Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 10

June 1, 2008

Network Risks

Did China have a hand in the 2003 Northeast blackout of 50 million customers and the February, 2008 South Florida blackout of 3 million customers? One report suggests the People's Liberation army (PLA) played a role in both blackouts [1]. The timeline for the 2003 blackout can be found at the Federal Energy Regulatory Commission (FERC) web page [2]. In the FERC congressional testimony (November 2003), there was no mention of cyber attacks as a possible reason for the blackout [3]. In the case of the Florida blackout, the cause was blamed on an electrical engineer that violated policy and disabled two safety controls in order to diagnose a damaged switch [4]. On March 19, FERC announced it would join a non-Public investigation into the Florida blackout [5]. On May 21, the FERC chairman, Joseph T. Kelliher, highlighted the unique threat posed by cyber-attacks against the US power grid [6]. Although the FERC chairman does not specifically implicate China, he does acknowledge a current vulnerability without adequate regulatory oversight . Whatever the reason for the Florida blackout (lack of dual controls or cyber attacks), IT security can be improved.

In other network news, hackers prevented customers from getting email and web access to Comcast.net [7]. The hackers that took control of Comcast.net described their attack as a combination of social engineering and a technical hack [8]. Comcast is not the only victim; hackers took over the NASA Phoenix Mars mission web page [9]. Another tool sometimes used by hackers is the rootkit; an application that gives a user or program root privileges. Should malicious software (malware) operate a rootkit, the rogue program could do anything that root access allows. A security researcher demonstrated how to install a Cisco rootkit at E.U. Security West Conference in London [10]. Still, it appears that the leading attack vectors are based on old exploits [11].

> *However, the cyber security threat is different. It is a national security threat that may be posed by foreign nations, or others intent on undermining the U.S. through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance. Given the national security dimension to the cyber security threat, there may be a need to act quickly to protect the bulk power system, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure. Our legal authority is inadequate for such action. – Joseph T. Kelliher FERC Chairman [6]*

New technology continues to offer hope for improved security; however shortcomings are quickly being identified. Consider the Microsoft CardSpace technology designed to improve security and provide single sign-

(Continued on page 2)

Monitoring Access

Monitoring access can be divided into logical and physical access. In the case of logical access, the DHS plans to implement the General Information Technology Access Account Records System (GITAARS) that will record regular department access [1]. As noted in the System of Records Notice "*Further, GITAARS security protocols will meet multiple NIST Security Standards from Authentication to Certification and Accreditation.*" [2] It is unclear which NIST standards will be used but we hope it will be more than user ID and password authentication.

Perhaps the most visible form of physical access monitoring are the new traffic cameras we see for red light and speeding violations. Police monitoring cameras are a valuable tool

(Continued on page 2)

Inside this issue:

Special points of interest:

- China embeds microchip in Olympic tickets with bearer's information
- Did cyber-attacks contribute to US power blackouts?
- Anti-P2P company inadvertently shuts down legitimate business
- Fourth bank failure this year
- Hacker takes over NASA Phoenix Public Web site

Network Risks

(Continued from page 1)

on functionality. One report indicates that researchers have found an exploit that allows token capture that can be used to access other legitimate sites [12].

The current wave of malware exploits poses a significant threat to the Internet economy [13]. If the losses to businesses and consumers get too high, will there be a focus on stronger protection such as that provided by smart cards?

1. Harris, Shane, National Journal Magazine, *China's Cyber-Militia*, May 31, 2008.
2. http://www.ferc.gov/industries/electric/indus-act/blackout/09-12-03-blackout-sum.pdf
3. http://www.ferc.gov/congress/cong-test/2003/11-20-03-wood.pdf
4. Patel, Julie, South Florida Sun-Sentinel, *Florida blackout*, March 3, 2008.
5. http://www.ferc.gov/news/news-releases/2008/2008-1/03-19-08.asp#skipnavsub
6. http://www.ferc.gov/EventCalendar/Files/20080521140041-Cybersecurity%20testimony.pdf
7. Jackson, Joab, Government Computer News, *Cisco router rootkit 101*, May 27, 2008.
8. Danchev, Dancho, ZDNet, *How was Comcast.net hijacked?*, May 30, 2008.
9. Associated Press (Tucson), *Hacker changes Phoenix Mars Lander Web site*, June 1, 2008.
10. McMillan, Robert, IDG News service, *Hackers knocked Comcast.net off-line*, May 30, 2008.
11. Leyden, John, The Register Channel (UK), *Old Windows exploits dominate hack attack traffic*, May 30, 2008.
12. Kirk, Jeremy, IDG News Service, *Researchers Breach Microsoft's CardSpace ID Technology*, May 30, 2008.
13. Dent, Hugh, AFP, *Zombies and botnets: OECD warns of hidden armies in cyber wars*, June 1, 2008.

We must use time as a tool, not as a couch.–John F. Kennedy

More Bank Failures Predicted

The fourth FDIC insured bank this year to fail, the First Integrity bank in Minnesota, with $54.7 million in assets was closed by regulators [1]. Prior to this news, the chairwoman of the FDIC, Sheila Bair, indicated more bank failures are likely as the credit crisis unfolds [2]. For its part, the Fed continues to make funds available to banks to ease credit markets [3].

Indeed, it seems that Fed loans will be a permanent fixture for investment banks [4]. This will likely result in new regulation oversight.

1. Associated Press, *Bank regulators shutter First Integrity bank*, May 30, 2008.
2. Chung, Joanna, and Scholtes, Saskia, *Financial Times, US banks likely to fail as bad loans soar*, May 29, 2008.
3. Aversa, Jeannine, Associated Press, *Fed to make fresh batch of bank loans*, May 29, 2008
4. Lanman, Scott, and Massucci, Anthony, Bloomberg, *Kohn Signals Wall Street May Get Permanent Access to Fed Loans*, May 30, 2008.

Monitoring Access

(Continued from page 1)

in combating crime. In New York, cameras aided police in arresting two men on burglary charges [3]. However, sometimes cameras are used for nefarious activities. For example, in China, a traffic camera was used to monitor women inside their residences [4].

1. Lipowicz, Alice, Washington Technology, *DHS to monitor access to IT systems*, May 21, 2008.
2. http://edocket.access.gpo.gov/2008/E8-10895.htm
3. McGuire, Jim, The Daily Gazette (Schenectady), *Surveillance cameras become valuable law enforcement tool Surveillance cameras become valuable law enforcement tool*, May 12, 2008.
4. Lisheng, Zhan, China Daily, *Anger over 'peeping' traffic cam*, May 13, 2008.

Imposters

Years ago there was a New Yorker cartoon showing a horrified patient on an operating table asking the masked doctor, "*how do I know you're not George Plimpton?*" [1] Readers may recall George was the great imposter who used participatory journalism. So how likely is it that fake doctors could exist today?

Consider, a fake doctor was video recorded roaming the halls of a children's hospital in Jacksonville, Florida [2]. The imposter's badge was a Humana ID card with a yearbook picture pasted on the front [3]. Meanwhile in Brooklyn an alleged fake dentist was indicted [4].

There have been cases where doctors receive bogus degrees. In one case, an 8-year old patent died following the advice from a bogus health care specialist [5]. Fake doctors are not new to the field of medicine. Back in 1984, several practicing doctors were arrested in New York [6].

Then there is the reoccurring case where someone impersonates a first responder. Consider the case in Baltimore where men dressed as public workers are accused of burglarizing 2 homes [7].

1. Time Magazine, *Antic Imposter*, November 8, 1968.
2. WJXT, *Fake Doctor Roams Children's Hospital*, May 22, 2008.
3. Coleman, Matt, The Florida Times-Union, *Police seek 'doctor' wandering hospital*, May 23, 2008.
4. WCBS, *Alleged Brooklyn 'Fake Dentist' Indicted*, May 13, 2008.
5. Armour, Stephanie, USA Today, *Diploma mills insert degree of fraud into job market*, September 29, 2003.
6. Lyons, Richard D., New York Times, *6 Arrested for Fake Medical Degrees, Including 3 Known as Doctors*, July 13, 1984.
7. Hager, Jeff, WMAR, Baltimore, Crime Alert: Public Works Imposters, May 27, 2008.

Identification News

In Denver, a man with stolen ID information used a computer to make bogus identification cards to defrauded banks and merchants of over $200,000 [1]. In North Carolina, a man was arrested for manufacturing and selling bogus driver's licenses [2]. Hopefully faking driver's licenses will become more difficult as new technology is used. For example, China is embedding Olympic tickets with a microchip containing the photograph, passport information, e-mail, address, and phone numbers of the bearer [3].

A man who once worked for the Wisconsin motor vehicles division was accused of selling false driving permits [4]. A man with a false birth certificate and social security card was finally identified by matching his fingerprints on record [5]. A Delaware man was sentenced to prison for trafficking in false identity documents [6]. In Georgia a man was found with fake identification cards and laminating equipment, believed to be used as part of a con [7].

Texas is experiencing an increase in fake document arrests with good quality documents (driver's license, social security cards, and green card) selling for $500 [8]. It seems that shared social security numbers are quite prevalent. Consider the case where a Chicago woman's SSN was being used by 37 other people [9].

1. Haigh, Steve, Rockey Mountain News, Oregon man pleads guilty to bank fraud, May 27, 2008.
2. WGHP, *Burlington Man Busted for Selling Fake Driver's Licenses*, May 29, 2008.
3. Wade, Stephen, AP, *China embeds microchips in Olympic tickets*, May 27, 2008.
4. Wheeler News Service, *Mexican immigrant wanted in Wisconsin for selling false ID cards arrested in Minneapolis*, May 21, 2008.
5. Hubartt, Megan, The Journal Gazette (Ft. Wayne), *Police: Man in pursuit had false ID*, May 23, 2008.
6. The News Journal (Delaware), *Selbyville man gets prison time for false ID selling*, May 9, 2008.
7. Gurr, Stephen, Gainesville Times (Georgia), *Police: Man's fake IDs may be part of con*, May 24, 2008.
8. Pinkerton, James, Houston Chronicle, *Fake documents swamp Houston*, May 6, 2008.
9. Sullivan, Bob, MSNBC, *The secret list of ID theft victims*, January 29, 2005.

I spend almost as much time figuring out what's wrong with my computer as I do actually using it. – Cliff Stoll

Chinese Spying

Did China copy the contents of Commerce Secretary Carlos M. Gutierrez's laptop during a trip to China? There is a report that an ongoing investigation is exploring the possibility [1]. It is unclear if the contents was properly encrypted or not. Travelers to the Olympics in China are advised to leave their computers at home or if they must bring them, have as few files as necessary and use encryption [2].

Domestically, it has been suggested that China's foreign secret service is amongst the most aggressive seeking military technology and information [3]. For example, a New Orleans man pleaded guilty to transferring *Secret* documents to China in exchange for $50,000 [4].

1. Brides, Ted, Associated Press, *US probes whether laptop copied on China trip*, May 29, 2008.
2. Bergstein, Brian, Associated Press, International travelers advised to take steps against computer espionage, May 29, 2008.
3. AFP (Washington), *Chinese woman admits to helping Pentagon-linked spying*, May 29, 2008.
4. UPI, *Man pleads guilty in China spy case*, May 13, 2008.

Web 2.0

We can expect more rogue exploits will be developed targeting Web 2.0 applications. For example, an Albanian hacker group is selling a Web 2.0 tool kit to help malware writers [1].

In the entertainment industry, copyright protection is a significant issue. Sometimes the protection is worse than the cure. A Web 2.0 company, Revision3 suffered a denial of services (DOS) attack that originated from MediaDefendor, an entertainment sponsored anti-peer to peer (P2P) company [2]. The estimated loss to Revision3 is $100,000 [3]. As with any security control, unexpected consequences should be fully explored.

1. Larkin, Erik, PC World, *Web 2.0 Sites a Thriving Marketplace for Malware*, May 30, 2008.
2. Hachman, Mark, Extreme Tech PC Magazine, *Anti-P2P Group Takes Down Revision3 Site*, May 29, 2008.
3. Morphy, Erika, Tech News World, *Aggressive Antipiracy Firm Snags Dolphin in Tuna Net*, May 30, 2008.

Give me a lever long enough, and a prop strong enough, I can single-handed move the world.- Archimedes

Unencrypted Data Loss

In the last newsletter we included a discussion of information on 4.5 million bank customers that was on a lost tape. Reports indicate the Bank of New York Mellon tapes were not encrypted [1]. The bank is offering affected customers one year of credit monitoring service [2].

In another example of lost unencrypted information; a lost disk drive containing 5,500 employee and 40,000 customer accounts was lost by a firm hired for data analysis [3]. On the positive side, the company maintaining the privacy information, State Street will provide two years of free credit monitoring [4]. So what happens to those people that notice credit violations? How do they prove the loss originated for the theft?

1. Fonseca, Brian, Computerworld, *Connecticut AG blasts BNY Mellon for failing to notify victims for three months*, May 30, 2008.
2. Valiante, Dave, Wall Street & Technology, *Security Breach Affects BNY Mellon, People's United Bank*, May 29, 2008.
3. Kerber, Ross, The Boston Globe, *State Street: Data stolen from vendor*, May 30, 2008.
4. Associated Press (New York), *State Street says personal data has been stolen*, May 29, 2008.