Femtosecond®

www.femto-second.com

In the News

Volume 1 Issue 18

July 27, 2008

Personal Identity Verification

The Interagency Advisory Board (IAB) held a meeting on Thursday, July 24. Some of the highlights from the meeting follow: the National Institute of Standards and Technology (NIST) published the new version of Special Publication (SP) 800-79-1. This document covers the certification and accreditation (C&A) requirements for PIV Card Issuance (PCI). Separately, NIST has a generic C&A document (SP 700-37). In the generic document, there is flexibility in the approach depending on the environment. In contrast, SP 800-79-1 derives requirements from Federal Information Processing Standards (FIPS) 201 and is therefore completely required.

Interagency Advisory Board (IAB) Meeting

July 24, 2008

The GSA Managed Service Organization (MSO) for PIV has issued over 39 thousand operating PIV cards. This is a significant achievement especially given the number of relying customers. Additionally, the MSO successfully integrated multiple Public Key Infrastructures (PKI) digital certificates into the PIV issuance process. For one agency, the MSO issues the authentication certificate, while the agency provides the encryption and digital signature certificates for the card. Three other agencies have expressed an interest in using their own PKI in conjunction with MSO issued PIV cards.

The Federal Emergency Management Agency (FEMA) continues working first responder scenarios that include a central reporting capability showing where and how users are authenticated in near real-time. Hand-held PIV reading devices set up in front of the GSA auditorium at the IAB were used to verify meeting participant's PIV cards. The results of the authentications were displayed on a separate projected display.

The Department of Defense (DoD) is in the process of upgrading their Common Access Cards (CAC) to PIV compliance. It was mentioned that 600,000 users within the DoD now have PIV compliant cards. In the past, the DoD only allowed a single direction trust path to the Federal Bridge CA. As of last week, this was changed to allow two-way trust. Thus, PIV cards issued by other agencies will be path validated within the DoD space. The DoD is the largest Government department with 3.4 million cardholders. Additionally, approximately 2.5 million cards are issued each year. Of particular interest is the DoD certificate revocation list (crl) size is in the 140—160 million byte range.

In non-IAB news, to date, PIV cards were issued to 450,000 Government and 130,000 contractor personnel [1]. This number appears small given the DoD has issued 600,000 PIV cards. However, the DoD Office of Inspector General identified 6 areas where the DoD

(Continued on page 2)

Financial News

The First National Bank of Nevada and First Heritage Bank were closed by regulators [1]. The larger of these two, the First National Bank of Nevada, had $3.4 billion in assets and $3.0 billion of deposits [2]. It is estimated that the First National Bank will cost the FDIC's insurance fund $862 million [3]. In contrast to the IndyMac takeover, depositors were promised full protection of their funds by the purchasing bank, Mutual of Omaha; thereby preventing the long lines of withdrawers seen in California [4]. In the IndyMac case, there was an ongoing run on the bank that continued into FDIC operation.

Troubles in the financial industry continue with the fourth largest US bank, Wachovia reporting a second quarter loss of $8.9 billion [5]. The current estimate for rescuing Freddie

(Continued on page 2)

Inside this issue:

Cyber-Crime	2
Financial Fraud	3
Counterfeit Money	3
Defrauding the Government	4
Vulnerabilities	4

Special points of interest:

- Over 75% of banks sites are insecure
- Regulators close two banks

Personal Identity Verification

(Continued from page 1)

PIV was not compliant [2].

1. Hardy, Michael, Federal Computer Week, *OMB claims progress on HSPD-12*, July 18, 2008.
2. SecureID News, *DOD not complying with HSPD-12*, July 15, 2008.

Cyber-Crime

New technology has ushered in new criminal elements. Whereas crime once was best described in Sherlock Holmes stories, criminal elements have kept current. Today, Cyber-criminals have organizations modeled after the mafia [1].

The Internet has had the consequence of making some crimes, such as child pornography easier for bad actors. For law enforcement to keep cyber-crime in check, more investment and resources are being applied to the threat. Case in point, in Florida, the CyberCrime unit was expanded to track down child predators [2].

There is pressure to have the large Internet Service Providers (ISP) block child pornography. In the latest example, New York is pressing Comcast to limit distribution of child pornography [3]. This follows Cox Communications announced efforts to target child porn web sites [4]. Other agreements to remove child pornographic newsgroups were reached with Verizon Communications, Sprint Nextel, Time Warner Cable, AT&T, and AOL [5].

At the Federal level, the FBI continues to track child predators by aggressively enforcing child pornography laws. The FBI sponsors the Innocent Images National Initiative (IINI) to combat the proliferation of child pornography/ child sexual exploitation (CP/ CSE) facilitated by an online computer [6].

Child pornography is a good example of unintended consequences of new technology. Similarly, terrorist organizations also use the Internet to convey their messages. The challenge is how best to tame the beast while still reaping the benefits of the Internet. Improved cryptographic controls will likely continue to be deployed to better ensure Internet security. Given that criminals are using strong cryptography, shouldn't law abiding citizens have equal protection?

1. Prince, Brian, eWeek, *The rise of cyber-crime families*, July 21, 2008.
2. Associated Press, *Cyber-Crime Unit opens office in Milton*, July 25, 2008.
3. Information Week, *N.Y. Leans On Comcast To Fight Child Porn*, July 22, 2008.
4. KRNV, *Cox Cable targets child porn Web sites*, July 18, 2008.
5. Washington Post, *National Briefing, Comcast Pressured Over Porn*, July 22, 2008.
6. www.fbi.gov/ innocent.htm

A billion here, a billion there, and pretty soon you're talking about real money–Everett Dirksen

Financial News

(Continued from page 1)

Mac and Sallie Mae is estimated up to $25 billion [6]. This news comes at a time when Sallie Mae's earnings fell 72 % [7].

1. Vekshin, Alison, Bloomberg News, *Regulators Close Two More National Banks*, July 26, 2008.
2. Paletta, Damian, Wall Street Journal, *Two More Banks Fail*, July 26, 2008.
3. Wiles, Russ, Arizona Republic, *Feds shut largest Ariz.-based bank*, July 26, 2008.
4. Myers, Amanda Lee, AP, *No angry lines of customers after bank takeover*, July 26, 2008.
5. AP, *Wachovia has $8.9B loss, exits wholesale mortgage*, July 22, 2008.
6. Davis, Julie Hirschfeld, AP, *Mortgage giant rescue could cost $25b*, July 22, 2008.
7. Bernard, Stephen, AP, *Sallie Mae's 2Q profit falls 72 percent*, July 23, 2008.

Financial Fraud

A dentist in New York was sentenced to 120 months in prison for fraudulently obtaining $2.76 million in mortgage loans [1]. In Illinois, state authorities closed a mortgage company that issued $6.6 million in mortgages based on false employment and income data [2]. A federal grand jury is investigating three of the largest subprime mortgage lenders for possible fraud [3]. In Florida, people with criminal records committed $85 million in fraudulent mortgage loans [4]. Finally, in Texas, a man pleaded guilty to a stock scam that bilked investors out of $ millions [8].

1. FBI, *Dentist Sentenced to 120 Months in Prison for Multi-Million Dollar Mortgage Fraud*, July 21, 2008.
2. Chicago Tribune, *State shuts loan firm for alleged fraud*, July 25, 2008.
3. Baltimore Sun/LA Times, *U.S. probes big subprime lenders*, July 24, 2008.
4. AP, *Florida to address criminals in mortgage industry*, July 24, 2008.
5. FBI, *Dallas Man Pleads Guilty in Multimillion Stock Scam Involving Tulsa Companies*, July 22, 2008.

Counterfeit Money

Usually, the money one gets from a bank is assumed to be good. However, one report indicates a central Florida bank was dispensing counterfeit $100 bills [1]. Perhaps the machines used by the banks are no longer able to detect some of the counterfeit currently. Case in point, in New York, bank counterfeit checking devices initially failed to detect bogus $20 bills [2].

Bogus money is a continuing problem. Consider the example in Wisconsin, where merchants received a number of bogus $10 bills [3]. In Memphis, a man was arrested for passing bogus $100 bills [4]. In Vermont, two people are being investigated for allegedly money counterfeiting [5].

Of course sometimes police do not have far to go in making a bogus money arrest. In Alabama, police arrested a man for posting another's bond using a counterfeit $100 [6]. In Holyoke, a couple was arrested passing bogus money at the Ingleside Mall [7]. In Tennessee, five were arrested for using bogus money to purchase 99% bogus marijuana [8]. In Missouri, a man found with 16 bogus $100 bills pleaded guilty to counterfeiting [9].

In Troy, New York, police described some of the counterfeit money made using computers and Kool-Aid for the coloring as top quality [10]. However, there is a class of bogus money, referred to as super notes. Supernotes are of such high quality, they may not be detected until they reach a Federal Reserve Bank. So where do these notes come from? In one case, a woman was arrested for trying to bring $380,000 supernotes into the country from Taiwan [11]. The supernotes appear to have the same fiber content as legitimate US currency and banks have found over $50 million so far [12].

1. WKMG (Channel 6 Orlando), *Bank Gave Counterfeit Bills, Couple Says*, July 22, 2008.
2. WFFF (Fox 44), *Troy, NY Cops Bust Rutland Pair in Funny Money Scheme,* July 23, 2008.
3. Dunn County News, *Menomonie merchants report counterfeit cash*, July 23, 2008.
4. Myers, Shane, WPTY (ABC 24), *Man Arrested for Using Counterfeit Money in Memphis*, July 21, 2008.
5. WCAX, *Rutland Duo Tied to Multi-State Counterfeit Scheme*, July 23, 2008.
6. Cason, Mike, The Birmingham News, *Man uses fake money to try to bond another out of Hoover jail*, July 18, 2008.
7. Walsh, Nate, WGGB (ABC 40), *Alleged Counterfeiters Hide Funny Money in Buttocks*, July 18, 2008.
8. WKSR (Pulaski, TN), Buying Fake Drugs With Fake Money, July 19, 2008.
9. KSPR, *Morgan Co. Man Pleads Guilty of Counterfeiting*, July 22, 2008.
10. WNYT, *Mayor's wife falls victim to funny money*, July 11, 2008.
11. Lee, Henry K., San Francisco Chronicle, *Woman charged with smuggling counterfeit cash*, July 18, 2008.
12. Fox News, *Mysterious $100 'Supernote' Counterfeit Bills Pop Up Worldwide*, January 14, 2008.

> *I figure you have the same chance of winning the lottery whether you play or not—Fran Lebowitz*

Defrauding the Government

With the number of government programs in place, fraud and proper oversight are continuous challenges. For example, in Oregon, the FBI arrested a Russian citizen for receiving $759,340.94 in fraudulent Medicare claims [1].

The Oregon example is small compared to other cases where the government was defrauded. In overseeing government contracts, maintaining audit integrity can be challenging. Case in point, the GAO reports that the Defense Contract Audit agency (DCAA) was pressured by contractors and senior government officials to limit negative findings [2]. To its credit, following the GAO report, the DCAA requested an investigation into the allegations [3]. In West Virginia, 4 pleaded guilty submitting fraudulent Medicare claims worth more than $10 million [4]. In Oklahoma, 16 people face charges for fraudulently exchanging $838,000 in food stamps for cash [5]. In Virginia, a nurse pleaded guilty to her part in a $14 million home health care Medicaid fraud [6].

Fraud impacts all levels of government. Consider the case in California where 21 people were arrested for $2 million in welfare fraud [7].

1. FBI, *Russian Citizen charged in $1 Million Medicare Fraud*, July 23, 2008.
2. Manning, Stephen, AP, *GAO says auditors pressured on Pentagon contracts*, July 23, 2008.
3. Reuters, *Pentagon auditors request probe after criticism*, July 25, 2008.
4. AP, *4 plead guilty to Medicare fraud*, July 19, 2008.
5. Schulte, David, Tulsa World, *16 Tulsans face food stamp fraud charges*, July 25, 2008.
6. Green, Frank, Richmond Times Dispatch, *Nurse pleads guilty to Medicaid fraud*, July 19, 2008.
7. AP, *LA County accuses 21 people of welfare fraud,* July 24, 2008.

Always be sincere, even if you don't mean it—Harry S Truman

Vulnerabilities

One report indicates that over 75% of bank web pages have an exploitable security vulnerability [1]. Researchers found that many bank sites redirect users to third party locations [2]. The problem of bank security is not limited to the US. Consider that according to the Japanese Bankers Association, 5.9 billion yen was returned to 53,102 bank account holders that were victims of bank transfer scams [3].

Readers may recall from the last Newsletter that a computer tech in San Francisco installed his own administrative password. This week, prosecutors say the tech booby trapped the network [4].

Recently, there has been much discussion regarding a Domain Name System exploit. Last week, researchers published attack code that can redirect users to bogus sites [5]. There are reports that the exploit is currently in use on a small scale [6]. The exploit allows cache poising, is being weaponized in the field; and as of last Thursday (7/24/08) over half the sites tested were still vulnerable to the exploit [7].

1. Kirk, Jeremy, Computerworld Security, *Design flaws impair security at banking sites*, July 23, 2008.
2. AP, *Study sees online banking flaws*, July 23, 2008.
3. Mainchi Daily News (Japan), *5.9 billion yen to be returned to bank transfer scam victims*, July 26, 2008.
4. Gonslaves, Antone, Information Week, *San Francisco Computer Tech Set Booby Trap In City Network*, July 24, 2008.
5. Keizer, Gregg, Computerworld Security, *Researchers unleash DNS attack code*, July 24, 2008.
6. BBC News, *Attacks begin on net address flaw*, July 25, 2008.
7. AFP, *Hackers get hold of critical Internet flaw*, July 25, 2008.