



Security views

Malware update

Numerous new worms have not unexpectedly surfaced recently. The Windows system-targeting Sasser worm was the most disruptive and prolific—it adversely affected operations at hospitals, post offices, airlines, and in other settings. Sasser exploits a recent buffer overflow vulnerability in the *lsass.exe* program (see Microsoft Security Bulletin MS04-011) in these systems, enabling an attacker or malicious program to run unauthorized code on victim systems with superuser privileges that result in total control of these systems. Sasser spreads by scanning randomly selected IP addresses for vulnerable systems and then sending excessive input to such systems to infect them by downloading an executable file. Sasser also changes a value in each infected system's Registry so that this worm starts every time a system boots. Several variants of this worm appeared in a few weeks. The self-admitted author of this worm was recently arrested—see the next section of *Security Views*.

Variants of another Windows-targeting worm, the Bobax worm, also recently spread itself over the Internet by capitalizing upon the same vulnerability that Sasser exploits. It copies itself into vulnerable systems and makes several Registry changes to cause the worm code to run every time an infected system boots. Next Bobax tries to delete every file in the %temp% folder that begins with “.” and then inserts itself in this directory as a file with a .dll extension. Bobax also inserts itself into *Explorer.exe*, something that may cause the Windows Explorer to crash. This worm also tries to connect to a remote Web server to record that it has infected another system. The Web server's response directs the victim system to send spam, to download and execute programs, to transmit information about itself, or to start or stop

scanning designated IP addresses. When it scans remote computers, Bobax determines whether they are Windows XP systems by trying to make a connection to TCP port 5000. If successful in connecting to this port, Bobax sends input to the system to TCP port 445 in an attempt to exploit the *lsass.exe* vulnerability. If it is able to do so, this worm creates an HTTP (Hypertext Transfer Protocol) connection from the victim system to the system that launched the attack to push the worm code into the victim. Finally, Bobax opens several randomly chosen ports on the victim so that remote connections can be made to this system.

Unlike Sasser and Bobax, the recent Wallon worm is an email-borne worm. It functions differently from most email-borne worms, however, in that this worm does not embed itself in an email attachment. Wallon instead simply sends a link that appears to be to the Yahoo site in an HTML (Hypertext Markup Language) message. If the message recipient clicks on the link, the resulting HTTP connection is redirected to a Web page that downloads an HTML file that contains an encrypted link to yet another page. This additional page is actually the one that is used maliciously; it exploits a vulnerability in object data that results in the downloading and execution of a file that downloads various components of this worm. These components include a binary file that replaces the executable for the Windows Media Player in addition to others, including the worm executable itself. Wallon changes the Internet Explorer's startup search page and then checks the value of a certain Registry key to determine whether a certain entry is present. If it is, it connects ten times to a certain Web site after an initial delay of 5 h; if it is not, it creates the Registry key. Wallon also attempts to open a Windows Address Book file; if successful in doing so, it creates a mail engine it uses to spew messages to the addresses it finds. Finally, it sends

a message to a particular email address to notify the worm's author of every infected system.

All of the major recent worms have once again targeted Windows systems. Some, such as Sasser, were particularly adept at infecting systems, with possibly as many as two million systems worldwide succumbing to this worm and some still falling prey to it. I seriously wonder how much longer many organizations and the user community at large will be willing to tolerate massive worm outbreaks such as those by Sasser, Bobax and Wallon (in addition to others). One of two outcomes is likely to eventually happen—either people will quit using Windows systems (or drastically curtail their use of these systems) or they will start ensuring that their systems have the latest hotfixes and anti-virus software updates. Keeping up with hotfixes is a particularly difficult challenge. For one thing, the sheer number of hotfixes that are released necessitates considerable effort in keeping up with hotfixes. Additionally, Windows Update, a built-in mechanism for automatically downloading hotfixes in Windows systems, is available only in certain Windows systems and works only for hotfixes that Microsoft deems “critical.” Interestingly, Service Pack 2 (SP2) for Windows XP will have capabilities that prevent outcomes such as buffer overflows, thereby protecting XP systems from the kinds of attacks that Sasser and Bobax launched. I predict, however, that authors of malware will quickly devise new methods that bypass many of SP2's features.

Update on the war against cybercrime

German police have been particularly busy recently in the war against cybercrime. Sven Jaschan of Rotenburg, Germany, has been arrested on charges of computer sabotage. Jaschan, an 18-year-old high school student, has according to German police, confessed to being the author of the Sasser worm after law enforcement authorities-tipped off by informants-seized his computer and reportedly found the worm's source code on it. He faces up to five years in prison. Jaschan may also have created several versions of the NetSky worm. German police have also arrested a 21-year-old man from Baden-Wuerttemberg who has reportedly confessed to being the author of the Phatbot worm. According to German law enforcement authorities, several others may have been complicit with the suspect in authoring this worm as well as possibly other worms.

Robert J. Murphy of South Carolina was arrested on 26 counts of using a computing system to

electronically stalk and harass Joelle Ligon of Seattle, Washington. Murphy is the first to be charged with violating an amendment to a US telecommunications law that forbids using methods such as electronic mail to send obscene information. Ligon pled innocent in US District Court; he remains free after posting USD 50,000 bail. Murphy is accused of flooding Ligon and those with whom she worked with sexually explicit and obscene messages and images, even after she changed from one job to another in different states. Ligon stated that she at first ignored what Murphy sent her, but she later started saving everything to collect legal evidence. The FBI, US Attorney's Office and King County prosecutors worked with Ligon to bring the case to prosecution. The US government maintained the right to examine Murphy's computer until the trial begins. Murphy could face up to two years of prison time for each count. Ligon's efforts have been a major catalyst for a recently passed law forbidding electronic stalking in the state of Washington.

A 21-year-old UK man is the first in his country to face charges of perpetrating a phishing scheme. The man, an unemployed person from Lytham St Anne's, Lancashire, was arrested after a National Hi-Tech Crime Unit investigation that was triggered by a complaint by Smile, an Internet bank. The man, whose identity has not yet been released, was free on bail while his computers underwent a thorough analysis to obtain potential evidence. A law enforcement spokesperson said that the man is probably not part of any organized crime ring; if anything, he instead allegedly engaged in the phishing scheme to imitate others who had perpetrated similar schemes. Meanwhile, the UK's Association for Payment Clearing Services (APACS) issued a warning to bank customers that a rash of phishing schemes is likely to occur in the near future.

A Texas federal court judge has given Zachary Hill a sentence of up to 46 months in prison for his participation in a phishing ploy. Hill, 20 years old, obtained nearly 500 credit card numbers by sending messages that appeared to be from AOL and PayPal notifying people that their accounts had expired. These messages directed recipients to type their card numbers into fake Web pages. Hill then gleaned the card numbers that were entered and used them to run up charges totaling almost USD 50,000.

A Vietnamese computer engineering student at the National University of Singapore has pleaded guilty to computer misuse charges in Singapore for embedding a keystroke capturing program in a game. Several of his friends, as well as others, unknowingly downloaded this program. He captured passwords and user IDs using the information

he obtained from one machine to steal money from another student. Nguyen Van Phi Hung may receive a fine of up to SGD 50,000 and up to ten years in prison for three of the four charges against him. The fourth charge may result in a fine of SGD 10,000 and up to three years imprisonment.

Benjamin Stark of Florida has admitted that he gained access to 11 US government and private sector networks. The 22-year-old Stark conceded that he had worked in complicity with a partner; collectively they referred to themselves as "The Deceptive Duo." This team took credit for defacing US government Web sites; messages on defaced sites implored the US government to deal with critical infrastructure protection issues. Stark also faces charges for allegedly selling stolen credit card numbers to an undercover FBI agent in a chat room several years ago. Stark, who faces between 24 to 36 months in prison, struck a plea bargain with prosecutors and will be sentenced in September.

The accused, self-confessed and/or convicted cybercriminals mentioned in these news items were arrested on a wide variety of charges. Cybercrime has diversified considerably over the past years; it appears that law enforcement is recognizing and dealing with its new manifestations in a most admirable manner. The recent arrests of several self-admitted worm authors in Germany are particularly intriguing. Given that there are so many Internet users in such a large number of countries around the world, tracking down individuals who have written and released worms must be a particularly difficult task. As the news of worm authors and their accomplices being identified and charged by law enforcement circulates, other would-be worm authors are likely to be deterred from creating and releasing such malicious code. Microsoft's rewards for informants who identify worm authors may ultimately help, as several individuals are likely to receive reward money from Microsoft for having provided information in the Jaschan case, for example. Finally, at least some of the many law enforcement agencies appear to be cooperating with each other, as evidenced by the fact that the arrest of Jaschan resulted from cooperative efforts by the US Secret Service, the FBI, and the German Federal Police.

Electronic voting system security still under fire

According to a group of security researchers, the electronic voting systems that nearly 30% of voters will use in the upcoming US Presidential election

have significant security-related flaws. In a recent testimony before the US Election Assistance Commission, these researchers asserted that it would be impossible to secure the large and complex 50,000 lines of computer code that runs on top of tens of millions of lines of operating system code. Somebody with access to the code base, in particular, any vendor, could readily fix the outcome of any election. Furthermore, the researchers asserted that there would be no way for election officials to guarantee that voting system software is free of malicious code that alerts election results. Without voter-verifiable paper receipts, the 50 million Americans who use electronic voting systems this fall will have no way of knowing if their votes were tallied properly. The end process may also be severely flawed. In a recent test, when the voting areas closed, memory cards were removed from some of the voting systems and then were inserted into one system for transmission via modem to back-end servers. A weak encryption algorithm was used and the key was hard-wired to all of the systems; there was no encryption for any transmissions to the back-end server. According to the researchers, registration databases additionally contain huge numbers of errors—a problem that led to between 1.5 million and 3 million votes not counting during the 2000 US Presidential election. Several vendors have countered that any product changes should be based on risk assessments, not solely because vulnerabilities exist, and electronic tampering with the voting systems would require a long-term commitment by motivated attackers.

Ireland's Prime Minister Bertie Ahearn requested an independent analysis of a planned electronic voting system after skeptics expressed doubts regarding its reliability and accuracy. The Ireland Commission on Electronic Voting determined that despite the many potential benefits of electronic voting, the validity and secrecy of the proposed system have not been proven. They have recommended that the Irish government not deploy the system until more rigorous testing on a stable version of the product can be conducted. In their report, the Commission propounded that there must be a final, definitive version of all hardware and software components that have been subjected to a complete, independent review as well as intense testing. The Commission also advises validity. Furthermore, the Commission asserted that as modifications to the system occur, each new software release should be analyzed and thoroughly tested before it can be deemed to be valid for use in actual elections.

I am still far from comfortable with what is occurring in the electronic voting arena, especially

in the US Security experts such as Dr. Avi Rubin of Johns Hopkins University have carefully evaluated electronic voting systems. Virtually no independent expert has to the best of my knowledge endorsed the security of such systems, yet vendors such as Diebold have typically deployed flimsy strategies such as simply questioning the validity of experts' findings rather than addressing the security-related concerns that have surfaced. Rushing into electronic voting, something the US appears to have done, thus seems incredibly unwise. It is comforting, therefore, to see that countries such as Ireland are taking a more cautious stance concerning the use of electronic voting systems.

UK parliament re-evaluates cybercrime legislation

The UK Parliament All-Party Internet Group (APIG) has started re-evaluating provisions of the UK's cybercrime legislation. Members of APIG have recognized that the Computer Misuse Act (CMA) that went into effect in 1990 needs to be updated to cover the types of Internet and other network attacks that occur today. The APIG, for instance, is worried that existing legislation may not cover attacks such as denial-of-service (DoS) attacks. These attacks are commonplace today, but they were relatively rare when the CMA first went into effect. The APIG wants to integrate IT industry viewpoints into what will ultimately be a revised version of this legislation. Other issues the APIG is pondering include whether the CMA should be changed to come into accordance with certain provisions of the UK's treaties with other countries and whether the penalties that the CMA prescribes are sufficient to inhibit the types of cybercrime that now occur. Several members of parliament also feel that authorized penetration testing should now be considered legal and thus excluded from any punitive provisions of the revised legislation.

Keeping cybercrime legislation up-to-date is an important part of the war against cybercrime. I fear that countries that have meaningful cybercrime legislation do not engage in this task often enough. Fourteen years in the UK is, after all, a long time interval for this kind of legislation to remain unchanged despite all the radical developments in the IT arena over this span. Still, the APIG deserves a great deal of credit for realizing that changes are needed and doing something about it. Furthermore, the issues this group has identified are by all appearances very important

ones. The APIG's task will by no means be easy. It is, for example, extremely difficult to gage the effect of legislative provisions upon potential cybercriminals' willingness to engage in unlawful computer-related activities. It will thus be extremely interesting to see the final result of the APIG's efforts. You will be hearing quite a bit more about this legislation in *Security Views* as the APIG proceeds in this arduous task.

UK parliament restricts the use of wireless

Members of the UK parliament will not be provided with wireless phones and related wireless technologies in the Parliament building until security concerns regarding them can be adequately addressed. Officials from the House of Commons Commission made this decision after learning that sensitive information transmitted over wireless networks could easily be captured by unauthorized persons. In a recent test, 46 cellular phones in the building succumbed to attacks in which unauthorized persons accessed cellular phones based on Bluetooth wireless communications in just 12 minutes. Afterwards parliament members were cautioned to disable the Bluetooth functionality in their phones.

Stories of unauthorized interception of wireless communications continue to fill the news. Fortunately, an increasing number of organizations, the UK Parliament included, are becoming more cautious in the use of wireless technology, at least until appreciable improvements in this technology become available. New, more secure technology is imminent, so any current inconveniences due to restricting the use of this technology are likely to be short-lived.

New international banking laws require disclosure of risks and incidents

New international banking laws resulting from Basel II regulations mandate that UK financial institutions divulge their exposure to IT-related security risks, including cyberattacks, so that insurers and auditors can determine the amount of liability. Under these provisions banks must create databases that reflect a minimum of three years of IT-related events that have occurred, including the number of security-related incidents that have taken place.

These data are to be given to banks' insurance companies and auditors in addition to international regulators. The compliance deadline is the year 2007; financial institutions must accordingly create systems that record attacks from this point on. Non-compliant banks must put 2.8% of their assets in reserve to address IT-related liabilities. Critics have complained that compliance will be excessively costly to UK financial institutions.

Basel II regulations have had an enormous impact on the IT arena in many countries, particularly on the IT security arena within financial institutions, and the impact will grow as the compliance date approaches. My consulting experience has taught me that in general financial institutions do better in security risk management than most other institutions, so one might question why financial institutions are being forced to comply with these new laws. Although the financial cost of complying with these laws will be high, divulging risk exposures and security-related incidents will likely be the most difficult part of complying. Financial institutions have been reluctant to disclose such information because of the potentially huge negative effect such disclosure has upon customer and stockholder confidence. US banks have for years been required to report certain kinds of security-related incidents they experience to the Office of Currency Control (OCC), yet few banks actually share such information with the OCC. It will be interesting, therefore, to see if international banks will comply with the disclosure requirements in this new legislation.

New US DOE initiatives include cyber security provisions

US Department of Energy (DOE) Secretary Spencer Abraham announced initiatives to boost security across DOE laboratories and defense facilities. In addition to prescribing initiatives such as those that call for storing sensitive nuclear material at fewer locations and creating a special protective security force, Mr. Abraham also described new measures for protecting classified computer information better, upgrading security systems at critical DOE sites, and elevating security awareness among managers. To elevate the protection of sensitive information, a Cyber Security Enhancement Initiative to protect the confidentiality, integrity, and availability of all information on critical systems is being launched. A significant provision is that systems that hold such information must be capable of functioning even if they are being

actively attacked. Further initiative measures for 2005 include use of intrusion detection systems to thwart cyberattacks, enhancing measures that counter Internet threats, and boosting protections for on-line information. Sensitive functions such as weapons design would be conducted in a more secure diskless environment, thus helping prevent attacks in which saboteurs steal removable computer media containing classified information. Other actions under this initiative include replacing mechanical keys with complex new technologies, thereby establishing an environment that is not likely to be compromised by any physical object that is subject to being lost or stolen. Mr. Abraham also announced that quicker background checks are being conducted during the employee security clearance granting process and an intern program is being established to recruit outstanding technical personnel in cybersecurity, nuclear material management, and physical security.

It will truly be impressive if the US DOE is able to successfully implement all or even most of the measures that Mr. Abraham recently described. The DOE arena is truly a complex one, consisting of everything from unclassified research and operations to highly classified weapons research and production. I particularly like the provision that says that managers need greater security awareness. In my experience I have too often seen where the ignorance and indifference of management to security issues was extremely detrimental to the success of information security programs. Another excellent provision in Mr. Abraham's initiative is that systems that store critical information must be functional even during the times they are being attacked. I feel that survivability of systems is one of the most important directions that information security research and ultimately computer and network design itself can take if we are going to make genuine progress in information security. We will never be able to defend systems and networks to the point that we can stop all attacks, so the capability of systems and networks to recognize and drastically lessen the impact of attacks is a truly promising direction.

Combined federal contract for smart cards

Five US federal agencies, the Department of Veterans Affairs, Defense Department, Interior Department, Homeland Security Department, and NASA, are cooperating to issue a large contract buy up to 40 million smart cards over the next three years.

Although these particular agencies have initiated the procurement, other US agencies can nevertheless buy smart cards in accordance with the terms of the contract. The combined order may save as much as USD 5–24 per card. The cost of the actual smart cards is, however, greatly overshadowed by the cost of the other elements needed, such as smart card readers and developing procedures for smart cards. This contract may also include keyboards with built-in smart card readers.

I would really like to see this effort succeed. Five important US agencies have agreed to buy a large number of smart cards—a significant step forward in the quest to provide stronger authentication than passwords can provide. Cooperation between these agencies (something that is not all too common within government circles) has made the price of smart cards much more affordable. If these agencies succeed in widely implementing smart card authentication, other agencies (and perhaps even the commercial sector itself) will sooner or later be pressured to follow suit—a major victory in the information security arena.

Microsoft and Germany sign security pact

Microsoft CEO Steve Ballmer and German Federal Government Interior Minister Otto Schily signed a pact that commits Microsoft to cooperating with several security-related organizations and supporting a German standard for secure legal transactions. Under this agreement, Germany will license extensible markup language (XML) dialects used in Windows Office 2003. Microsoft committed to incorporate support for OSCI, a German standard for secure legal transactions, into its .Net framework. Microsoft also agreed to continue participating in Interior Ministry programs to promote open standards and interoperability among software applications. This agreement is significant because Germany has been vigorously promoting open-source software to supplant Microsoft software. Last year, the city of Munich elected to migrate 14,000 government-owned Windows PCs to Linux; the German government has actively promoted several other Linux development projects. After an experiment with the Danish government, Microsoft agreed last year to supply royalty-free licenses for the XML schemas used by the main applications in Office, which uses XML to ensure that data in documents can also be read by systems other than Windows systems.

This development is intriguing, especially considering that in the past the German government has adopted an anti-Microsoft posture and also that Microsoft has previously taken a strong stance against open-systems software. Now Microsoft is agreeing to promote open-systems standards in addition to interoperability. Interoperability is a special sore point with Microsoft critics, who have accused Microsoft of deliberately making its products non-interoperable to force the user community to buy its products. Will this agreement between Microsoft and the German government really work? Will Microsoft now say that open-source software is conducive to security? Only time will tell, but given what has happened in the past, I would not bet on it.

Security breaches drive away customers

Security breaches and malware such as worms and Trojan horse programs can cause a company's systems to crash or function poorly for extended periods of time, seriously diminishing customer confidence and making it impossible for customers to access that company's Web sites. A recent survey shows that phishing attacks, attacks in which a scam artist uses a phony rendition of a financial institution's Web site to obtain personal banking information from gullible customers, can result in even more damage. Competing firms often mention such security breaches to motivate customers to switch from another firm to theirs. In a survey conducted by Energis, a telecom firm, 47% of customers in the business-to-business sector switched firms after a firm experienced a security breach. Those who did not switch firms tended to spend slightly less—an average of 4% less—after a security breach. A second survey showed that 75% of individuals with bank accounts were less likely to respond to email their banks sent them because of being suspicious of phishing attempts. Approximately the same percentage of account holders shopped less on-line because of the phishing threat.

I do not know much about the scientific rigor with which this survey was conducted, but the results are certainly intriguing. I remember one unfortunate byproduct of the well-publicized break-ins into Citibank computers in 1994 by two Russians that resulted in transfer of funds to various accounts around the world. Although Citibank dealt admirably with this incident, a number of its corporate customers switched to other banks

after the news of this incident became public. An increasing number of studies, the present one included, indicates that security breaches produce tangible financial loss independent of any money stolen or the cost of responding to these breaches. Slowly but surely organizations will catch on, so to speak, something that will invariably lead to improved security.

Recent arrests based on new US anti-spam law

In the US government's first test of new legislation against spam email (the CAN-SPAM Act), US Federal Trade Commission (FTC) authorities arrested two email marketers, Christopher Chung and Mark Sadek, and are looking for two others, James Lin and Daniel Lin, on the grounds that they all allegedly sent volumes of email advertisements for a reportedly bogus weight-loss patch. The four could face up to five years in prison if they are convicted under the US anti-spam law that went into effect last January. All employees of a company named Phoenix Avatar, they have also been charged with mail fraud, which could result in a sentence of up to 20 years. The defendants allegedly spoofed the senders' email addresses, something that is illegal under the new anti-spam law. Phoenix Avatar's operations have been shut down and the defendants' assets have been frozen pending trial. The FTC also filed charges to stop an operation by Global Web Promotions Pty Ltd, an Australian company that is accused of sending a considerable amount of spam in the US.

I previously predicted that the CAN-SPAM Act would not be overly successful in stopping spam, mainly because so much spam originates from

outside of the US. According to one source, spam has actually increased since this Act was passed. Still, it is good to see that the US government is at least trying to enforce this Act, as evidenced the recent arrests for violating this Act. Although legislation may do some good, ultimately significant progress in the war against spam will have to come from new anti-spam technology, technology that is much smarter than current technology in discriminating between spam and non-spam traffic.

Cisco source code leak reported

The Russian security site SecurityLab.ru reported that some (an estimated 800 MB) of Cisco System's proprietary operating system code used in most of the company's networking devices was pilfered from Cisco's corporate network. Later some of it was reportedly leaked over the Internet. Cisco is investigating what happened, and now the FBI is also involved. Cisco discounted the possibility that any code leakage that occurred would threaten security in its devices.

Events such as this give strong support for those who favor open-systems security because the worse case event in proprietary systems is source code leakage. The one that occurred at Cisco was apparently not earthshaking, but it once again illustrates that unless very strong precautions are used in protecting proprietary software, any security-related advantages associated with the proprietary nature of this software quickly dissipate.

Eugene Schultz
Editor-in-chief

2 June 2004

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®