Femtosecond®
www.femto-second.com

In the News

Volume 1, Issue 2

April 6, 2008

The Chaos Computer Club

The Chaos Computer Club (CCC) is back in the news. Within Europe, there is a large organization of computer hackers known as the Chaos Computer Club. During the late 1980s, they successfully attacked National Aeronautics and Space Administration computers from West Germany [1]. In late 1987, they successfully penetrated the NASA Headquarters (NASA) VAX cluster and installed trap doors. The actual exploit used was published in one of CCC books in chapter 1 titled, Welcome to NASA Headquarters [2].

Now, they claim to have the German Chancellor Merkel's fingerprints and are threatening to publish them [3]. Similarly, they have published the fingerprints of the German home secretary, Wolfgang Schäuble, in their publication, *Die Datenschleuder* [4]. The CCC has a history of innovation and should not be quickly dismissed. With libraries of actual fingerprints, any injection attacks may be successful. For this reason, agencies might consider the enhanced security offered by smart cards when considering fingerprint only biometric approaches.

The CCC attack against NASA highlighted problems in incident response. In 1987, they discovered a vulnerability with the VAX 11-780 VMS operating system. "In attacking the National Aeronautics and Space Administration systems, the West German Chaos Computer Club masqueraded, bypassed access controls (partly by exploiting a subtle operating system flaw), and used Trojan horses to capture passwords. [1]" As the Department of Energy (DOE) used the VMS for classified processing so they classified the vulnerability; thereby preventing Digital Equipment from conveying the seriousness of the problem to its vulnerable community. Concurrently, unbeknownst to NASA Headquarters, they were being hacked for approximately 3 months by the Chaos Computer Club. So DOE, Digital Equipment Corporation, and the CCC knew of the vulnerability but the victim, NASA did not.

A good question here is should vulnerabilities be kept secret? To follow this line, in October, 2001, the Oulu University Secure Programming Group in Oulu, Finland, discovered a serious bug in the Simple Network Management Protocol (SNMP) and passed the information on to the US. This was immediately following

(Continued on page 2)

Another Week in the Financial Industry

In the last newsletter, the older BIF and SAIF funds were referenced. It was pointed out, these have been combined into the Deposit Insurance Fund (DIF) that had assets of $53 billion in 2007 [1]. Some comments suggested that everything is okay and there is no cause for concern.

With that as a backdrop, it is worth reviewing the history leading up to the current financial mess. In 2006 a Dubai company was trying to buy a controlling interest in operating a number of US Ports. [2] Based on pressure from many sources, the deal collapsed. However, following the subprime crisis, the same company was allowed to purchase a 4.9% ownership in Citi, the largest US bank, for $7.5 billion. [3] From June 30, 2004 through June 29, 2006, the Federal funds

(Continued on page 2)

Inside this issue:

Special points of interest:

- The Chaos Computer Club is maintaining a database of fingerprints
- Rumor became fact causing Bear Stearns to tether on bankruptcy
- Census goes paper

More Trouble in the Financial Industry

(continued from page 1)

rate grew from 1% to 5.25%. [4] However, starting on September 18, 2007 through March 18, 2008, the rate fell to 2.25%. In February, the health of the biggest banks and investment houses, such as Citicorp, J.P. Morgan, Bank of America and Merrill Lynch, which cumulatively have reported more than $150 billion in losses [5]. Then came Bear Sterns; with little notice, the Fed arranged funds for JP Morgan Chase to purchase Bear Sterns for pennies on the dollar [6]. The Fed transactions took place with amazing speed.

This week, the scope of the financial institution problem became clearer. The United Kingdom and the US are working on plans to monitor and regulate the banking system [7]. Consider that Government did nothing to aid the Enron investor's. In contrast, following the Bear Stearns bail-out, the Department of the Treasury announce new regulatory changes that give new power to the Fed [8]. That a Government agency (Treasury) would allow part of its organization (OCC & OTS) to fall under Fed authority is unprecedented. A cautionary note here, the current and the last Chairmen (Bernanke and Greenspan) both embarked on a program to raise interest rates just prior to the current crisis. If the sitting Chairman get's it wrong, the consequences to the economy could be disastrous.

Each week the loss estimates continue to rise. Some are estimating the loss to be $1 Trillion [9]. Meanwhile, the FDIC is increasing staff to support failed bank closings [10]. At the Senate Banking Committee hearings on April 3, Christopher Cox (SEC) stated Bear Stearns liquidity pool dropped from $12.4 billion to $2.4 billion on the Thursday before the Citi purchase. The SEC takes rumors spread by stock manipulators seriously [11] . We will likely see some lengthy investigations following the Bear Stearns collapse.

Today there are ample examples of how fast malware can attack networks and systems. If adequate security controls are not in place, what is to prevent significant equity transfer on the order seen by Bear Stearns? Can we afford to overlook the threat from bad actors while we debate the sub-prime crisis? Maybe we have seen the last of the current crisis, then again, maybe not. Unlike well understood attacks, IT security could devastate a financial institution in a very short period of time. Consider the short timeline leading to the current crisis and the expedited response from the Fed in addressing the crisis. This indicates how fast the problem escalated. What are losses due to weak security controls? Did malware play a part in promulgating rumors? The regulators missed the Savings and Loan crisis in 1990 and the latest crisis. Shouldn't internal security controls be a significant regulated item? Strong isolated cryptographic controls, such as proper smart card use, can provide a strategic control to mitigate future attacks. On a good day, financial institutions can weather cyber attack losses; however, when in a crisis mode, this may be the difference between survival and insolvency.

1. GAO, AGO-08-416, Financial Audit Federal Deposit Insurance Corporation Funds' 2007 and 2006 Financial Statements, February, 2008.

(continued on page 3)

"Three may keep a secret, if two of them are dead." - Benjamin Franklin

The Chaos Computer Club

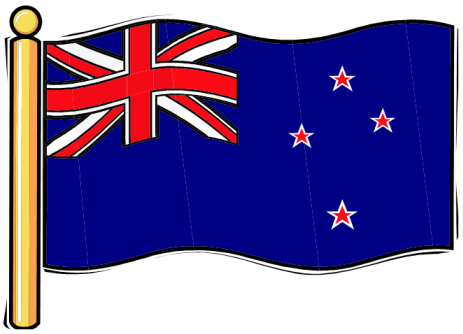
(continued from page 1)

9/11 and the US enjoyed unprecedented cooperation. However, a advisory by the US-CERT was not posted until February 12, 2002 [5]. The message should be clear, especially to organizations that are not one of the classified Department of Homeland Security (DHS) authorized recipients, serious vulnerabilities will be known and a computer emergency response team is not a panacea for serious attacks. Controls that provide isolated processing (read smart cards) can fill a significant gap.

Additionally, the CCC may have had a hand in writing the first mainframe computer virus in 1987. Klaus Brunstein, University of Hamburg, at the time described a mainframe virus. Some of the CCC information exchange indicates it was written on IBM PCs using a shareware program (Cross Assembler for the IBM 370 Version R1.1). The advice here is do not assume any operating system is immune from malicious attack and consider layered security.

1. National Research Council, *Computers at Risk*, pages 61-62, National Academy Press, 1991
2. Wunderlick, *Das Chaos Computer Buch, Hacking made in Germany*, 1988
3. AFP, *German hackers threaten to publish Merkel's fingerprints*, March 31, 2008.
4. Heise online, CCC *publishes fingerprints of Wolfgang Schäuble, the German Home Secretary*, March 31, 2008.
5. Lemos, Robert, ZDnet, *SNMP bugs put Net traffic at risk*, February 13, 2002.

New Zealand Bot Virus Convicted



An 18 year old hacker, Owen Thor Walker was convicted [1]. His Bot net virus code infected approximately 1.3 million computers world-wide. Losses from the hacker are estimated at $20 million. In Meanwhile, the Department of Justice secured a conviction for a person that used botnets to infect 250,000 computers. These machines were then used to harvest passwords and account information.

A botnet can utilize a large number of *Zombie* computers to provide significant processing and network power. A botnet propagating rumors or transferring funds could quickly bring down a healthy financial institution.

1. AFP, *NZealand teen convicted over global cyber-crime ring*, April 1, 2008.
2. DOJ, *Computer security consultant charged with infecting up to a quarter million computers that were used to wiretap, engage in identity theft, defraud banks*, November 9, 2007.

More Trouble in the Financial Industry

(continued from page 2)

2. MSNBC, Dubai firm says it will delay U.S. port takeover, February 23, 2006.
3. The Wall Street Journal, *Citi of Arabia Abu Dhabi takes Manhattan-and Washington, too?*, November 29, 2007.
4. www.federalreserve.gov/fomc/fundsrate.htm
5. Hill, Peter, The Washington Time, *Bernanke expects bank failures*, February 29, 2008.
6. Barnett, Ted, CNN, *Senators want details of Bear Sterns bailout*, March 26, 2008.
7. Blitz, James, and Parker, George, Financial Times, *Bush and Brown in push to deal with crisis*, March 30, 2008.
8. Labaton, Stephen, The New York Times, *Obstacles Seen as Treasury Proposes New Financial Rules*, March 31, 2008.
9. Pressley, James, Bloomberg, *Brace for $1 Trillion Writedown of 'Yertlt the Turtle' Debt*, March 31, 2008.
10. Zibel, Alan, Associated Press, *FDIC Plans Staff Boost for Bank Failures*, March 25, 2008.
11. Scheer, David, Bloomberg, *SEC Takes False Rumors About Banks `Very Seriously'*, April 3, 2008.

"A banker is a fellow who lends you his umbrella when the sun is shining, but wants it back the minute it begins to rain." - Mark Twain

Cybercrime

Cybercriminals are using the concept of "fast flux" to hide phishing sites [1]. The botnets hosting the malware keep changing the DNS records. In effect, there is no single site that can be shut down to stop the attack. Bot and spyware were identified as most worrisome problems in a recent survey [2].

Botnets are a continuing problem. For example: "On a typical day, 40% of the 800 million computers connected..."[3] What can happen is that a home computer can be infected with a malicious program that effectively controls that computer. In turn, this computer can be used to launch attacks against other Internet resources or mine for sensitive information (such as bank account passwords).

1. Knight, Gavin, The Guardian, *Cybercrime is in a state of flux*, March 27, 2008.
2. Hickey, Kathleen, GCN, *Bots, spyware top worry list for federal IT security*, April 2, 2008.
3. Acohido, Byron, and Swartz, Jon, USA Today, *Botnet scams are exploding*, March 17, 2008.

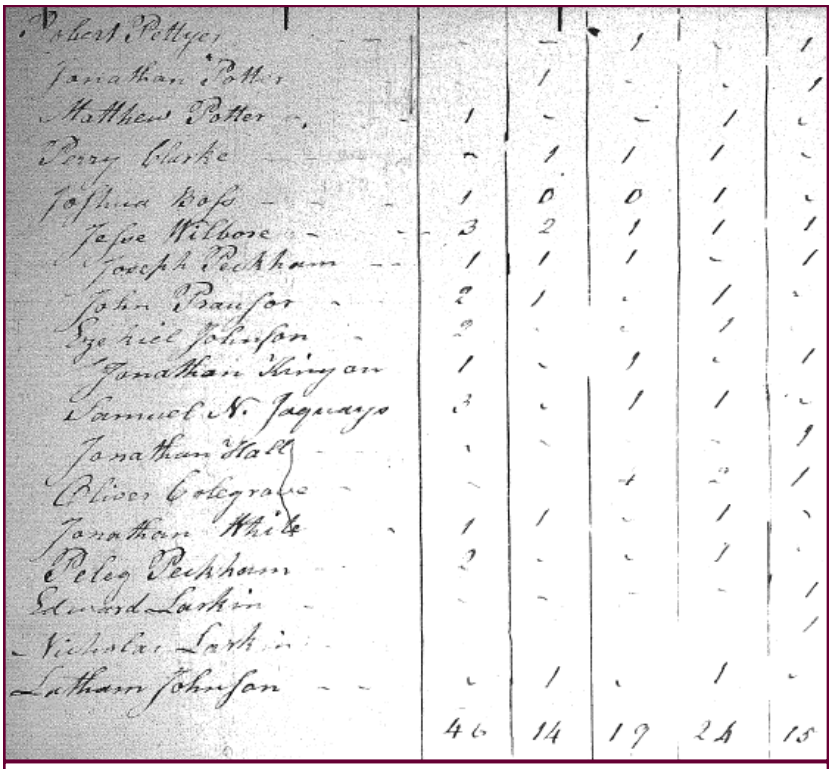
2010 Census to use Paper

Citing IT risks, the Census has opted to use a paper follow-up questionnaire [1]. The additional cost is estimated to be between $2.2 and 3.0 billion. This would bring the revised total to approximately $14 billion. A price increase exceeding 15% before the project starts. The problems cited included the complexity and data transfer of hand held computers: "The computers proved too complex for some temporary workers who tried to use them in a test last year in North Carolina. Also, the computers were not initially programmed to transmit the large amounts of data necessary." [2]

This is perhaps a good example where the initial business requirements were not fully vetted. In managing projects, requirements that are discovered later are costly. Hopefully, the 2010 lessons learned will be used during the 2020 census.

1. Chan, Wade-Han, Federal Computer Week, Census turns to paper, rejects IT risks, April 3, 2008.
2. CNN, *Back to pencil and paper for 2010 census*, April 3, 2008.

"The economic and technological triumphs of the past few years have not solved as many problems as we thought they would, and, in fact, have brought us new problems we did not foresee" - Henry Ford



From the 1800 Census, Washington County, Rhode Island

Cyber-Warfare

The US Air Force is planning to have an offensive cyberwarfare capability in place by October [1]. This comes at a time when there is considerable concern over Chinese cyber attack capabilities [2]. As nations embark on cyber attack methodologies, what other targets besides military are at risk? If a countries economic structure collapses, how can it fund a viable military. As seen from other article in this newsletter, prudent isolated security controls are in the best interest of all.

In addition to China, Russia also has a cyberwarfare capability [3]. While nations await full scale cyberwar, China appears to be cyber-spying [4]. Unlike previous wars, cyberwars will be fought in the corporate computer rooms throughout the US. Can we afford to ignore strong IT security controls in light of the obvious?

1. Jesdanun, Anick, Associated Press, *US cyberwarfare prep includes offense*, April 6, 2008.
2. Sumner, Lemon, PC World, China Crafts Cyberweapons, May 28, 2007.
3. Koman, Richard, ZDNet, *China, Russia at forefront of cyberwarfare*, November 30, 2007.
4. The Seattle Times/AP, *British firms told of China cyber spying*, December 2, 2007.