Femtosecond®
www.femto-second.com

In the News

Volume 1 issue 3

April 13, 2008

Computer Crime

Companies are continuing to experience security data breaches. This should come as no surprise given the effort applied to making malicious code. A analyst from the Gartner Group reported that more malicious code was being developed worldwide than legitimate code [1]. If true, this is a serious problem that will continue to haunt IT for the foreseeable future. The main motivation of the cyber-crime appears to be money [2]. For example, Advance Auto Parts is alerting up to 56 thousand customers that a network intrusion may have exposed their financial information [3]. While companies are reporting new breaches, vulnerabilities exit in Federal systems. To illustrate this point, there are a number of users at the IRS that have elevated privileges [4].

2008 looks like it will be a banner year for security breaches. By some estimates, breaches during the first three months of 2008 are double 2007 [5]. To assess the overall of security crime one needs to consider the annual loss is now estimated at $200 billion [6]. Clearly, with loss this large, computer crime must be impacting most IT segments, including Government. Yet implementing adequate controls is still lacking. Consider the Government Accountability Office (GAO) is urging Office of Management and Budget (OMB) to focus on informing Government agencies how to use the Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) cards [7].

There is a general belief that the U.S. lags in cyber security readiness [8]. Perhaps another issue is the lack of understanding regarding cybercrime. In a study discussed at the RSA conference, the National Cyber Security Alliance found noted that a large percentage of consumers did not understand cybercrime threats [9]. One approach to addressing computer crime is to enact new legislation. Unfortunately, laws can only do so much [10]. Proper technical controls must be incorporated to stem the time. For example, U.S. laws will not deter hacker in countries not bound to our laws.

1. Weil, Nancy, InfoWorld, *Top 10 stories of the week: Windows worries, visa caps, malware spreads*, April 11, 2008.
2. Ward, Mark, BBC News, *Boom times for hi-tech crimi-*

(Continued on page 2)

Inside this issue:

Special points of interest:

- GAO urges OMB to focus on agency use of PIV cards
- More malicious code is developed worldwide than legitimate code

Insider Information

In late March IBM and its subsidiaries were suspended from receiving new federal contracts [1]. The suspension was lifted on April 3. The reason behind the original suspension was that allegedly some IBM employees had obtained protected source selection information and used it to their advantage during contract negotiations [2]. Within industry, the drive for profit is a powerful motivator that sometimes drives people to do things they shouldn't. We do not know how protected source documents were compromised nor how the loss was detected. It does highlight that all companies and Government agencies have the challenge of protecting sensitive information.

Sometime the insider threat is more than a casual breach of confidentiality.

(Continued on page 2)

Insider Information

(Continued from page 1)

Consider the UBS trial against an insider accused of planting a logic bomb. With just 50—70 lines of code, it took down 2,000 servers [3]. Repairing the damage was estimated to cost $3.1 million

Trying to secure a conviction is and remains a challenge. Consider that new technology continues to advance and juries and lawyers are unlikely to understand the complexities of the insider attack. If a lawyer cannot explain what was done, how can there be a conviction? Conversely, if the rules of evidence are relaxed to accommodate the lack of IT knowledge, might unscrupulous companies use this to secure convictions against innocent insiders? Could a successful outside hack result in an innocent administrator conviction? Without strong identification and authentication, such as proper use of smart cards, there may be no easy answer.

1. Aitoro, Jill R., Government Executive, *IBM suspended from new federal contracts*, March 31, 2008.
2. Weigelt, Matthew, FCW, *IBM is back, but what happened?*, April 7, 2008.
3. Gaudin, Sharon, Information Week, *UBS Trial Puts Insider Security Threats At Center Stage*, June 17, 2006.

Computer Crime

(Continued from page 1)

nals, January 2, 2008.

3. Naraine, Ryan, and Prince, Brian, eWeek, *Data breaches cause Concern*, April 7, 2008.
4. CNN Money, *IRS computers may be vulnerable to attack*, April 7, 2008.
5. Carr, Jim, SC Magazine, *2008 on pace for record number of breaches*, April 4, 2008.
6. Swartz, Jon, USA Today, *Online crime's impact spreads*, April 11, 2008.
7. Bain, Ben, Federal Computer Week, *GAO: OMB should move on HSPD-12*, April 9, 2008.
8. Weinberg, Neal, Network World, *U.S. cyber readiness lagging, panel says*, April 9, 2008.
9. Claburn, Thomas, Information Week, *Study Finds 'Alarming' Ignorance About Cybercrime*, April 11, 2008.
10. Katyal, Neal, The New York Times, *How to Fight Computer Crime*, July 30, 2002.

> *"Having the capacity to lead is not enough. The leader must be willing to use it." - Vince Lombardi*

Cybercrime Treaty

In 2001, the Council of Europe's Convention on Cybercrime was adopted. To date, 22 countries have ratified the treaty [1]. The U.S. Senate ratified the treaty in 2006 [2]. One controversial aspect of the treaty, it does not require dual criminality. That is, a country investigating political unrest could request FBI assistance.

So far, 43 countries have signed the treaty (21 have yet to ratify). Other countries outside the 47 members of the Council of Europe have expressed interest in joining. Closer to home, Brazil, Mexico, and Costa Rica are considering joining the treaty [3]. Obviously, there could be some problems down the road if the U.S. is called in to help find democracy groups to our south.

1. Kirk, Jeremy, PC World, Cybercrime Treaty Gains Momentum, April 6, 2008.
2. Broache, Anne, and McCullagh, Declan, CNET, *Senate ratifies controversial cybercrime treaty*, August 4, 2006.
3. Kirk, Jeremy, Network World, *Cybercrime treaty gains more interest, momentum*, April 1, 2008.

Hacker Underground

Once your identity has been stolen thieves have a sophisticated selling mechanism. Identities, vulnerabilities, and credit card numbers are sold through instant message groups and web forums [1]. These groups typically exist for a very brief period. Hacking has become a big business.

Prior to TJX disclosure of compromised identities, the credit card companies were already detecting increased incidents of fraud; possibly indicating identities were sold over the Internet [2]. Hacker groups going back to the Chaos Computer Club (see last newsletter) have been active for decades. New technology and evolving exploits will necessitate better security controls or conversely more loss.

1. Robertson, Jordan, Associated Press Technology, *Online crooks face tough competition*, April 8, 2008.
2. Greenemeier, Larry, and Hoover, J. Nicholas, Information week, *How Does The Hacker Economy Work?*, February 10, 2007.

DHS Increases Cyber-Security Staff

The Department of Homeland Security (DHS) has more than 300 Government cybersecurity positions open [1]. The secretary of DHS, Michael Chertoff, is creating a National Cyber Security Initiative [2]. DHS cybersecurity budget request increased to $190 million for the next fiscal year.

The DHS remains in the cybersecurity cross-hairs. Consider the example where DHS computers were hacked and sensitive information moved to Chinese web sites [3]. According to the article, the contractor assigned to protect DHS computers, including maintaining Intrusion Detection software, hid the attacks. Software based security products alone cannot fully protect a Government computing environment. Perhaps the lessons learned from the successful implementation of CAC cards for network authentication could be adopted by the DHS. Hacker attacks are not likely to subside any time soon.

1. Lipowicz, Alice, Washington Technology, *DHS to beef up cybersecurity staff*, April 3, 2008.
2. Jackson, William, GCN, *Chertoff outlines goals of national cybersecurity initiative*, April 8, 2008.
3. CNN, *Investigators: Homeland Security computers hacked*, September 24, 2007.

> *"It's kind of fun to do the impossible." - Walt Disney*

Digital Certificate IDs

At the RSA security conference in California, some vendors predicted digital certificates will be part of driver's licenses within 12 to 24 months [1]. During this election year, it is important that the integrity of the election process be maintained. Yet there are concerns that the system is vulnerable to hacking [2]. Clearly, a system that uses smart card with digital certificates identifications could provide additional security. However, such a system requires strong identification as part of the smart card issuance process.

1. Jackson, William, GCN, *Digital certificates could become standard in IDs*, April 8, 2008.
2. McMillan, Robert, IDG News Service, U.S. Presidential Election Can Be Hacked, April 10, 2008.

Scope Creep

In a follow-up from the last newsletter article on the Census decision to revert to paper, there is a call for a congressional investigation [1]. It seems that Census officials did not do an adequate job in specifying the technical requirements for the prime contractor, Harris Corp [2].

It is interesting that the Census should revert to paper at a time when extraordinary efforts are taking place to minimize paper counterfeiting. Consider the case of paper currency. Every so often the paper currency changes to thwart the latest advances in counterfeiting. An estimated $62 million entered circulation in 2006 [3]. With all the anti-counterfeiting controls, that more money was circulated indicates that at some point, paper may have to be replaced by something more secure. More recently, a new $100 bill that appears to have the same paper content as legitimate bills has been detected in circulation [4].

So what does this imply for the Census? If the integrity protection of paper is important, it may be a more difficult task than securing digital information. Paper consumes volumes of space. As the Census scans the information, additional time and quality will factor in.

1. Chan, Wade-Han, FCW, *Davis: Census didn't heed warnings*, April 8, 2008.
2. Associated Press, *Back to pencil and paper for 2010 Census*, April 3, 2008.
3. Hagenbaugh, Barbara, USA Today, *More counterfeit money changed hands in '06*, February 27, 2007.
4. Fox News, *Mysterious $100 'Supernote' Counterfeit Bills Pop Up Worldwide*, January 14, 2008.

> *"The more laws and order are made prominent, the more thieves and robbers there will be." - Lao-tzu*

If we don't plan for change, we could be headed for a wreck

The State of Technology

Intel has released a low power process called "Atom" with over 45 million transistors [1]. The key phrase here is low power in terms of power consumption (not processing capability). Intel is using a 45 nm (nanometer) transistor size with a power consumption of 30 mW to 2.5 watts [2]. The target is mobile devices. These devices will operate with a clock rate up to 1.6 GHz

Certainly there are more powerful processors available today but the trend to use smaller size transistors means more processing power, less size, and less power consumption. Consider for the moment the power of a single device operating inside of an enclave. Contrast this with the Cray-1 supercomputer of 1979. The Cray-1 includes 350,000 chips, could process 80 million instructions per seconds, and required 100 Kilowatts of power to run [3]. Any compromised new technology device has more power than the older supercomputers. So a single compromised device inside a firewall could provide a hacker with tremendous processing power. New technology requires new security approaches.

1. Greene, Kate, MIT Technology Review, *Inside Intel's New Chip*, April 7, 2008.
2. www.intel.com/technology/atom/index.htm
3. Schefter, Jim, Popular Science, *Supercomputer*, June, 1979.