Femtosecond®

www.femto-second.com

In the News

Volume 1 issue 4

April 20, 2008

Inside this issue:

Special points of interest:

- Retail PCI is not a panacea
- IPv6 taking hold as IPv4 addresses deplete

The Shape Of Things To Come

Although there are some alarm bells in the financial services area, things appear controllable. We expect (or at least hope) that losses are manageable . However, if current trends continue, what can we expect in the future? There are some that believe the Fed will not be successful in abating the latest financial crisis [1]. The Fed decision to help Bear Sterns and other financial institutions indicated the seriousness of current events. The question that should not be lost in the current panic management is what are the losses due to cyber-crime? Alan Schwartz, the CEO of Bear Stearns, testifying before the Senate banking Committee asserted that the Bear Sterns collapse was due to rumor [2]. This illustrates how volatile the modern financial system is. Spreading false rumors is typically referred to a pump and dump [3]. The key point here is that malware can be used in spreading false rumors. For a pump and dump example, consider the Prime Time Group Inc., a Ft. Lauderdale, Fla.-based company that was the focus of a huge spam dump [4].

> ***For the first time, a major investment bank that was well-capitalized and apparently fully liquid experienced a crisis of confidence that denied it not only unsecured financing, but short-term secured financing, even when the collateral consisted of agency securities with a market value in excess of the funds to be borrowed.*** ~ Christopher Cox testimony regarding the Bear Stearns collapse, April 3, 2008

Rumors are not the only threat for financial institutions. One of the security product vendors, Symantec detected a man-in-the-middle attack directed against 400 banks [5]. As noted in the Symantec description: *The scale and sophistication of this emerging banking Trojan is worrying, even for someone who sees banking Trojans on a daily basis*. The silentbanker Trojan has the ability to bypass typical multifactor authentication currently used [6]. The *silentbanker*, is not the first to attack banks. Last year, malware known as the *Prg Banking Trojan*, was detected stealing funds from commercial banks in the US, UK, Spain, and Italy [7]. This Trojan is believed to have originated in Russia. It should come as little surprise that e-crime has become a big business with sophisticated criminal to criminal (C2C) business models [8].

Many times, businesses assume their computers and network are secure because that has been no detected entry into the system. That does not mean no-one broke into the system, only no break-in has been detected. Consider the example where Grad students hacked into a computer typically used by banks that was thought to offer adequate security [9]. In another

(Continued on page 2)

Retail Security

Since identity theft has become a widely recognized threat, efforts have evolved to strengthen credit card security. A highly visible approach is the Payment Card Industry (PCI) Data Security Standard (DSS) [1]. It seems that retailers need to complete a large questionnaire and there are a multiplicity of controls included [2]. The question remains, if a retailer is PCI compliant, does identity theft disappear? This question is best answered by the Hannaford breach where the retailer claims to have been PCI compliant [3].

Looking back at the past TJX breach, the exploit went undetected for a number of months [4]. Clearly, hackers are interested in the financial gains achieved from attaching retail stores.

(Continued on page 2)

Retail Security

(Continued from page 1)

1. www.pcisecuritystandards.org/tech/index.htm
2. Radcliff, Deb, SC Magazine, *Fall In Line*, April, 2008.
3. Offner, Jim,E-Commerce Times, *Hannaford: Malware Caused Massive Data Brea*, March 28, 2008.
4. Dash, Eric, International Herald Tribune, *Retail security breach may be biggest in U.S.*, January 19, 2007

The Shape Of Things To Come

(Continued from page 1)

example, the Commerce Bank was hacked and the bank asserts that although the hacker gained entry into a database with 3,000 customer records, only 20 were accessed [10]. One argument is that security models are typically obsolete and security in general is reactive [11]. Clearly, we should expect to see more attacks to our financial systems and the attacks will be ever more sophisticated. For example, a couple of years ago, hackers were able to get debit card PINs and hit a number of banks including Citibank, Bank of America, Wells Fargo, and Washington Mutual [12]. Debit cards require a Personal Identification Number (PIN) and were thought to be secure. However, the debit card is not a smart card with an active processor. It is instead a magnetic stripe that is easy to use but lacks the security of a smart card.

Any change, even a change for the better, is always accompanied by drawbacks and discomforts.—Arnold Bennett

The next obvious question is how will we prepare for our future? Indications are the number of Computer Science undergraduate enrollments in the US is dropping [13]. *The output of American computer science programs is plummeting, even while that of Eastern European and Asian schools is rising. China and India, the new global tech powerhouses, are fueled by 900,000 engineering graduates of all types each year, more than triple the number of U.S. grads. Computer science is a key subset of engineering* [14]. It would seem that other countries, many of which are home to sizable hacker communities, will soon be in a dominant position.

1. da Costa, Pedro Nicolaci, Reuters, *Experts see Depression parallels in U.S. crisis*, April 17, 2008.
2. MarketWatch, *Bear's demise was just a rumor*, April 3, 2008.
3. http://www.sec.gov/answers/pumpdump.htm
4. Keizer, Gregg, Computerworld, *Unusual 'pump-and-dump' spam run continues*, August 13, 2007.
5. OMurchu, Liam, Symantec, *Banking in Silence*, January 14, 2008.
6. Reed, Brad, Network World, *New Trojan intercepts online banking information*, January 14, 2008.
7. Ben-Itxhak, Yuval, Infosecurity, *New defence strategy in battle against e-crime*, April 18, 2008.
8. Messmer, Ellen, Network World, *Botnet-controlled Trojan robbing online bank customers*, December 13, 2007.
9. USA Today, Reuters, London, Cambridge: *Hacking bank computers not so hard*, November 9, 2001.
10. Kirk, Jeremy, IDG News Service, *Hacking Damage Limited, Bank Reports*, October 10, 2007.
11. Berghel, Hal, Communications of the ACM, *Faith-Based Security*, April 2008.
12. Keizer, Gregg, InforWorls, PIN Scandal 'Worst Hack Ever'; Citibank Only The Start, March 9, 2006.
13. IEEE Computer, *Computer Science Enrollments Drop*, page 87, April, 2008.
14. Business Week, *A Red Flag in The Brain Game*, May 1, 2006.

Attacking Hardware

The University of Illinois demonstrated how a nearly undetectable backdoor could be applied to a microprocessor [1]. They changed 1,341 logic gates on a chip that has more than 1 million. The significance of a hardware attack includes the ability for malicious software to bypass security software.

Of course hardware devices start off written in hardware definition language. This is then run against test fixtures, then synthesized, linked to manufacturer cell libraries and then run again using the original test fixture. There are ample steps along the way to introduce hardware back doors. Consider an attack against the synthesis tool. This could impact any hardware synthesized using this tool.

1. McMillan, Robert, Info World, *Malicious microprocessor opens new doors for attack*, April 15, 2008.

Cyber Security in the News

A tool credited with infecting 20,000 web sites since January has been partially dissected by SANS [1]. The tool reports to a server in China, possibly indicating the source of the malware. Hackers in China have received quite a bit of news. In another example, Chinese blogs have detailed a *zero-day* vulnerability with Microsoft Works [2]. Note, a zero-day vulnerability is one for which the vendor does not yet have a security patch to correct.

In describing the attack on Estonia last year, there were botnet attacks from 76 countries thereby masking the true source of the attacks [3].

Sometimes, cybercrime is closer to home. A “Security Expert” consultant pleaded guilty to compromising hundreds of thousands of machines for the purpose of identity theft [4]. He was the first person to plead guilty to wiretapping using botnets.

1. Kirk, Jeremy, PC World, *SANS Solves Mystery of Mass Web Site Infections*, April 17, 2008.
2. Kirk, Jeremy, Infoworld, *Chinese blogs detail zero-day flaw in Microsoft Works*, April 18, 2008.
3. Trevelyan, Mark, Reuters, *Security experts split on "cyberterrorism" threat*, April 17, 2008.
4. AFP, *US consultant pleads guilty to identity theft: authorities*, April 17, 2008.

> *We've arranged a civilization in which most crucial elements profoundly depend on science and technology–Carl Sagan*

The Rush to IPv6

The Internet relies on Internet Protocol (IP) version 4 (IPv4) and soon version 6 for networking. Most of the existing Internet used IPv4 which is limited to just over 4 billion addresses. There are estimates that there will not be enough addresses as soon as 2010 [1]. The world leaders for embracing IPv6 are those countries that are quickly running out of IPv4 addresses [2].

If one looks through the various Personal Identity Verification (PIV) documentation, such as PACS version 2.3, one will see hope that the Federal Agency Smart Credential Number (FASC-N) will be replaced by an IPv6 address [3]. It remains to be seen how fast agencies adopt the FASC-N replacement.

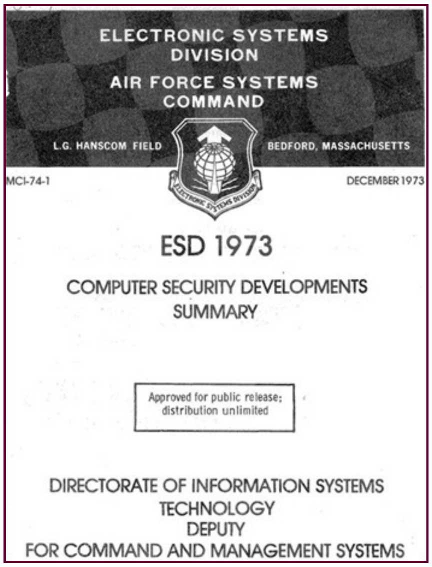
1. Schwankert, Steven, IDG News Service, *Sound the Alarm, IPv6 Execs Say*, April 16, 2008.
2. Essex, David , FCW, *IPv6: How the rest of the world lives*, February 4, 2008.
3. http://www.smart.gov/iab/documents/PACS.pdf

Back to Security Basics

Some have recommended the Turing Machine be used for security functionality [1]. A Turing machine emulates a full computer. Perhaps a good example is the processor located on a smart card. Indeed, one architecture posited an isolated processor to mediate information in-line [2].

Another early concept was the use of Ra Reference Monitor. Its limited functionality allowed proving security. The reference monitor was described as the hardware and software mechanism controlling subject (process) access to objects [3], The Air Force document credits the work of JP Anderson in describing the reference monitor. So after 35 years, are we are returning to the roots of computer security?

1. Jackson, William, GCN, *Needed: A 'Turing machine' for security*, April 11, 2008.
2. Proceedings of the Sixth Annual Computer Security Applications Conference, Hoffman, Lance, and Davis, Russell, *Security Pipeline Interface (SPI)*, pp. 349-355, 1990.
3. US Air Force, ESD 1973, page 5, Computer Security Developments Summary, December 1973.



ELECTRONIC SYSTEMS DIVISION

AIR FORCE SYSTEMS COMMAND

L.G. HANSCOM FIELD BEDFORD, MASSACHUSETTS

MCI-74-1 DECEMBER 1973

ESD 1973

COMPUTER SECURITY DEVELOPMENTS SUMMARY

Approved for public release; distribution unlimited

DIRECTORATE OF INFORMATION SYSTEMS TECHNOLOGY

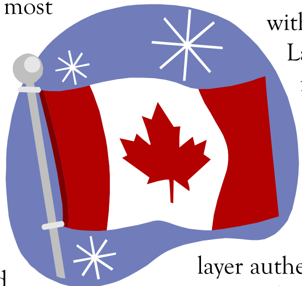
DEPUTY

FOR COMMAND AND MANAGEMENT SYSTEMS

> *Sometimes one pays most for the things one gets for nothing.—Albert Einstein*

On-Line Security

Five major Canadian banks were giving online banking customers a false sense of security [1]. To meet the security requirements, most customers would not be able to implement the controls. In one paper, researchers found that users tend to believe they are less vulnerable and often do not change default security settings [2]. Placing the security burden on end users is a risky business as users will not take the time to learn security practices and loss is likely.



The study of Canadian banks also identified problems with Secure Sockets Layer (SSL) implementation. In general, many SSL connections are vulnerable. The vast majority of application layer authentication SSL/TLS-based e-commerce applications are vulnerable to man-in-the-middle (MITM) attacks. [3] One control to mitigate MITM vulnerabilities is the PKI enabled smart card and SSL configured for client side authentication.

1. Schmidt, Sarah, *The Ottawa Citizen, No 'peace of mind' for online bank users: experts*, April 10, 2008
2. West, Ryan, Communications of the ACM, *The Psychology of Security*, April, 2008.
3. Oppliger, Rolf, et.al., IEEE Computer, *SSL/TLS Session-Aware User Authentication*, March 2008.