Femtosecond®
www.femto-second.com

In the News

Volume 2 issue 1

January 4, 2009

IT Security

One ever present risk is that at some point in the future, past algorithms will be cracked. For historical archives, this may necessitate other controls to ensure archived copies have not been tampered with. For example, older US currency no longer in circulation, such as the $500 bills are often sealed in plastic where some third party vouches for the authenticity of the bill inside. This is necessary due to the advances in counterfeiting. The same threat exists for digitally signed legal documents. We know that at some future date, technology will allow forging these documents. For example, a team of researchers the United States, Switzerland, and the Netherlands used 200 PlayStation 3 video game consoles to defeat some of the PKI approaches supported by many commercial, Certification Authorities (CA) [1]. The problem is that popular browsers pre-populate with a number of CA certificates that are vulnerable. Consumers connecting to bogus web site would see the SSL locked key and think they are secure when in fact they are not. The Chaos Communication Congress unveiled a vulnerability to the MD5 hash algorithm still used by some CA's [2]. In general, if a bogus document can be made to result in the same hash as a legitimate signed document, then the forgery properly validates. Six CA vendors issued certificates in 2008 using the weak and exploitable hash algorithm: RapidSSL, FreeSSL, TC TrustCenter AG, RSA Data Security, Thawte, and verisign.co.jp [3]. Microsoft and Mozilla are working with affected certification authorities to ensure they update their certificates [4].

Readers may recall the Year 2000 Bug concerns that computers would fail during the millennium roll over. As it turned out, a leap year problem plagued owners of the Microsoft 30-Gig Zune players when their devices froze on December 31 due to a bug where 2008 was programmed for 365 days and not 366 (leap year) [5]. On December 31, Zune users trying to start their device saw a Zune image as the device froze [6]. Microsoft recommended waiting for 24 hours and the device would return to normal [7]. However, on January 1, Zune users were still having trouble getting their devices functioning again [8]. In other Microsoft news, a trial version of Windows version 7 not scheduled for release until January was leaked to Internet sites in late December [9].

In Government news, FEMA is investigating how a spreadsheet with 16,857 lines of privacy information on Hurricane Katrina victims was posted on one of its web pages [10]. Web based problems are not limited to the US. For example, the Industrial and Commercial Bank of China suffered a very costly 23 minute computer glitch when it traded gold for six times its rate

(Continued on page 2)

Economic News

When Lehman Brothers filed for bankruptcy, there was a considerable loss of value. Because of the unplanned bankruptcy, $75 billion more was lost than would have been the case of a planned bankruptcy [1]. This illustrates the impact of fast transaction technology in today's world.

In other news, the US Securities and Exchange Commission Inspector General will testify before the House Financial Services Committee regarding the Madoff Ponzi scheme [2]. The list of Madoff assets will not be made public [3]. Moreover, the trustee overseeing the Madoff bankruptcy, Irving H. Picard, is requesting broad subpoena powers in trying to determine where the assets are [4]. In Austria, the Government there took over the Bank Medici that had a $2.1 billion exposure to the Madoff Ponzi scheme [5]. For the few that withdrew money from Madoff earlier,

(Continued on page 2)

Inside this issue:

Special points of interest:

- MD5 exploit used to make fake digital certificates
- Leap year bug freezes 30-G Zune players
- Computer glitch caused Chinese bank to lose money when gold traded for 6 times it rate

IT Security

(Continued from page 1)

[11].

As mobile devices increase in sophistication the number exploits increases. For example, older versions of Nokia cell phones (S60 interface versions 2.6 to 3.1) will crash when a specially crafted Internet email is received [12]. Elsewhere overseas, the Indian Computer Emergency Response Team (CERT-In) estimated that over 100 cyber attacks originated from Pakistan since the November 26th Mumbai attack [13]. For example, the Indian Eastern Railway website was hacked allegedly in response to the Pakistan air space violation [14].

1. Ricadela, Aaron, Business Week, *Cracks Emerge in a Web Security Scheme*, December 30, 2008.
2. Fox Business News, *VeriSign Transitions All New RapidSSL Certificates to SHA-1 Algorithm in Response to Newly-Published Security Threat*, December 31, 2008.
3. Claburn, Thomas, Information Week, *200 Sony PS3s Harnessed To Crack Secure Site Certification*, December 31, 2008.
4. Adhikari, Richard, Internet News, *Mozilla, Microsoft Move to Nix Web Security Flaw*, December 31, 2008.
5. Wortham, Jenna, New York Times, A Year Ticks Over, and Zunes Get Hiccups, December 31, 2008.
6. Kim, Ryan, San Francisco Chronicle, *Zune users wake up to find their music gone*, January 1, 2009.
7. Hackman, Mark, PC Magazine, *Zune Issues Caused by Leap Year Bug*, December 31, 2008.
8. Skillings, Jonathan, Cnet, *New Year's hangover for Zune users*, January 1, 2009.
9. McDougall, Paul, Information Week, *Windows 7 Leaked To The Internet*, December 30, 2008.
10. Lipowicz, Alice, FCW, *FEMA investigates breach of Katrina victims' private information*, December 24, 2008.
11. Reuters, *Easy come, easy go after gold glitch*, December 29, 2008.
12. Ray, Bill, The Register (UK), *Nokia 'Curse of Silence' SMS exploit uncovered*, January 2, 2009.
13. Bagga, Bhuvan, India Today, *India has to gear up to face the virtual assault*, January 2, 2009.
14. Express News (India), *Hackers deface Eastern Rail website*, December 25, 2008.

An optimist stays up until midnight to see the new year in. A pessimist stays up to make sure the old year leaves–Bill Vaughn

Economic News

(Continued from page 1)

this money might have to be returned for redistribution to all victims [6]. One consequence of the Madoff scheme is that regulators are now probing other money managers suspected of using similar tactics [7].

In other news, E*Trade was fined $1 million by the Financial Industry Regulatory Authority for failing to establish policies to prevent money-laundering [8].

1. McCracken, Jeffrey, Wall Street Journal, *Lehman's Chaotic Bankruptcy Filing Destroyed Billions in Value*, December 29. 2008.
2. Katz, Ian, Bloomberg, *Markopolos, SEC Inspector General Will Testify on Madoff Scheme*, December 31, 2008.

3. Scheer, David, and Dodds, Allan, Bloomberg, *Madoff's Asset List Won't Be Made Public, U.S. Regulator Says*, January 1, 2009.
4. Henriques, Diana B, New York Times, *Madoff Trustee Seeks Wide Power to Subpoena*, January 2, 2009.
5. CNN, *Austria takes over bank hit by Madoff case*, January 3, 2009.
6. Hosenball, Mark, Newsweek, *Made Money With Madoff? Don't Count On Keeping It*, January 3, 2009.
7. Scheer, David, Bloomberg, *SEC Said to Examine More Ponzi Schemes After Madoff*, January 2, 2009.
8. Kell, John, Wall Street Journal, *E*Trade Fined $1 Million Over Monitoring Lapses*, January 2, 2009.

Goodbye 2008

The new year is here and the 2008 is but a memory. Last year, the stock market suffered the worst year since the Great Depression [1]. Overall, the stock markets and price of oil fell during the year of financial turmoil. The number of FDIC insured banks shuttered by regulators stood at 25 [2]. However, the non-FDIC insured banks were big newsmakers for 2008. In march, Bear Sterns, the 5th largest investment bank required a Government bailout [3]. The bank was absorbed by JPMorgan Chase after what was called a liquidity crisis.

Up until July 11, the price of oil kept increasing reaching a high of $147.27 on July 11 [4]. Later that same day, IndyMac was closed by regulators [5]. Note that following the collapse of IndyMac, oil never reached the same high.

The next shock came with the announcement that Freddie Mac and Fannie Mae were placed into Government conservatorship (Government control) [6].

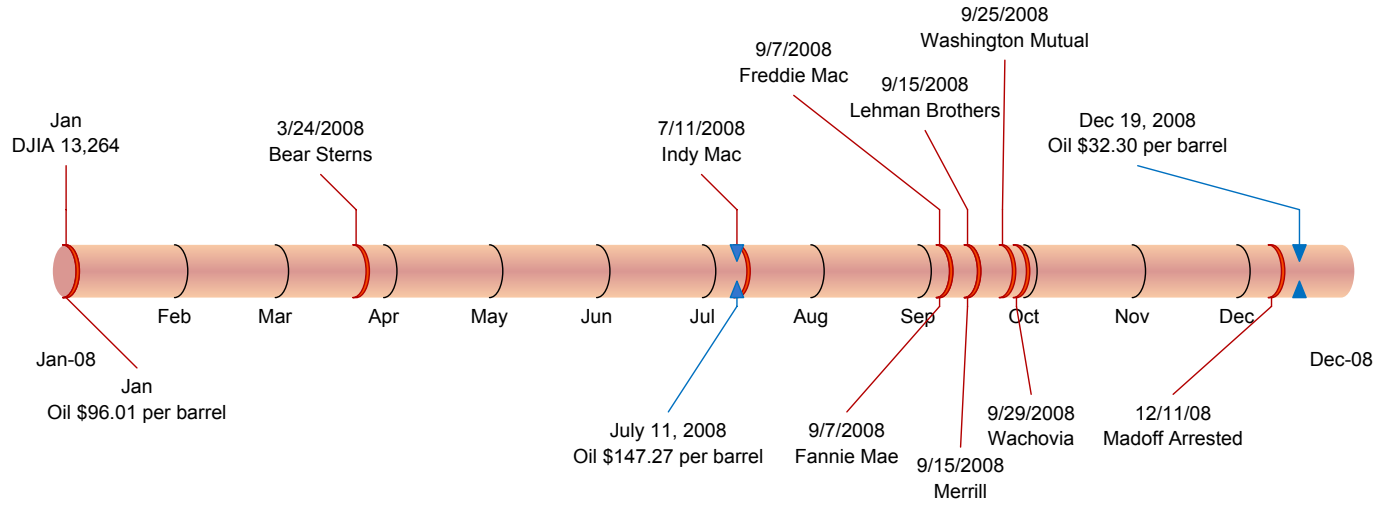
Then came, perhaps the most devastating event of the year on September 15 when Lehman Brothers filed for bankruptcy [7]. This purged any chance of a near term recovery. The next domino to fall was Washington Mutual [8]. Days later, Wachovia was forced to sell [9].

The markets continued to test the bottom and then along came the largest Ponzi scheme on record, the $50 billion Madoff fraud on December 11 [10]. One estimate places the losses on Wall Street at $6.9 Trillion for the year [11]. We can only hope that 2009 will be a good year and 2008 a distant memory. On a positive note, in the first trading day of 2009, the market rose over 250 points [12].

1. Gray, Alan, Financial Times, *US stocks suffer worst year since Great Depression*, December 31, 2008.
2. UPI, Texas, *Georgia banks shuttered*, December 13, 2008.
3. Crutsinger, Martin, ABC News, *Government to Bail Out Bear Sterns*, March 14, 2008.
4. Forbes, *London shares close lower, in bear market; oil hits $147; U.S. weaker*, July 11, 2008.
5. Clifford, Catherine, and Isidore, Chris, CNN Money, *The fall of IndyMac*, July 13, 2008.
6. Kopecki, Dawn, and Vekshin, Alison, Bloomberg, *Fannie, Freddie Capital Concerns Prompt Paulson to Take Control*, September 7, 2008.
7. Wam, Allen, and Cimino, Adria, Bloomberg, *U.S. Stock-Index Futures Tumble on Lehman; AIG, JPMorgan Fall*, September 15, 2008.
8. Comlay, Elinor, and Stempel, Jonathan, Reuters, *WaMu is largest U.S. bank failure*, September 25, 2008.
9. Lepro, Sara, AP, *Wells Fargo acquiring Wachovia for $15.1 billion*, October 3, 2008.
10. Glovin, David, and Scheer, David, *Bloomberg, Madoff Charged in $50 Billion Fraud at Advisory Firm*, December 11, 2008.
11. Merle, Renae, Washington Post, *Wall Street's Final '08 Toll: $6.9 Trillion Wiped Out*, January 1, 2009.
12. Paradis, Tim, AP, *Wall Street enjoys upbeat start to 2009*, January 2, 2009.

Those parts of the system that you can hit with a hammer are called hardware; those program instructions that you can only curse at are called software—

Anonymous

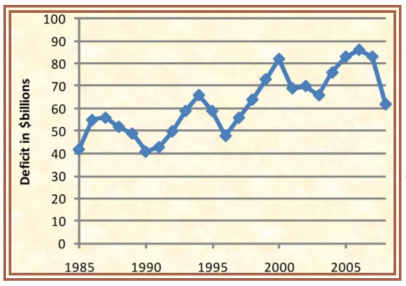


Asian News

In a further sign of protectionism, starting January 1, China will impose a 10% tax on loans made to Chinese banks from overseas lenders [1]. Elsewhere in China, ringleaders of a $2 billion software pirate gang were sentenced from 1½ to 6½ years in prison [2].

In the Middle East, there is currently a shooting war between the Hamas terrorist group and Israel. Some of the missiles raining down on Israel are sophisticated Chinese rockets [3].

In Japan, it is estimated that 85,000 part time and 3,300 permanent employees will lose their jobs between October and March [4]. By contrast, in the US, for the week ending December 27, first time unemployment claims fell to 492,000 [5]. Having a strong export oriented economy has kept Japanese workers employed. The trade imbalance with Japan has lasted decades will continue as the value of the Yen fell to a three week low against the dollar [6]. In the latest Census trade news for October, the trade deficit with Japan was $6,046.85 million, second only to China. With such staggering trade deficits, how could the value of the dollar increase?



US Trade Deficit with Japan Through October, 2008

1. Reuters, *Foreign banks ask for China tax delay*, December 29, 2009.
2. AP, *Chinese software pirates get prison sentences*, December 31, 2008.
3. Katz, Yaakov, Jerusalem Post, *Latest rockets manufactured in China*, January 1, 2008.
4. Kageyama, Yuri, AP, *Japan's jobless fill tent village in Tokyo park*, January 3, 2008.
5. Reddy, Sudeep, Wall Street Journal, *Jobless Claims Decline but Remain High*, January 1, 2009.
6. McGee, Jamie, and Xie, Ye, Bloomberg, *Euro Falls for First Week Since November on ECB Rate Outlook*, January 3, 2008.

Heavier than air flying machines are impossible– Lord Kelvin (1895)

Fake CA Certificates

Adding to other exploits, fake digital certificates can now be creating MD5 hash values identical legitimate certificates [1]. When setting up an SSL session or passing a signed message, the receiver would check the bogus certificate and it would path validate correctly. The National Institute of Standards and Technology (NIST) continues to look for ever stronger hash algorithms, recognizing that future advances could allow future digital certificate exploits. For example, in 2007, the NIST embarked on soliciting algorithms for the next generation of hash algorithms [2].

In 2005, one tool was developed to search for multi-bit consistencies (read weaknesses) and was applied against the NIST SHA-256 algorithm [3]. The approach used a Statistical Process Control (SPC) threshold (mean plus three standard deviations) across every two bit patterns in the resulting SHA-256 values. Large numbers of hash values were calculated in sequential order and the statistics for each two bit sequence recorded. The results indicated there were some consistencies (weaknesses) but not how to correct the problem. The theory is that if there are 2-bit weaknesses, they will be detected when the SPC threshold is exceeded.

This does not mean there is currently any exploit that places Public Key Infrastructures (PKI) at risk. It does however demonstrate there are as yet undiscovered exploits that could dramatically impact future e-commerce. In any cryptographic algorithm, predictability is a weakness. For example, the Data Encryption Standard (DES) has weak keys, such as all zeros or all ones.

1. Jackson, Joab, *SSL certs busted*, December 31, 2008.
2. Federal Register, *Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family*, November 2, 2007.
3. Davis, Russell, www.femto-second.com/papers/SHA256LimitedStatisticalAnalysis.pdf, *SHA-256 Limited Statistical Analysis*, 2005.