Femtosecond®
www.femto-second.com

In the News

Volume 1, Issue 1

March 30, 2008

Smart Card Business Roundtable First Meeting

The kick-off meeting took place on March 26, 2008 at suite 800, 888 14th NW. The purpose of the roundtable is for information exchange between business and Government. Bob Donelson discussed the challenges of change. He used the analogy that bodies at rest tend to remain at rest. On the political front, there will be change originating from the new administration. Bob described the original business case prepared by the Interagency Advisory Board (IAB) for using smart cards to their fullest. With the Homeland Security Presidential Directive 12 (HSPD-12) mandate requiring Personal Identity Verification (PIV) cards; the biggest expense is addressed. Next Roy Hayes made a presentation that emphasized the smart card is the enabler. He described a six step PIV implementation and emphasized the need to demystify the technology. Finally, Russ Davis provided an overview into current IT security issues. He described some of the advantages of having a good PIV support program instead of supporting a multiplicity of solutions. The audience suggested that a Webinar format

Bob Donelson discussing organizational change

From left to right: Bob Donelson (Organizational Change Future Workplace, LLC), Russell Davis (Femtosecond), and Roy L. Hayes (Systems Engineering, Inc.)

(Continued on page 2)

More Trouble in the Financial Industry

This week, the losses attributed to the Subprime crises increased to $460 billion [1]. This comes after the news that the Societe Generale bank in France lost $7.1 billion to a single insider [2]. The question here is how good are the internal security controls in other financial institutions? What are the US financial industry losses resulting from IT security breaches?

We have seen unprecedented effort by the Fed to provide relief to a bank normally protected by the FDIC [3]. However, the FDIC relies on the Bank Insurance Fund (BIF) and Savings Association Insurance Funds (SAIF) for assets needed to cover insured bank loss. Unfortunately, these funds together are perhaps below $50 billion in total. Perhaps this is

(Continued on page 2)

Inside this issue:

Special points of interest:

- First Smart Card Business Roundtable
- BIF and SAIF funds inadequate to cover bank losses

More Trouble in the Financial Industry

(continued from page 1)

why the FDIC posted help wanted to fill a number of job positions assigned to bank receivership on one day (February 20, 2008).

Back in 1990, during the troubled Savings and Loan Crisis, a letter was sent to the Chairman on the Judiciary, Congressman Jack Brooks [4]. The letter posited that financial institutions were reluctant to report IT security losses and that since the Government was bailing out failed Savings and Loan companies, this was an excellent time to uncover what the true losses are.

To appreciate the problem companies' face in reporting IT security losses, consider what happened to Egghead Online [5]. After being the good steward and reporting that a hacker had gained access, the company went insolvent in under a year. So the incentives for reporting losses include collecting unemployment compensation.

To be sure, the Fed actions are absolutely critical for the financial markets. There can be no question that only the Fed has the ability to quickly act to dynamic changes in the financial industry. As noted by the AP, "It also has employed Depression-era provisions to provide money to investment banks" [6]. There is a realization ion that action must be taken quickly, especially since the US is a trade imbalance dwarfs the Federal deficit. One proposal is the creation of a new Fed controlled cross-cutting Government regulatory agency that can quickly respond to the latest crisis [7].

The financial industry illustrates an area that could benefit from the security afforded smart cards. The microprocessor on the smart card operates separately from host operating systems. Proper utilization of smart cards provides a powerful security control that established a person's identity. Without strong Identification and Authentication, there is little basis for security.

Hopefully, the financial regulators will take this latest opportunity to ensure that adequate technology is used for internal controls. If the financial institutions cannot improve their security, Fed interdiction may become the norm rather than the exception. Obviously the opportunity that presented itself during the Savings and Loan crisis was not seized.

1. Yidi, Zhao, March 25 (Bloomberg), *Wall Street May Face $460 Bln in Losses, Goldman Says* .
2. Laurent, Lionel, *Societe Generale Boss Feels The Heat*, Forbes, January 29, 2008.
3. Bel Bruno, Joel and Raed, Madlen, Associated Press, *JPMorgan to get Bear Stearns for $2 a share*, March 17, 2008.
4. www.femto-second.com/papers/NewsLetters/JackBrooks.pdf
5. Rosencrance, Linda, Computerworld, *Egghead.com finally cracks, shutters shopping site*, October 29, 2001.
6. Crutsinger, Martin, Associated Press, *Fed offers $100 billion more to banks*, March 28, 2008.
7. Andrews, Edmund L, New York Times, *Treasury Dept. Plan Would Give Fed Wide New Power*, March 29, 2008.

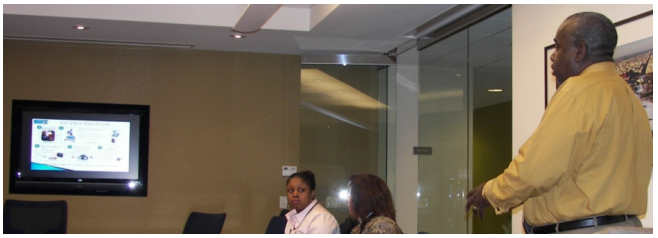
"We cannot direct the wind but we can adjust the sails." - Anonymous

Smart Card Business Roundtable First Meeting

(continued from page 1)

should be considered for future meetings so that people in other regions could benefit from the exchange. For more information go to www.femto-second.com/RoundTable/smart_card_round_table.htm.

The first meeting brought together Government and industry to discuss the next steps following HSPD-12. Monthly meetings are planned for the foreseeable future and special working groups will likely address specific issues that arise.



Roy L. Hayes presenting at the First Smart Card Business Roundtable

Malicious Software (Malware)

The Hannaford supermarket chain has identified Malware running on their servers [1]. There have been over 2,000 cases of fraud connected with the grocery store chain attack and an estimated 4.2 million credit card numbers were stolen [2].

The malware was loaded at the 300 Hannaford stores and customers that swiped their credit cards had their information stored and later forwarded to off-shore locations [3]. This is an example that illustrates one of the weaknesses of a magnetic credit card. Had smart cards been used, no malware on the point-of-purchase machine could have compromised the private key on the smart card. A question here is how much loss are we willing to assume?

1. Associated Press, *Malware cited in Hannaford breach*, March 28, 2008.
2. Reuters, Credit card data stolen from supermarket chain, March 17, 2008.
3. Kerber, Ross, Boston Globe, Advanced tactic targeted grocer, March 28, 2008.

Rush to Market Vulnerabilities

Businesses are in a race to get their products to market. This results in less time to provide adequate security and testing.

The latest example is the Microsoft Excel security patch [1]. There are reports that hackers are actively exploiting un-patched versions.

We tend to focus exclusively on software problems; however, there are cases where hardware companies have similar problems. AMD has released new processors that fix a hardware flaw [2].

1. Kirk, Jeremy, Info World, *Hackers seize on Excel vulnerability,* March 26, 2008.
2. Santo Domingo, and Kackman, Mark, PC Magazine, AMD Fixes Phenom, Adds Triple-Core Processors, March 27, 2008.

"Give me six hours to chop down a tree and I will spend the first four sharpening the axe." - Abraham Lincoln

Biometrics

The time card is being replaced by fingerprint scanners. In another example of change, companies such as Hilton Hotels and Dunkin Doughnuts tracks employee arrivals using fingerprints [1]. Systems are available that replace the punched clock and barcode schemes. [2] One of the selling points is to prevent another employee from punching the clock for an absent person.

Perhaps a larger issue is the idea of "big Brother" types of security controls that track our every whereabouts. Companies that embark on biometric approaches to tracking employees will need to address privacy issues. A main challenge is in educating the workforce that there is little difference in the authentication mechanism (punched time or biometric). What the company does with the tracking of employee actions is another matter that might require vetting through trade unions and privacy officials.

It is worth mentioning that a smart card containing a private encryption key provides come capabilities that a biometric does not. For example, an NIH researcher lost a laptop with information on 2,500 patients . A smart card could have been used in conjunction with commercial software to encrypt the sensitive information on the laptop.

1. Caruso, David B., Associated Press, *Fingerprint scans replace clocking in*, March 26, 2008.
2. Morochove, Richard, PC World, *Lift a Finger (print) to Track Employee Time*, March 8, 2008.
3. Ferris, Nancy, Federal Computer Week, *NIH researcher loses laptop with data on 2,500 patients*, March 24, 2008.

Why Digital Signatures?

As if US investment banks were not in enough trouble, it seems that Lehman was defrauded based on forged documents [1]. The amount of the fraudulent transactions was approximately $353 million [2]. The case has been referred to Japanese police and Lehman plans to sue.

The question here is will reliance on paper documents wane? A smart card with proper digital signature capability can remove the ambiguity of document authenticity. At a time of sub-prime crisis, can companies afford fraudulent losses? Another question is since most corporations have been victimized by hackers and malware, what is happening to US financial institutions?

1. Biggadike, Oliver, and Ueno, Takashi, Bloomberg, Lehman to Sue Japan's Marubeni, Claiming Loan Fraud, March 29, 2008.
2. Reuters, Toyko, Lehman hit by fraud involving Marubeni employees, March 29, 2008.

The Hacker Contest Winner Is

"If you want to make enemies, try to change something." - Woodrow Wilson

There was a Hacker super bowl that included a prize for the hacker that could first break into a Mac, Vista, or Linux [1]. The event was hosted at the CanSecWest security conference. During the first day, limited to network attacks, there was no successful attack. However, on the second day, Charlie Miller broke into the Mac using a previously undisclosed "0day" attack [2]. The reader should be cautions and not interpret that the Vista and Linux operating systems are secure. Years ago, when the National Security Agency (NSA) evaluated security, the evaluations took a long time for a reason.

1. McMillan, Robert, InfoWorld, *Hacker Super Bowl pits Mac OS vs. Linux, Vista*, march 27, 2008.
2. McMillan, Robert, PC World, *Gone in 2 Minutes: Mac Gets Hacked First in Contest*, March 27, 2008.

Outsourcing Risks.

It has been common practice for Government agencies to outsource whenever work needs to be done. There is some risk however that should be addressed. Consider the passport scandal where the presidential candidate's passport records were accessed [1]. It was discovered that the unauthorized access was done by as yet unnamed private contractors [2].

Outsourcing security considerations should be considered before an outsourcing decision is made. Some Government agencies do not want to be burdened with security requirements and think outsourcing relieves them of the burden. As the Department of State has just learned the actions of private contractors reflects directly on the department.

Senator Obama has called for an inquiry [3]. What will the final cost in labor and dollars be to the Department of State when this matter is concluded?

1. Lee, Matthew, Time, More US Passport 'File Breaches', March 27, 2008.
2. Flarherty, Anne, Associated Press, Passport scandal raises questions on private contractors, March 25, 2008.
3. CNN, Obama urges inquiry into passport snooping, March 21, 2008.