Femtosecond®

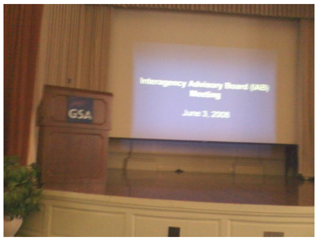
www.femto-second.com

IN THE NEWS

VOLUME 1 ISSUE 11

JUNE 8, 2008

Government Smart Card Use



On June 3, the Interagency Advisory Board met in the GSA Headquarters auditorium. Judy Spencer (GSA) described work in progress to allow non-Personal Identity Verification (PIV) cards issued outside of Government sponsorship to be recognized by Federal agencies. Three areas and possible solutions were discussed. The first, trusting the issuance process could met by using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 level 4 guidance. The second issue was how best to ensure a unique ID. It was suggested that using an IPv6 address could meet this requirement. The last area requires the digital authentication certificate to be validated. The certificate issuance requires cross-certification with the Federal Bridge Certification Authority (FBCA) meeting medium hardware. Judy mentioned the aerospace industry is in the process of such a cross-certification. Between speakers, Tony Cieri (moderator) provided a 9/11 example of why we need to authenticate people. According to Tony, on 9/11 firemen were first denied access to the Pentagon, then were allowed in. On their way out, their identities were checked and some reporters dressed as firemen were discovered. Their film was confiscated; however, 6 months later, pictures taken from inside the Pentagon on 9/11 were discovered in Afghanistan. The next speaker, Tim Baldridge (NASA) describe an approach that uses the same fingerprint scan for both the Electronic Fingerprint Transaction and for 2-finger minutiae conversion (required for storage in the PIV card). The last presenter, Christopher Runde (TSA) described the on-going Aviation Credential Interoperable Solutions (ACIS) project. This project's goal is for airports and airlines to use the same credential.

Perhaps the biggest challenge will be in using the PIV and other technologies for securing information. Many agencies are being slow in using the cards for access control [1]. It makes sense to have a single proven card, read PIV card, rather than a multiplicity of different technology cards.

There are a number of important activities at the Federal level that conduct work without much visibility. One activity, the Federal Public Key Infrastructure Policy Authority (FPKIPA) consists of members that have cross-certificated with the Federal Bridge and observers. Their work has a direct bearing on digital certificate trust. Digital certificates can have a number of extensions, including the Subject Information Access (SIA). A performance problem with certificates that included this extension was discussed in the FPKIPA April meeting: "*Microsoft reports that the SIA*

(Continued on page 2)

Inside this issue:

Special points of interest:

- IAB—Government working to authenticate non-PIV cards
- Contactless Visa and Master Credit Cards

Web Exploits

People don't expect to get infected when visiting known sites. However, one of the giants, Wal-Mart discovered an exploited Flash vulnerability on their web site [1]. Customers were redirected to other sites where malicious software (malware) is common.

Some domains have more risk than others. Nineteen percent of names ending in "hk" for Hong Kong are said to pose a security problem [2]. Closely behind Hong Kong are site ending in "ch" for China [3].

Last month Web exploits hit the campaign trail. A hacker redirected traffic from BarackObama.com to Hillary Clinton's site [4]. One report indicates that 1.3 % of Google searches turned up at least one malicious page; 5% of web sites have malware; and 65% of web sites are vulnerable [5].

(Continued on page 2)

Government Smart Card Use

(Continued from page 1)

extension brings Vista to its knees, and as a result, the Common Policy certificate cannot be included." [2]

In smart card deployments, the Department of Defense (DoD) made significant progress using Common Access Cards (CAC) [3]. Soon New York State will issue enhanced driver licenses that includes a radio frequency identification microchip and meets the requirements for border crossing [4]. Getting a criminal fingerprint check can take some time. However, one report indicates that the turnaround time for the Automated Fingerprinting Information Systems (AFIS) is fifteen minutes [5].

1. Mabeus, Courtney, Federal Times, *Secure ID cards on slow path to implementation*, May 21, 2008.
2. Federal Public Key Infrastructure Policy authority (FPKIPA) meeting minutes, April 8, 2008
3. Robinson, Brian, Federal Computer Week, *DOD blazes HSPD-12 trail*, June 2, 2008.
4. Lipowicz, Alice, Federal computer week, *N.Y. opts for hybrid driver's licenses*, May 28, 2008.
5. Halperin, Evan, B2G Exchange, *Fingerprint Database Delay Leads to Release of Murder Suspect*, may 30, 2008.

Identity Theft

The University of California, Irvine has seen 155 graduate students victims of a scam where criminals file false tax returns and pocket the refunds [1]. At the Walter Reed Army Medical Center and other military hospitals, 1,000 patients privacy information may have been compromised [2]. Indications are the Walter Reed exploit was due to unauthorized peer-to-peer file sharing [3]. In another case, the *1st Source* bank serving parts of Indiana and Michigan is issuing new debit cards following a security breach [4]. Even small schools are subjected to security breaches. Consider the Pocono Mountain school district in Pennsylvania noticed unusual activity and alerted parents to the possible breach [5]

Victims of identity theft are distributed throughout the entire population. Sometimes the good guys get lucky. Case in point, an 84-year old Georgia woman provided her checking account number after being informed she'd won a million dollars; fortunately she changed her account number before exploitation [6]. So if every check you write has your account information on it, how can you prevent exploitation?

1. McMillan, Robert, IDG News service, *United-Healthcare Data Breach Leads to ID Theft*, June 3, 2008.
2. Mosquera, Mary, Federal Computer Week, *Walter Reed patient data exposed*, June 3, 2008.
3. Poremba, Sue Marquette, SC Magazine, *Walter Reed suffers peer-to-peer data breach*, June 3, 2008.
4. Associated Press, *Bank issues new debit cards after security breach*, June 5, 2008.
5. Schaffer, Scott, WNEP, *Possible Security Breach in School Files*, June 2, 2008.
6. Morgan, Carly Flynn, WMAZ, *State Targets Identity Theft*, June 4, 2008.

> *He that is good for making excuses is seldom good for anything else. — Benjamin Franklin*

Web Exploits

(Continued from page 1)

These percentages are staggering and will eventually necessitate enhanced security measures. How long will it be before smart card readers are standard with new personal computers? When will banks and regulators adapt?

1. Dunn, John E., Techworld, *Wal-Mart website hit by Flash hole*, June 4, 2008.
2. AFP (Hong Kong), *Hong Kong's websites the world's riskiest: survey*, June 5, 2008.
3. Investor's Business Daily, *Internet's riskiest domains ID'd*, June 5, 2008.
4. Naraine, Ryan, ZDNet Blog, *Obama looking for help thwarting Web site hackers*, May 30, 2008.
5. Greenberg, Andy, *Forbes, Where The Web Is Weak*, May 14, 2008.

Monitoring Personal Activities

The technology we take for granted can have other uses. For example, a study was secretly conducted on 100,000 cell phone users to determine how far they traveled from home [1]. Whenever the cell phones were used the phone company recorded the time and location of the nearest cell tower [2]. While such a study would be illegal in the US, it does highlight the capability of the technology. What might a nefarious user do with such information? Could the location of a person ever be used to blackmail them?

Monitoring personal activities is one method for identifying criminal activities. In Sweden, the government there is to vote on allowing phone and email monitoring for local law enforcement [3].

1. Borenstein, Seth, Associated Press, *Study secretly tracks cell phone users outside US*, June 4, 2008.
2. Schwartz, John, The New York Times, *Cellphone Tracking Study Shows We're Creatures of Habit*, June 5, 2008.
3. Ricknäs, Mikael, IDG News service, *Swedish Gov't to Vote on Allowing E-mail, Phone Monitoring*, June 5, 2008.

More Financial News

In past newsletters, examples of bank fraud, hacking, and other exploits were (and will continue to be) reported. The question put forward remains; what percentage of the current meltdown can be attributed to computer crime? Especially given the prediction the credit recession will last another 2 years [1].

Consider the following examples impacting financial institutions. A fifth person pleads guilty in a $25 million bank fraud indictment where a builder was alleged to be running a "fraudulent real estate machine" [2]. In Louisiana, a new charge of trying to steal $20 million from a bank account has been added to wire fraud and money laundering [3]. In Las Vegas, there is a multiplicity of mortgage fraud cases, including one for a dubious $107 million loan [4]. In Florida, a Financial Industry Regulatory Authority (FINRA) member was charged with fraud [5]. A former student finance CEO, involved with $40 million in questionable loans, pleaded guilty to 10 counts of fraud and money laundering [6]. In Newark, a man who sold run-down houses to straw buyers pleaded guilty to a million-dollar scam [7]. In Gettysburg, a former Bank VP was sentenced to 33 months for embezzling $400,000 [8].

In other news, there are fears that the Fed's credit extension will encourage financial institutions to take greater risks [9]. The warning from the Federal Reserve Bank of Richmond president, Jeffrey Lacker, could give rise to more crises [10]. The Fed is getting more involved with financial corporations. For example, The Fed announced its approval of the Bank of America purchase of Countrywide Financial Corporation [11].

Finally, the situation we like to avoid is when regulators close a bank. One report describes the FDIC's stealth tactics leading to the takeover of the First Integrity Bank [12].

1. Siew, Walden, Reuters, *Subprime debacle may spark 2-year credit recession*, June 4, 2008.
2. Davis, Mark, Kansas City Star, *Fifth person pleads guilty in bank fraud*, June 2, 2008.
3. Addo, Koran, Advocate (Louisina), *Zachary man faces charge in bank scam*, June 4, 2008.
4. Farrell, Greg, USA Today, *Las Vegas called 'mortgage fraud ground zero'*, June 3, 2008.
5. Curtis, Carol E., Securities Industry News, *SEC Charges FINRA Board Member with Fraud*, June 2, 2008.
6. Blumenthal, Jeff, Philadelphia Business Journal, *Former Student Finance CEO Yao pleads guilty in fraud case*, June 4, 2008.
7. Sherman, Ted, The Star Ledger, *Newark brains behind mortgage scam admits guilt*, June 4, 2008.
8. WGAL, *Former Bank VP Sentenced For Embezzling*, May 30, 2008.
9. AFP, *Fed officials worry that central bank went too far in crisis*, June 5, 2008.
10. Politi, James, *Financial Times, Banker warns over Fed's credit moves*, June 5, 2008.
11. Robb, Greg, Market Watch, *Fed approves Bank of America purchase of Countrywide*, June 5, 2008.
12. Paletta, Damian, Wall Street Journal, *Anatomy of a bank failure: When the liquidators come calling*, June 8, 2008.

We can draw lessons from the past, but we cannot live in it.—Lyndon B. Johnson

Laptops

We are periodically reminded that laptops are a target of theft. The problem is exasperated when the sensitive data is not encrypted. Case in point, a stolen AT&T laptop contained sensitive information on employees [1]. In another case, a laptop at Stanford University with information on 72,000 employees was stolen [2].

Lost laptops containing sensitive personal information are not limited to the US. For example, the Canadian government lost a laptop containing personal data on 32,000 farmers and took two months to report the incident [3].

In the last newsletter, we referenced reports of an ongoing investigation alleging China clandestinely copied the Secretary of Commerce's laptop hard drive. China has since denied this allegation [4].

1. Kaplan, Dan, SC Magazine, *AT&T management staff data on stolen laptop*, June 4, 2008.
2. Krieger, Lisa M., Mercury News, *Stanford laptop with employee data stolen*, June 6, 2008.
3. UPI, *Personal data on 32,000 farmers missing*, June 5, 2008.
4. AP/USA Today, *China denies hacking U.S. government computer*, June 6, 2008.

IPv6

The NSA is suggesting the migration approach to IPv6 may introduce additional security vulnerabilities such as a dual stack (IPv4 & IPv6 both supported) [1]. Expect to see more problems as IPv6 deployment continues. For example, one report indicates that SMTP (email) over IPv6 was crashing servers [2].

With the migration to IPv6 shouldn't we expect many of the past problems to be corrected? One report indicates there may be a buffer overflow when handling IPv6 data. "*An unspecified buffer overflow error has also been reported in snmplib when handling UDP/IPv6 data.*" [3] Readers may recall that a buffer overflow was one of the exploits used in the Morris Worm back in 1988 [4]. So what has changed to improve security in the last 20 years?

1. Campbell, Dave, Government Computer News, *Gradual move to IPv6 makes time to address security threats*, June 3, 2008.
2. Oswald, Ed, BetaNews, *Apple releases OS X 10.5.3, users report problems*, May 30, 2008.
3. French Security Incident Response Team, *Net-snmp Perl Interface "__snprint_value()" Buffer Overflow Vulnerability*, May 14, 2008.
4. Eisenberg, T., et. al., Communications of the ACM, *The Cornell commission: on Morris and the worm, June*, 1989.

I have not failed. I've just found 10,000 ways that won't work.—Thomas A. Edison Thomas A. Edison

New Deployments

Credit cards with a magnetic stripe are vulnerable to cloning. The credit card industry understands the importance of improving security while maintaining user friendliness. The closest fit is a contactless processor chip. This will necessitate new merchant readers. Visa and the U.S. Bank have introduced a contactless smart card [1]. Similarly, Master card will soon pilot its PayPass contactless chip technology in cell phones [2].

While there is considerable talk regarding the privacy of biometrics, airport security is about to get revealing. Scanners capable of displaying intimate body features are going operational at ten airports [3]. It will be interesting to see if there are privacy challenges to this technology. At Reagan National where the scanners are now operational, some are saying the new scanners are too revealing [4].

1. Centre Daily Times, *U.S. Bank Launches Visa payWave Program on Debit Accounts*, June 2, 2008.
2. Smith, Briony, Computerworld Canada, *MasterCard gets moving on mobile payments*, May 28, 2008.
3. Frank, Thomas, USA Today, *10 airports install body scanners*, June 6, 2008.
4. WJLA, *Travelers Say Airport Body Scanners Reveal More Than Intended*, June 6, 2008.