and groups with a strong motivation to disrupt the services or gather intelligence, either for personal gain or other reasons. Competing organizations may be also lured by information about customers, debtors and suppliers besides strategic plans of the company. Certain outside organizations and individuals may be criminal or terrorist organizations or their representatives looking for opportunities to create fraud or disrupt or bring down e-commerce services.
b) Legitimate users, business associates and employees. These individuals may unintentionally damage e-commerce services or cause disruption to them sometimes as a result of mistakes, other times due to poor training, yet other times due to security breaches caused by them. In most of these cases, violations may be traced to the individual concerned and corrective actions such as sanctions and additional training are possible.

METHODS OF ATTACK

The following are the major types of attack.

a) Unauthorized access. This means accessing or misusing a computer system to intercept transmissions and steal sensitive information. This may be from an external source or by an insider acting on behalf of a hostile organization or for self-interest.
b) Service denial. This means that an attacker shuts down your site or denies access to visitors. This is done by overloading the system with excessive numbers of requests for service. This may also be done by the use of a malicious software such as a virus.
c) Repudiation. A party to an online purchase denies that the transaction occurred or was authorized.
d) Forgery, deception, theft and data alteration. These may result in theft or alteration of the content of a transaction -- user names, credit card numbers, and dollar amounts, for example -- during transmission or in stored files.
e) Malicious software may also threaten the confidentiality and privacy of stored information.
f) Spoofing. A fake site pretends to be the legitimate organization’s and steals data from unsuspecting customers or just disrupt business.
g) Repudiation. A party to an online purchase denies that the transaction occurred or was authorized.

Increased automation, sophistication of attack tools, faster discovery of vulnerabilities and increasing permeability of firewalls are among the key trends in computer attacks in the past few years, according to a recent report by CERT (Computer Emergency Response Team)

Coordination Center, a federally funded research organization operated by Carnegie Mellon University (3). CERT-CC identified four types of infrastructure attacks, namely:

a) Distributed denial of service -- This type of attack uses multiple systems to attack one or more victim systems. The main intent of the attack is to deny service to legitimate users of the victim systems.
b) Worms -- a self-propagating malicious code that could attack a large number of systems globally in a matter of hours.
c) Attacks on the Internet Domain Name System (DNS) which include cache poisoning, compromised data, denial of service, and domain hijacking.
d) Attacks against or using routers -- According to CERT-CC, intruders can use poorly secured routers as platforms to redirect traffic to other sites under their control.

According to the CERT-CC report, the level of automation and sophistication in attack tools continues to increase. "Today, scanning tools are using more advanced scanning patterns to maximize impact and speed," the CERT-CC report says. The report also notes that new attack tools allow attackers to devise attacks that can self-propagate at an incredible pace. "We have seen tools like Code Red and Nimda self-propagate to a point of global saturation in less than 18 hours." Attackers are also taking advantage of public communications protocols such as the Internet Relay Chat (IRC) and instant messaging to launch more coordinated attacks. Also, attackers' common use of the IRC or Internet protocol to send data or commands to victims' hosts makes it more difficult to differentiate it from normal network traffic.

It is interesting to note that according to CERT-CC, *the number of newly discovered vulnerabilities more than doubles each year*. This situation makes it more difficult for system administrators to keep up-to-date with software patches, hence, compromising the ability of their computer systems to counter attacks that exploit such vulnerabilities.

SECURITY PROBLEMS WITH SOLUTIONS

In this section we discuss some aspects of network security in the context of virtual marketing or e-commerce, that have been partially or wholly solved with technology.

Secure web connection

SSL (secure sockets layer) is the security technology that is used most frequently to provide an encrypted link between a point in one computer system to a point in another computer system. SSL was developed by Netscape. It uses public key cryptography to secure messages from web browsers (clients) to Internet transaction servers (merchants). Information that flows between those two points is encrypted using a symmetric algorithm; 128 bit SSL uses a good algorithm to securely protect information traveling between two points in computer systems. SSL also uses digital certificates to verify the identity of the server. However, SSL does not offer a means to confirm the customer, merchant or financial institution involved in a given transaction.

Secure Payment

According to surveys conducted by CommerceNet, Inc. in 1998 (5) secure payments was listed in the "Top Ten Barriers for Retailing" and in the "Top Ten Consumer Barriers". According to Burns (1), an ideal secure payment system should have the following characteristics:

- Ease of automated processing -- Automate the generation and processing of multiple payments with minimal effort.
- Immediacy of result -- The ability for the intermediate systems and providers to process payments in real-time.
- Openness and accessibility of payment processes -- Provide a range of payment services that were previously only available to large organizations via dedicated networks
- Loss of collateral information -- The new technology dispenses with, or alters, *collateral information* (which is not essential) accompanying transactions
- Globalization -- Minimization of geographical factors

Most e-businesses rely on established Internet transaction providers for their payment systems, which use debit and credit cards. The two most common security protocols used for this purpose are secure sockets layer (SSL) and secure electronic transaction (SET).

SET was developed by Visa International in conjunction with several other companies, and is widely used for debit and credit card transactions. SET uses digital certificates to identify the client (buyer), server (merchant), and merchant bank. SET employs public key cryptography to secure the messages between the three entities as they are transmitted over the Internet. SET allows the parties to confirm each other's identity. It uses digital certificates to allow a purchaser to confirm that the merchant is legitimate and allows the merchant to verify that the credit/debit card is being used by its owner. Lastly, it uses digital signature to identify the card holder to the retailer. These provide a certain level of trust, as well as protection from repudiation and unauthorized payments. It may be said of SET that it comes close to satisfying the five characteristics of a good payment system, as specified by Burns (1).

Authentication – Digital Certificates

As we saw, SET provides authentication by the use of digital signatures, which is the common means to provide authentication in e-commerce transactions. In general, customers and merchants generate these certificates through the mutual use of secret keys that shows the legitimacy of each party to the other. Most of these digital certificates conform to the X.509 standard, widely accepted as the best choice for digital certificates. X.509 compliant digital certificates are thought to strengthen simplicity and interoperability.

But, certificates do not completely solve the authentication problem, because the result is only as reliable as the process that created it.

Identity

Identity is often mistaken for authentication. Establishing a physical identity requires a manual process. One of the most frequently used identity schemes is a token or a smart card, a small device carried by the remote user; based on a challenge-response system, the user is allowed or denied access to the remote system.

It is worth remembering that many e-commerce transactions do not require the knowledge of a physical identity, but some do. What is often needed is authorization, which is the granting of a privilege, and is also sometimes confused with authentication.

Other vulnerabilities

In October 2001 SANS and FBI, in combination with dozens of leading security experts from the government, industry and the two leading university-based security programs, CERT/CC and the SANS Institute, came up with a “Top twenty” list of vulnerabilities (7). The report also includes advice on how to correct each vulnerability. This list proved very valuable, especially to small and medium size organizations with Internet exposure and individuals. Subsequently, the Center for Internet Security has come up with an automated scanning tool to help check a system to see if it has each of the listed vulnerabilities. According to the Center for Internet Security, the majority of successful attacks against computer systems via the Internet can be traced to exploitation of unpatched vulnerabilities on this list.

Increased emphasis on quality in software and system design

The prevalent approach to network security has been one of “patchwork,” a race against perpetrators and often one step behind. This is not the best way to operate and is enormously expensive and inefficient in the long term. Security has to be part of the design of the software. New standards of software quality need to take into account effective methods built into the software that would reduce or avoid the impact of current vulnerabilities. Newly developed information systems should be robust enough to withstand present and potentially new cyber attacks. It is a national challenge that needs to be addressed by the industry.

Interoperability - Lack of coordinated effort in security standards, tools and solutions

There is a host of tools, solutions and standards addressing various aspects of network security promoted and supported by different standard bodies, vendors and groups. Some of the most popular security tools in use today, according to SANS (6) are the following:

- Host-based Auditing Tools:
  - COPS, NCARP, crack, Tiger, Tripwire, logcheck, tklogger, Safesuite, NetSonar
- Network Traffic Analysis & Intrusion Detection Tools:
  - tcpdump, synsniff, NetRanger, NOCOL, NFR, RealSecure, Shadow
- Security Management and Improvement Tools:
  - crack, localmail, smrsh, logdaemon, npasswd, op, passwd+, S4-kit, sfingerd, sudo, swatch, watcher, wuftpd, LPRng

- Firewall, Proxy amd Filtering Tools:
    - fwtk, ipfilter, ipfirewall, portmap v3, SOCKS, tcp_wrappers, smapd
- Network-Based Auditing Tools:
    - nmap, nessus, SATAN, Safesuite
- Encryption Tools:
    - md5, md5check, PGP, rpem, UFC-crypt
- One-Time Password Tools:
    - OPIE, S/Key
- Secure Remote Access and Authorization Tools:
- RADIUS, TACACS+, SSL, SSH, Kerberos

As this list would show, there are many diverging viewpoints, approaches, and methodologies that have given rise to a diverse set of solutions to some of the most pressing security problems. It is reasonable to assume that the best course of action would be for the government, industry and other security experts to work together to develop industry standard security solutions.

Interoperability is not limited to security issues alone. It is a pervasive problem, and undoubtedly the single most pressing issue that needs to be addressed if electronic commerce is to live up to its full potential. For electronic commerce to really succeed, interoperability must exist (5):

- Between technologies
- Between applications
- Between companies (especially between the e-commerce sites of complementary companies)
- Between markets
- Between countries

Furthermore, interoperability must exist with legacy systems. As Galvin points out (5) interoperability is not just about technology and is one of the most critical barriers facing electronic commerce.

Trust and Risk

In all the surveys done by CommerceNet (5), there is not one issue that appears more often than trust and risk. “Trust is the grease in the wheel s of commerce,” says Professor Michael Rappa. Customers new to e-commerce worry about the integrity of seller organizations, merchants new to virtual marketing worry about the legitimacy of buyers and the validity of the payment of the goods and services, and so on and so forth. Yet, millions have come together in electronic market places such as eBay and successfully conduct business. EBay’s Safe Harbor site is a very good example of enforcing trust.

Trusted third parties are often used to provide the “seal of approval.” These include TRUSTe and WebTrust. Another approach, especially in large transactions, is the use of an escrow service. Yet another approach to solving this problem is the architecture for Public-Key

Infrastructure (PKI) by the Open Group, one of whose required services is the “establishment of domains of trust and governance.”

CONCLUSION

Digital enterprises can be managed more securely, and are being managed more securely than at any time in its short history. The magnitude of network security threats is large but it has not shunted the growth of virtual markets. With interoperability, a coordinated effort on the part of the key solution providers, and better overall security awareness in the design, implementation and operation of the computer systems, businesses ought to be able to more than keep pace with the criminals, terrorists, unethical businesses and customers.

REFERENCES

1. Stephen Burns (2002). Unique Characteristics of E-commerce Technologies and their effects upon Payment Systems, http://rr.sans.org/ecommerce/payment.php

2. Center for Internet Security (2001). The "Top Twenty" automated scanning tool, http://www.cisecurity.org/scanning_tool.html

3. CERT Coordination Center (2002). Overview of Attack Trends, http://www.cert.org/archive/pdf/attack_trends.pdf

4. Michael Froomkin (1996). The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon L. Rev. 49, available at http://www.law.miami.edu/~froomkin/articles/trusted.htm

5. James A. Galvin (1998). EC Solutions – State of the Art. http://www. Commerce.net

6. The SANS Institute (2002). The Network Security Roadmap. http://www.sans.org/newlook/publications/roadmap.htm

7. The SANS Institute (2002). The Twenty Most Critical Internet Security Vulnerabilities, Updated Version 2.504, May 2, 2002, http://www.sans.org/top20.htm

8. Timothy J. Shimeall, Casey J. Dunlevy, Phil Williams. (2001) Intelligence Analysis for Internet Security: Ideas, Barriers and Possibilities. CERT Analysis Center, Software Engineering Institute, Carnegie-Mellon University, available from: http://www.cert.org/archive/html/spie.html