Vigilinx
Digital Security Solutions

Vigilinx, Inc. – Security Trends 2002/2003

At the end of each year our analysts meet to discuss the trends of the previous year and what those trends may mean in the year ahead. This paper contains our assessment of the important security trends in 2002, as well as some predictions about what the security community will experience in 2003.

TOPICS

Insecure Software
Scripting Language
Access/Authentication
Open Source
Worms
Backdoor Trojans
Wireless
Cybercrime
DMCA/Legal
Cyberterrorism

Insecure Software

The top security problems in 2002 involved software vulnerabilities as opposed to malicious code or denial of service attacks. A large number of the vulnerabilities reported during the last year involved buffer overflows, improperly handled user input, and poorly implemented authorization and access controls.

In February 2002, researchers reported that almost half of the e-business applications they studied suffered from exploitable security flaws. The majority of these problems occurred because software developers continue to marginalize security in the design and development process.

As the chorus of complaints from users grew, security professionals began asking software developers to renew their commitment to designing and developing safer products to eliminate common exploits. Particularly at the end of 2002, many were questioning vendors' commitment to security, as vulnerabilities continued to plague certain products. This prompted several major software vendors, most notably Microsoft and its Trustworthy Computing Initiative, to initiate code audits of their products and begin to incorporate security in their development programs.

In addition to vendors' efforts to secure their own software, several security organizations, including Sun Microsystems and RSA, responded with application security products that help protect vulnerable software. While the preferred solution is to create secure applications, application security products, many of which are currently only in their earliest versions, are designed to prevent exploits by restricting the applications' functions. During the next year these products are expected to improve and become a key feature of a defense-in-depth security strategy.

Scripting Language

Many scripting language vulnerabilities were discovered in 2002, ranging from information disclosure vulnerabilities to buffer overflows issues that lead to a remote compromise. The script language with the most security issues in 2002 was PHP (Personal Home Page or PHP Hypertext Preprocessor).

Others that suffered security problems in 2002 are Perl and Common Gateway Interface (CGI). CGI connects external gateway programs to information servers. Many CGIs are used in shopping cart programs when purchasing goods on the Internet. There are other uses for CGIs, most of which involve submitting information to servers. For this reason, many CGI script vulnerabilities allow attackers to gain sensitive information. This information may lead to a simple user compromise or a total system compromise. These are used in many non-commercial, open-source or free software applications. The applications or scripts are often designed by inexperienced developers and released to the public without proper security engineering and testing. As is the case with most programming languages, the vulnerabilities are more often found in the way the application is coded rather than in the language itself.

PHP, a popular scripting language project overseen by the Apache Software Foundation, is used on nearly 10 million domains. PHP scripts can be embedded in HTML pages used in web development. Many of the vulnerabilities in PHP applications allow attackers to obtain sensitive information, such as other users' cookie files. Other vulnerabilities allow more malicious actions, such as the execution of arbitrary code or remote compromises.

Perl, a popular open-source programming language that originates from C and a few other languages, is used in many web applications. Most of its security vulnerabilities are in the Perl code for web applications. Perl contains many of the same vulnerabilities present in other languages.

Most of the vulnerabilities in these programming languages are caused by the manner in which the language is implemented. The very thing that makes these languages and scripts so popular, ease of use, may also be their downfall. These languages and scripts are fairly easy to learn and implement, which makes them popular among new Internet developers.

Because of the increasing popularity of these languages, inexperienced programmers are releasing applications and scripts before they pass the proper security checks. Users are advised to implement applications only after they have been thoroughly tested. Users may also want to have the software audited by their software development department or another department that is capable of auditing code. With the use of these languages increasing, users can expect more vulnerabilities to stem from them in the coming year.

Access/Authentication

A major security issue in 2002 that will become more complex in 2003 involves authentication and access controls. Security managers face a difficult environment in which more users require remote access to more information. At the same time, they have to stringently authenticate users and control access to more data and e-business processes.

Improvements in search and data-mining capabilities, and the growing use of credit cards, countered by privacy, liability and regulatory requirements, means security managers can no longer rely upon usernames and passwords, which are far too vulnerable to compromise, and difficult to implement to meet the security needs of complex environments. In response to this need, three major smart card programs emerged in 2002. The Department of Defense Common Access Card (CAC), Europay-MasterCard-Visa, and the American Express Blue Card have worked out their bugs and are maturing into highly reliable methods for authentication, controlling access and accounting.

The smart card is designed around an embedded chip, a magnetic strip, and a barcode for use with multiple current systems. The smart card chip uses a two-factor identification and authentication schema, combining a card reader and a PIN. The chip also includes on-card encryption and certificate capabilities. Recently compiled statistics show that fraudulent and criminal use of the card is near 0.07 percent, well below that of skyrocketing identity theft and credit card fraud statistics. Now that these pioneer Java-based and MULTOS card programs have achieved initial success, the expansion of smart card programs and products is probable in 2003.

Open Source

Largely in response to tightening budgets as much as intensifying security concerns, 2002 also saw a shift in use from proprietary products to open-source software. The debate over the security of open-source software, including comparisons of Windows and Linux vulnerabilities and overall ROI, has not slowed the increase in the number of businesses and government organizations adopting Linux-based systems in their data centers. Several major vendors are now providing Linux solutions and developing software for these platforms.

Although Linux is not expected to move to the desktop as quickly, its use in the server market is expected to continue to grow through 2003. Two key factors will affect the growing presence of Linux systems. First, the developing vendors must remain true to the open-source concept and make their code available to users and other developers. Administrators and security professionals are far more confident in a product when they can examine the source code and technical details, and they have greater flexibility when configuring and securing the system. The second factor is whether vendors develop proprietary Linux implementations and products, referred to as forking, as many vendors did when developing their Unix products. Forking complicates and restricts the use of available products, and only increases dependence on the vendors who supply patches. This product shift will present several challenges to security professionals.

The security of open-source products is quite different from that of proprietary products. First, more detailed technical information is available from multiple sources and the release of vulnerabilities and fixes from open-source products occurs more rapidly. Security managers should review their security policies and procedures, and adjust them to the growing presence of open-source products in 2003.

Worms

In 2002, there was a significant decrease in the number of dangerous, quick propagating worms. In 2001, worms such as *Magistr, Sadmind, CodeRed, Sircam, Nimda, SQL Server worm, Badtrans.B* and *Klez* hit the network and fooled users into executing their malicious payloads. Additional information about these worms is available in Vigilinx Alerts 1958, 2184, 2446, 2450, 2664, 2853, 2859 and 2790.

Some of the worms exploited vulnerabilities. *CodeRed, Sadmind* and *Nimda* attacked vulnerabilities in Microsoft IIS. The *SQL Server worm* took advantage of the blank administrator password misconfiguration in SQL Server. Some of the worms are still circulating. This year, a variant of *Klez, Klez.H*, emerged with a Christmas theme. Of the 10 million viruses that MessageLabs captured in 2002, almost half were related to *Klez*.

In 2002, major worms included *MyLife* (Vigilinx Alerts 3426 and 3504), *Scalper* (Vigilinx Alert 4090), *Slapper* (Vigilinx Alert 4629) and *Bugbear* (Vigilinx Alert 4741). *MyLife* spawned several potentially destructive variants. *Scalper* exploited the Apache Chunked Encoding Vulnerability (Vigilinx Alert 4014). *Slapper* exploited the OpenSSL vulnerability (Vigilinx Alert 4296). *Bugbear* was quite popular, especially with virus writers, so much so that they were using its familiarity to fool users into downloading malicious code by advertising it as a *BugBear* removal tool. Virus writers have favored script viruses such as *LoveLetter*. But in 2002, almost 90 percent of the viruses reported involved Win32 executable files. Several hundred new viruses were also in circulation in 2002. More than 78,000 viruses are now in existence.

There were four major worms in 2002 and 11 in the previous year. The significant decrease is puzzling. The possibility exists that users are more educated, can more readily identify malicious code, and do not open suspicious e-mail. Another possibility is that more users are installing antivirus software. ISPs are continuing to install filters on web mail to block potentially malicious e-mail. In any case, there has not been a drop in the overall number of worms as much as in the number of users who have fallen victim to the worms and caused them to spread.

The most destructive and fast-moving worms exploited unpatched vulnerabilities in the most popular products. Virus writers continue to use Microsoft Security Bulletin MS01-020, which provides information about how to automatically execute attachments in a user’s Preview Pane. There were plenty of major vulnerabilities discovered this year that virus authors could have used to spread malicious code, including several vulnerabilities in Internet Explorer. It is only a matter of time before more vulnerabilities are used to spread a destructive worm.

Backdoor Trojans

Unfortunately, 2002 saw an increase in the number of backdoor trojans, which are not as easy to detect as worms and can lie on a user's computer undetected for some time.

Most trojans do not propagate independently through e-mail, but are accidentally downloaded from malicious web sites and through peer-to-peer file sharing applications such as KaZaA. Even trusted open-source packages such as Sendmail, OpenSSH and *tcpdump/libpcap* were compromised by backdoor trojans this year. Infections can be greatly reduced by implementing safe browsing habits, using PGP keys and verifying the MD5 checksums on files.

The increase in the number of backdoor trojans while the number of worms decreased across the same time frame may be only a coincidence. However, it could be that users are getting smarter and virus writers are trying to find better ways to spread their malicious code. Vigilinx issued a total of 2109 Alerts in 2002, 635 of which involved malicious code. Users should always keep antivirus software updated, deploy firewalls and use caution when handling e-mail. Notify an administrator of any irregular activity and browse only trusted sites.

Wireless

Wireless networks are becoming more integrated in America's communications system. The convenience and ease of use of wireless networks makes them popular with home and office users. The common wireless interface is 802.11b. Wireless networks are naturally insecure, sending information through the air unencrypted, allowing any user with a receiver to capture it. Wireless devices are required to arrive with built-in Wired Equivalent Privacy (WEP). This is the main option users rely on to keep their information safe from malicious listeners.

WEP contains flaws that can allow an attacker to bypass the encryption and obtain any sensitive information on the network. Standard use leaves little to fear because one to six million packets must be intercepted before the WEP key can be broken. Changing a WEP key every few weeks can help ensure that it remains unbroken. Solutions for these problems are being developed. To make any solution work with previously released versions, TKIP (Temporal Key Integrity Protocol) is being used. This protocol uses a longer initialization vector, increases randomness, and uses a master key to develop other keys.

Another standard is the EAP (Extensible Authentication Protocol), which is a middle protocol placed between the access point and the WLAN or LAN. Recently, a new form of protection was introduced as a temporary replacement for WEP until the IEEE ratifies the new proposed standard. The replacement is called Wi-Fi Protected Access, or WPA. Introduced in November 2002 by the Wi-Fi Alliance, WPA is expected to serve as the next interim fix until a permanent solution is adopted. WPA advances the effort to secure wireless networks. Consumers may be introduced to this technology in the coming year through upgraded firmware and devices.

Cybercrime

Pursuing cybercriminals became a major trend in 2002, and that trend will continue into 2003. As federal and international legislative bodies and courts attempt to address the legal issues surrounding cyberspace, incident response and forensics have become key issues for security managers. As a regulatory and liability issue, and to support their own prevention and prosecution of crime, administrators now must respond to incidents in a manner that both defends the organization and preserves evidence.

While quality incident response and forensics has previously been limited to a small number of highly skilled specialists, the development and availability of specialized security products, and the training of more security administrators in these areas, should continue to grow in 2003. Some of these developments can be attributed to the aftermath of the 9/11 attacks, but the draft National Strategy to Secure Cyberspace will probably languish in Washington for the majority of 2003 and, therefore, will have little overall impact on real network security initiatives this year. In any case, whether the cyberstrategy will actually strengthen the nation's IT infrastructure is still in doubt. Many IT organizations are opposed to the establishment of new standards bodies and federal assessment of ISPs. Many fear costly new regulations.

While the rules governing the legal jurisdiction of cyberactivity begin to evolve, criminal use of the Internet is developing at a much faster rate. Criminals are exploiting gaping holes in the legal system – a legal system that is finding it difficult to keep pace with new technology. Cybercriminals are finding new ways to exploit technology to reap their illicit profits, but they usually use tried and true methods. Fraud and theft are two of the most popular incarnations of cybercrime.

There have been numerous reports of cybercriminals stealing the identity of individuals and engaging in further criminal activity in the guise of the victim. The online auction house eBay has repeatedly been the vehicle used by cybercriminals to conduct online fraud and identity theft.

Other online auction and commerce sites have also been used to perpetrate online fraud and identity theft. The Internet Fraud Complaint Center, run by the FBI, received almost 50,000 complaints in 2001, and that number is increasing each year. According to the IFCC, only one in 10 incidents of fraud are reported. That leaves close to 450,000 unreported online crimes involving fraud in 2001.

The figures for 2002, when released, should be even more alarming and continue to show a steady increase in interest in online crime, not just by script kiddies, but also by professional hackers, organized crime entities, and possibly even terror groups seeking funding for their offline activities. It has been said that online crime is more lucrative than the narcotics trade. That temptation may be too much to resist for criminals who may now move their efforts to the Internet.

Another form of cybercrime that will continue into the next year and beyond is malicious activity by trusted users. Recently, a former employee of a major financial services company installed a piece of malicious code across the internal network that had the potential to cause significant damage to the network. The former employee hoped that the damage caused by the malicious code would generate enough publicity to cause the stock price to drop drastically. The attacker arranged a series of stock market transactions that would enable him to make a significant profit when the stock bottomed out.

The malicious code executed as planned, but the damage failed to generate the desired media attention, rendering the former employee's ploy useless. He was eventually identified and charged with one count of federal securities fraud and one count of computer-based fraud. If the extent of the damages had been more serious, the former employee might have faced cyberterrorism charges. As this type of activity becomes more prevalent, expect to see a growth in Internet insurance offerings designed to help organizations cope with security and liability issues.

The attack on the 13 DNS root servers this year was also interesting, and may have been a reconnaissance or intelligence-gathering operation. Although it is remotely possible, it would be extremely difficult to compromise all 13 root servers. Even if a major DNS compromise were accomplished, it probably would cause no more difficulty than that caused by a major snowstorm on the Eastern seaboard.

DMCA/Legal

The realm of cyberspace continued to become an integral part of everyday life in 2002, but regulating it proved to be difficult.

The global reach of the Internet is creating many difficulties in determining jurisdiction for a given cybercrime. This question was brought to center stage early in 2001 when Adobe Systems filed charges against ElcomSoft, a Russian software developer. ElcomSoft built an application that bypassed the copy protection mechanism Adobe uses to protect its eBook product line from unauthorized duplication. The application directly violated provisions of the Digital Millennium Copyright Act (DMCA).

Even though the process of developing, storing and selling the application took place in Russia, one of the primary programmers, Dmitri Sklyarov, was arrested for criminal violation of the DCMA when he arrived in the United States for a hacker conference. Sklyarov was eventually released and permitted to return to Russia, but only with the agreement that he would return to the U.S. to testify in the case against his employer.

The case against ElcomSoft and Sklyarov was recently concluded in their favor, but it raised interesting questions about establishing jurisdiction. These questions will not be resolved soon and will continue to play a significant roll in the development of cyberspace. International regulation similar to that governing telecommunications and trade will probably evolve to regulate cyberactivity and jurisdictional issues.

Another instance of jurisdictional problems involved *Barron's* magazine and a businessman in Australia. Barron's magazine, a Dow Jones publication, published an online article about the businessman, which he perceived to be defamatory. Although the article was published in the United States, the businessman filed a defamation of character suit against Dow Jones in an Australian court. The Australian court ruled against Dow Jones' motion to move the case to the U.S. This event set a dangerous precedent for other online publishers who must now carefully consider the laws anywhere their content may be viewed.

However, a Connecticut court recently ruled that a man in Virginia cannot sue an organization in Connecticut for publishing what he considered to be an inflammatory article. If the courts within the U.S. are already struggling with intranational jurisdictional issues, how will they handle international issues?

Cyberterrorism

Cyberterrorism continues to evolve into a more credible threat. Immediately following the events of 9/11, most of the focus was correctly placed on the physical aspects of terrorism, but the electronic aspects have gained more attention as well. In November 2002, an unclassified CIA report was released that listed cyberterrorism as a legitimate threat. Its inclusion in the CIA report gives cyberterrorism new legitimacy as a threat to the United States, its industry and economy. Vigilinx Alerts 3595, 4290 and 4990 provide additional analysis concerning the threat of cyberterrorism.

Unfortunately, cyberterrorism is a new threat vector and it is uncertain how it will be used. Initially, it will probably be used as a secondary attack in support of a physical attack. If cyberterrorism proves its worth as a supporting attack, terrorists could begin to use it exclusively in individual terrorist attacks or as the primary effort in a combined physical and cyberattack.