INTERNET, INTRANET, AND EXTRANET SECURITY

Alin MUNTEANU
„TIBISCUS" UNIVERSITY OF TIMIŞOARA, FACULTY OF ECONOMICS

Abstract:
Organizations today depend heavily on the Internet, intranets, and their network infrastructures to conduct business. Ensuring the security and integrity of data shared across networks is essential, especially in light of the various regulatory and legislative mandates they must comply with.

Key words: *Internet, Intranet, security*

JEL classifications: *L86, H55, M15*

Organizations strive to implement technical controls to assist in enforcing their security policies; however, under certain circumstances some organizations need to monitor the content of packets entering and leaving their network to ensure they detect leaks of confidential information. At the same time, the enforcement challenges facing them are on the rise, and the need for effective security controls is greater than ever.

Signature - or behavior - based detection and prevention technologies depend on the automated recognition of anomalous conditions: in the first case through signatures and in the second through exceeding a set threshold of deviation from known normal conditions (or baseline).

The prevention of unauthorized disclosure of proprietary or confidential data (information leaks) through conventional technologies (such as intrusion detection or prevention) is difficult to manage.

Signature - based intrusion detection and prevention relies on attack signatures (bit patterns in packet streams); extending that to include words or word patterns that are contained in application files (databases, office productivity documents, portable document files, or any of the numerous file formats in use today) that would be indicative of a leak of information is difficult.

Conventional technology solutions such as identity and access management, security information management, content management systems, and digital rights management – individually or in combination - help organizations control who has access to sensitive data; however, once authorized access is granted, they have little control over how that data is utilized.

Information - handling security policy should have teeth: a strong policy that clearly outlines the information-handling requirements of the organization and mandates disciplinary measures for policy violations is the first step in controlling information leaks through networks. But a policy without the means to enforce it remains ineffective. Limiting the protocols or applications that can be utilized by network users in connections to foreign networks helps organizations reduce the vectors through which sensitive information could be leaked. Placing too many restrictions will, however, impede the business, and organizations need to compromise between security and usability. Once this exercise is complete, and a clear picture of the traffic to be allowed is established, the attention can turn to the mitigation methods for permitted traffic.

- **HTTP/FTP.** Any document types can be uploaded to a Web site that is designed to "accept" attachments (Web-based e-mail, bulletin boards, etc.). Universal resource locater (URL) filtering - which is typically part of the defense arsenal of

companies - can help mitigate this risk. Free Web-based e-mail services are typically classified in the "Web mail" category of URL filtering solutions; thus access to these services can be curtailed by implementing appropriate security controls over Web access (a functionality that is available either in a stand-alone solution or as an add-on to the existing Web caching servers from several vendors). The residual risk will come from uncategorized sites. Denying access to such sites can further reduce the residual risk, but may be deemed unacceptable to the business. Either way, insofar as leak control is concerned, the URL filtering method is binary and lacks granularity.

- **HTTP/SFTP/SSH and other encrypted traffic**. The scenario is similar to the preceding one. Control is binary and lacks granularity. Once access is granted, no further control is possible over content.

- **Peer-to-peer applications.** Risk is best mitigated by preventing the use of such applications. A combination of controls at different layers can be used for maximum effectiveness.

On desktops in Active Directory (AD) environments, group policies can prevent users from installing or running unauthorized applications, including peer-to-peer. On desktops in all Windows environments, desktop security solutions available from several vendors help organizations control desktop usage and prevent the installation or execution of peer-to-peer applications. These can be used stand-alone or in combination with AD group policies in AD environments.

At the network layer, periphery defenses can be configured to block peer-to-peer traffic, with varying degrees of effectiveness.

- **Electronic mail (corporate mail systems).** Technical solutions exist to:

(a) inspect the content of messages and attachments (specific file formats) or

(b) archive all or selected mailboxes.

Encrypted e-mails or attachments would, however, be difficult to inspect with either of these solutions. In the first case, if the business allows it, rules can specify that unrecognized or encrypted file formats be automatically blocked.

- **General controls.** Network forensics solutions that capture and store all (or filtered) traffic (see simplified network diagram) enable the reconstruction and replay of sessions that were previously "recorded," enabling organizations to spot security policy violations. The technology does have limitations though it is expensive and requires expertise to operate effectively.

Furthermore, though encrypted traffic can be recorded "as is," its clear-text content cannot be visualized unless the organization has prior knowledge of the encryption algorithms and associated keys, which is rarely the case. HTTPs and SSH are common methods of transferring data in encrypted form.

In addition, archive tools (such as WinZip) now offer built-in strong symmetrical encryption capabilities (up to 256-bit advanced encryption standard [AES]). Any documents encrypted with a strong key that is transferred to the addressee out-of-band cannot be visualized unless the sender discloses (or is forced to disclose) the encryption method and key used. Things are even more difficult in the case of symmetrical keys that are negotiated online through an asymmetrical key exchange (such as during a Secure Sockets Layer session establishment).

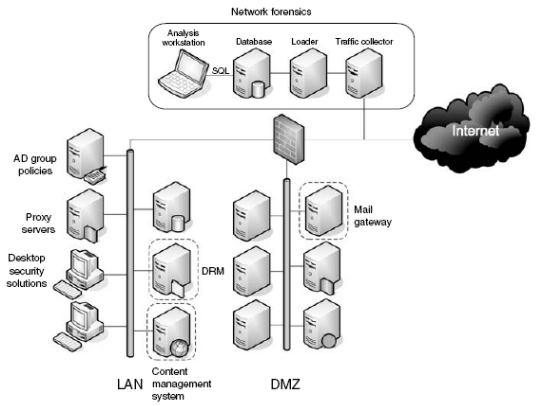

Figure 1. Network Content Filtering

It was only a little more than a decade ago when "the Internet" was not part of most individual's daily vocabulary. Today, the use of the Internet, e-mail, and text messaging is ubiquitous throughout coffee shops, cities, cell phone communications, and the workplace. This medium, despite the lack of inherent security at the network level, has become "trusted" by many to perform daily personal and business operations.

Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication."

Originally, phishing attempts obtained passwords by tricking users into supplying the passwords in response to an e-mail request.

Now, these statements are prevalent across banks, online payment services, and organizations providing E-commerce activity. E-mails have been made to look like they were coming from the Internal Revenue Service (IRS) to obtain tax information to be used in identity theft criminal activities.

Phishing Delivery Mechanisms

Simple Mail Transfer Protocol (SMTP) is the primary avenue of vulnerability exploitation by phishers due to failures within the protocol. In addition to the e-mail communication channel, other methods such as Web pages, messaging services, and Internet Relay Chat (IRC) are increasingly being used to extract personal information. As vulnerabilities are plugged within SMTP over time, other methods of exploitation will emerge, because of the lucrative financial opportunity presented by phishing. Therefore, it is critical that organizations take a proactive stance to reduce consumer fears that their information may be compromised. Organizations whose primary livelihood depends upon the Internet for E-commerce and large banking institutions have been implementing proactive education for consumers and implementing tighter controls for the past several years. Obviously, with the increasing number of phishing attempts previously noted, the breadth of organizations being phished and the type of delivery are expanding.

E-Mail and Spam Delivery Method

This is the most common method of delivery, by which the end user is tricked into clicking on a link or an attachment. The e-mails are meant to look legitimate, complete with the logos of the company and an official looking e-mail address in the "Mail From:" field of the e-mail. Flaws in SMTP permit the "From" address to be spoofed, and the phisher may also put an address in the "RCPT To:" field to direct any responses to the spoofer. When the recipients of the e-mail click on the link included in the e-mail, they are directed to a fraudulent Web site set up by the phisher.

Personal information is collected at the Web site to be used in further the criminal activity. These e-mails look official and use language to sound like they could come from the company.

In fact, the e-mail may be a replica of a similar notice from the organization. There is usually a sense of urgency stated in the e-mail request for a quick response to the e-mail. Some of the e-mails are Hypertext Markup Language (HTML) based to hide the target URL information using different color schemes and substituting letters, such as an I for an L, to direct the user to different sites.

These e-mails are often constructed in an attempt to defeat the antispam filters by inserting random words in a color to match the background of the e-mail so that they would not appear to the end user. Open e-mail relays are also utilized to hide the real source of the e-mail. The URL may point to a different Web site through the use of an escape coded into the HTML. Nonstandard ports specified in the URL may be clues that the phisher's Web site is being hosted on a personal computer (PC) exploited by the hacker earlier.

Although most of the e-mails would direct the unsuspecting end users to a fraudulent site after clicking on the link, some may actually direct them to a real site. In this case, a JavaScript pop-up containing a fake log-in page could be used to store the credentials. Subsequently, the application could forward the credentials to the real application, and the user would be none the wiser.

Although most of the attacks have been through random e-mails sent to people that may or may not have a relationship with the company, some phishers are getting smarter and are performing spear-phishing, which is targeted phishing. In the case of spear-phishing, a group is targeted for their relationship. For example, employee names listed in a Web site directory may be sent a notice from the company's health insurance company or credit union or another firm known to provide services for the company. Additionally, as companies become larger in size and have millions of customers, there is a greater chance that their Web sites contain more information about their organizations in the name of customer service, as well as a greater likelihood that even a random e-mail will connect with someone who has a relationship with the organization.

Web-Based Delivery Method

Web sites are constructed to contain HTML links that are disguised such as in the e-mail scenarios noted earlier. Fake advertising banners with diff erent URLs may be posted to legitimate Web sites, directing traffic to the phisher's Web site. Malicious content embedded within the Web site may then exploit a known vulnerability within the user's browser software and then be used to install a keylogger (monitors keystrokes), screen-grabber (monitors portions of the user's input screen), backdoor (to gain control of the computer for later remote or bootnet access), or other Trojan program.

Keyloggers may be coded to intercept specifi c credential information, such as the log-in information for certain banks. Phishers may establish an online account, use a fake banner pointing to a fake Web site, all with a stolen credit card and other bank information obtained to cover their tracks.

IRC and Instant Messaging Delivery Method

Communication in the instant messaging area makes it possible for the end user to fall victim to the same techniques used in other delivery methods. Embedded dynamic content is permitted in these clients, which can also point to other links that would point to fictitious Web sites.

Trojaned Host Delivery Method

PCs that have been previously compromised may act as a delivery mechanism for sending out phishing e-mails, which makes tracking the originators of the phishing scams very difficult.

Although antivirus software can help with the reduction of the risk of Trojans, it is becoming increasingly difficult. Home users are often tricked into installing software as an upgrade that provides the ability for the PC to be controlled at a later date.

Phishing Attacks

Man in the Middle

In this type of attack, the attackers insert themselves in between the consumer and the real application, capturing the credentials along the way. The end user may have a false sense of security by relying on the HTTPs, as the man-in-the-middle attack could set up a secure communication path between the hacker's server and the customer and subsequently pass the information to the real Web site. While the phisher remains in the middle, all transactions can be monitored. This can be accomplished by multiple methods, including transparent proxies, Domain Name System (DNS) compromises, URL obfuscation, and changing the browser proxy configuration. Transparent proxies reside on the network segment on the way to the real Web site, such as a corporate gateway or an intermediary Internet Service Provider (ISP). Outbound traffic can then be forced through the proxies, which would deliver the information back to the consumer unnoticed. DNS caches can also be poisoned to point certain domain names to different Internet Protocol (IP) addresses controlled by the phisher. The cache within a network firewall could redirect the packets bound for the real Web site to that of the attackers. The DNS server itself could also be compromised, as well as the local host's file on the user's PC ahead of receipt of the phishing e-mail.

The browser proxy can also be overridden to proxy the traffic for, say, the HTTP port, to a proxy server. This involves changes on the client side and may be noticed by the end user by reviewing the setup. Many users, however, would not be actively looking at those controls and there is a high likelihood that the controls would be named something that would sound technical, making noticing them difficult.

Man-in-the-middle attacks are particularly troublesome, as the end users think they are interacting with a trusted entity when executing transactions with a trusted bank, online shopping storefront, or service provider; meanwhile, their identity is being captured for later exploitation.

URL Obfuscation Attacks

URL obfuscation involves minor changes to the URL and directing the consumer to a different Web site. There are multiple techniques for changing the URL to make it appear as though the user is being directed to a normal Web site.

The first technique leverages bad domain names to appear like the real host, although in reality these are domain names that are registered by the phisher. For example, a firm with the name Mybrokerage.com may have a transaction site named http://onlinetrading.mybrokerage.com. The phisher could set up a fraudulent server using one of the following names:

http://mybrokerage.onlinetrading.com
http://onlinetrading.mybrokerage.com.ch
http://onlinetrading.mybrokerage.securesite.com
http://onlinetrading.mybrokerage.com
http://onlinetrading.mybrokeráge.com

In the foregoing examples, the name was varied, extensions were added, words were misspelled, or different character sets were used. To the average user, the URL looks like a valid site.

There are also third-party services that shorten URLs to make entry easier. These sites map other URLs to their shorter ones to make entry by the user easier. These sites can also be utilized by phishers to hide the real site.

Friendly log-in URLs are another method by which the user can be deceived. URLs can include authentication information, in the format of URL://username:password@hostname/path. To trick the end user, information would be placed in the username and password fields to resemble the company Web site while directing the user to the host-name Web site, which is managed by the phisher.

In the preceding example, the URL may look like http://mybrokerage.com: etransaction@fakephishersite.com/fagephisherpage.htm. Several browsers have dropped support of this method of authentication due to the success it has had in the past with phishers.

The host name can also be obfuscated by replacing it with the IP address of the fraudulent Web site. Another technique is the use of alternate character set support, which is supported by many browsers and e-mail clients. Escape encoding, Unicode encoding, inappropriate UTF-8 (8-bit UCS/Unicode Transformation Format or variable length encoding for unicode) encoding, and multiple encoding are all techniques for representing the characters in different ways.

Other Attacks

Cross-site scripting attacks are another method by which the attacker can utilize poorly written company Web site code to insert an arbitrary URL in the returned page. Instead of returning the expected page for the application, the attacker returns a page that is under the control of their external server.

Preset session attacks make use of a preset session ID, which is delivered in the phishing e-mail. The attacker then polls the server continuously, failing as the session ID is not valid. When the end user authenticates using the session ID, the application Web server will allow any connection using the session ID to access the restricted content, including the attempts by the attacker.

Each of these methods for obfuscation can be combined with others, making it even more difficult to identify when the URL is being used to direct traffic to a fraudulent Web site.

Educating Consumers

Educating consumers about the dangers of phishing is a delicate balance. On the one hand, consumers need to be vigilant in not responding to e-mails with links to sites requesting their personal information; on the other hand, consumers should not be afraid to participate in online commerce and use e-mail wisely. Many banking and E-commerce sites have included information on phishing on their Web sites in an eff ort to reduce the risks.

The key points for reduce fraud by phishing included the following:

- if you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And do not click on the link in the message, either.
- area codes can mislead (and may not be in your area due to Voice-over-IP technology).
- use antivirus and antispyware softwares, as well as a firewall, and update them all.
- do not e-mail personal or financial information.

- review credit card and bank account statements as soon as you receive them.

- be cautious about opening any attachment or downloading any file from e-mails.

- forward spam that is phishing for information to the bank or company that was impersonated with the e-mail.

Conclusion

The technology designed to protect highly sensitive data from leaks through networks is complex and expensive in terms of acquisition and ongoing operation costs, and its effectiveness is dependent upon what type of traffic an organization allows to permeate through its periphery.

Encryption is a double-edged sword: it helps in ensuring the confidentiality of information traveling across networks, but it also prevents organizations from maintaining the visibility of what sort of information is leaving their networks.

To combat information leaks effectively through networks, organizations must follow the continuous information security plan cycle: assess, design, implement, educate, monitor, and correct.

The security personnel's awareness and understanding of vectors that could be used by ill-intentioned persons to sneak sensitive or confidential information out of a network is key to mitigating its risk.

Bibliography:

[1] Hulme G., "Under Attack", Information Week, July 5, 2004

[2] Munteanu A., "E-Commerce Security Strategies", Analele Universitatii din Oradea-Stiinte Economice, tom XVI, vol.2, 2007, pag. 855-858

[3] Smith, M. K. (2001) "Theories of action, double-loop learning and organizational learning", www.infed.org/argyris.htm

[4] The SANS School Store, "The SANS Security Policy Project", February 6, 2006, http://www.sans.org/resources/policies/

[5] Terena's Guide to Network Resource Tools, "Smart Card Types", February 6, 2006, http://gnrt.terena.nl/content.php?section_id=131

[6] Bezakova, I.; Pashko, O.; Surendran, D., "Smart Card Technology and Security", February 6, 2006, http://people.cs. uchicago.edu/~dinoj/smartcard/security.html