Femtosecond®
www.femto-second.com

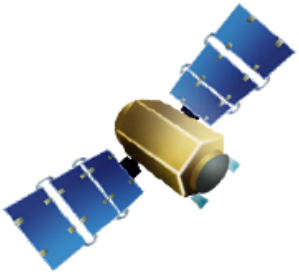
In the News

Volume 1 Issue 36

November 30, 2008

IT Security News

In a Business Week article, there is a suggestion that a successful cyber-attack at the Goddard Space Flight Center culminated with the Röntgen Satellite (ROSAT) satellite pointing at the sun; thereby rendering the spacecraft useless [1]. The satellite sun pointing event took place on September 20, 1998 at 0:47 UT and the HRI UV filter was destroyed [2]. "*Shortly before a revised version of the AMCS software was uplinked an 'accident' happened on 20th September: during a slew the pointing direction of the satellite came close to the sun; as a result the HRI was irreversibly damaged*" [3].



Back on Earth, while financial markets are down, the cybercrime economy is booming [4]. In one example, hackers are breaking into companies to gain access to the payment processing system so they can verify if on-line stolen credit card numbers are good [5]. The next administration will be confronted with cybersecurity protection issues, including completion of the Personal Identity Verification (PIV) card deployment [6]. Cost will be a dominant factor in any solution. For example, a Verizon Business VP argues that too much is spent in the wrong types of security and that servers (not PC) are the big risk [7]. From the telecommunication company's point of view this is perhaps a correct statement; however botnets and compromised PCs are a dominant world cost. Consider if 1 server results in $1 million in loss how does this compare against 10 million PCs with $100 loss per machine? The PC loss is $1 billion compared to $1 million. In other news, there is a worm referred to as Win32/Conficker.A that is exploiting a security hole that Microsoft patched last October [8]. Following the brief reprise when McColo was shut down, junk email has returned to full annoyance level with the return of spamming botnets [9]. Spammers are reestablishing connections to the infected ***Zombie*** machines bringing the botnet back to its full capability [10]. As the holiday shopping on-line cyber criminals are at the ready. For example, cyber criminals tend to come out in force as holiday shopping increases [11]. It is suggested that cybercrime will become as destructive as the credit crisis if international regulation and cooperation are not improved [12].

1. Epstein, Keith, and Elgin, Ben, Business Week, *Network Security Breaches Plague NASA*, November 20, 2008.
2. NASA, ROSAT News Number 66, October 15, 1998.

(Continued on page 2)

Economy

Perhaps business is about to rebound. Case in point, once the doors opened, anxious shoppers at a Wal-Mart trampled a store worker who unfortunately died [1]. Last Sunday, news filtered out that the government was exploring ways to rescue Citigroup [2]. As the week went on, the Government came up with a plan to insure up to $249 billion of $306 billion mortgage related debt [3]. To reduce their expenses, Citigroup plans to halt dividend payments [4]. Meanwhile, the number of problem banks tracked by the FDIC increased from 117 ($78 billion in assets) in the second quarter to 171 ($115.6 billion in assets) his quarter [5]. This number of problem banks is the highest since the end on 1995 [6]. In a sign of the times, the FDIC is allowing firms without bank charters to bid on failed bank assets [7]. In fresh signs of deflation, the yield rate for 10 year Treasury debt fell below 3% for the first time in

(Continued on page 2)

Inside this issue:

After SP 800-116	3
Asia	4
Crime	4

Special points of interest:

- Did hackers render the ROSAT satellite useless in 1998?
- Number of problem banks rises to 13 year high
- Yield on 10-year Treasury debt falls below 3%, lowest in 50 years

IT Security News

(Continued from page 1)

3. NASA, ROSAT News Number 67, November 3, 1998.
4. Leyden, John, The Register, *Booming cybercrime economy sucks in recruits*, November 24, 2008
5. Robertson, Jordan, AP, *Hands-off hackers: Crooks opt for surgical strikes*, November 24, 2008.
6. Vijayan, Jaikumar, Computer World Security, *Obama administration to inherit tough cybersecurity challenges*, November 19, 2008
7. Tippett, Peter, eWeek, *The economics of security*, November 24, 2008.
8. Mills, Elinor, CNet News, *Internet worm exploits Windows vulnerability*, November 26, 2008.
9. Keizer, Gregg, Computer World, *Massive botnet returns from the dead, starts spamming*, November 26, 2008.
10. Kirk, Jeremy, IDG News Service, *Spammers Regaining Control Over Srizbi Botnet*, November 26, 2008.
11. Wolverton, Troy, The Mercury News, *Cybercriminals are shopping for holiday steals*, November 24, 2008.
12. Marsh, Sarah, Reuters, *Cybercrime as destructive as credit crisis: experts*, November 19, 2008.

Economy

Failure is success if we learn from it–Malcolm S. Forbes

(Continued from page 1)

50 years [8].

There remains much discussion on a bail-out for the big three automakers. To better understand what they are up against, consider that GM bonds due in 2033 reached an effective yield of 44.5% [9]. The increased cost of borrowing money comes at a time when the markets are soft. The big 3 are seeking $25 billion in loans for a lower rate of interest [10].

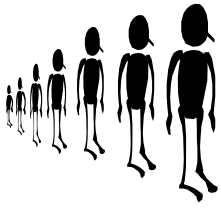
Projections for the Federal deficit now exceed $1 trillion for this fiscal year [11]. As the economy weakens, and the Federal deficit increases, expect greater pressure to shrink budgets. For example, President-elect Obama vowed to scour wasteful spending form the federal budget [12]. This includes a line-by-line review and killing programs that have outlived their usefulness [13]. There are suggesting that budget cuts will include entitlement programs [14].

1. Long, Colleen, AP, *Wal-Mart worker dies after shoppers knock him down*, November 28, 2008.
2. Aversa, Jeannine, AP, *Sources: Government working on Citigroup rescue*, November 23, 2008.
3. Reinhardt, Uwe E., The New York Times, The *New Bernanke-Bair-Paulson Insurance Company*, November 28, 2008.
4. Dash, Eric, The new York Times, *Citigroup to Halt Dividend and Curb Pay*, November 23, 2008.
5. Goldman, David, CNN Money, *Problem banks rise to 13-year high*, November 25, 2008.
6. Reuters, *U.S. problem banks rise to 171 at end of third quarter: FDIC*, November 25, 2008.
7. Keehner, Jonathan, Bloomberg, FDIC Lets Firms Without Charters Bid for Bank Assets, November 26, 2008.
8. Van Duyan, Aline, and Mackenzie, Michael, Financial Times, *Yield on 10-year Treasury debt below 3%*, November 26, 2008.
9. Coppola, Gabrielle, and Salas, Caroline, Bloomberg, *Junk Bond Yields Reach Record 20% as Economy Declines*, November 19, 2008.
10. Gray, Steven, Time, *The Ripple Effect of a Potential GM Bankruptcy*, November 28, 2008.
11. Lochhead, Carolyn. San Francisco Chronicle, *Obama says he'll rein in spending, lift economy*, November 26, 2008.
12. Zelney, Jeff, The New York Times, *Obama Vows to Look for Budget Savings to Help Finance Recovery Plan*, November 25, 2008.
13. The Wall street Journal, *Obama's Rich Revelation*, November 26, 2008.
14. Nicholas, Peter, Los Angeles Times, *Obama promises to weed out wasteful spending*, November 26, 2008.

After SP 800-116

We are reminded why physical security is so important by the events in India. Last Wednesday (November 26), terrorist attacked in the city of Mumbai, India [1]. Targets where foreigners were likely to be, such as Luxury hotels and a Jewish center, were attacked by terrorists [2]. The focus of this article is to discuss what's next following the recent National Institute of standards and Technology (NIST) SP-800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*.

The document (SP 800-116) recommends a risk based approach when implementing PIV/PACS solutions. One lesson from Mumbai is that Terrorists want to inflict as much damage as possible. If the number of people trying to get through a security checkpoint backs up, then this becomes a target for terrorist. For example, in 1993, a terrorist gunman killed two and injured three people stopped at a turn light leading into CIA Headquarters [3]. The terrorist did not know the victims, only where they were heading and that fact they were stopped. A slow authentication process could present terrorists with a number of idle people waiting to gain entry into a Federal facility. This vulnerability will tilt many risk assessments to focus on contactless authentication approaches, due to their speed.



One problem with contactless only approaches is that without checking the Public Key Infrastructure (PKI) digital certificates, how do you determine if the card has been lost or stolen? Years ago, our suggestion was to have the card holder digitally sign the CHUID. In this manner, the signature on the CHUID could be checked to see if it was revoked or not. Unfortunately, it was decided that a system signer would instead be used. The signer certificate cannot be revoked as this would invalidate the signature one every CHUID signed.

In the case of PKI path validation approaches, it is important to consider other ongoing Government activities. Case in point, the OMB is trying to reduce the number of Internet interfaces to around 50 [4]. Network architectures should be designed with this in mind going forward. Moreover, PACS vendors will need connectivity to the PKI paths and will be exposured to the network risks typical of IT applications.

Another OMB effort is migrating to IPv6 [5]. The PACS system design using digital certificate path validate should address IPv6. One glaring problem with the current approach is that the FASC-N currently is limited to Government. In contrast, the IPv6 (in the GUID) could be used by anyone. Since the CHUID cannot be verified using the current approach digital certificate path validation, we believe using IPv6 could be addressed using Internet verification approaches. Like an unused address, the IPv6 address could be listed as unused, effectively revoking the CHUID.

For this reason, we believe that the FASC-N must be replaced by an IPv6 address as soon as practicable. This would allow non-Government cards greater interoperability. More importantly, having an IPv6 address in the PIV would facilitate remote VPN access again consistent with the OBM direction [5].

At the September 24 Interagency Advisory Board meeting, Bill Burr and others pointed out the need to include cryptographic controls for strong authentication using contactless. We believe that in the future, when PIV cards have a bit more capability, contactless VPNs between the reader and PIV card will be feasible without significant delay. However, IPv6 migration does not require semiconductor technology advancements.

1. Bradsher, Keith, and Sengupta, Somini, The New York Times, *Mumbai Fighting Narrows to One Hotel*, November 28, 2008.
2. BBC, *Troops battle to end Mumbai siege*, November 28, 2008.
3. CNN, *CIA shooting suspect held without bond*, June 18, 1997.
4. OMB, M-08-05, *Implementation of Trusted Internet Connections (TIC)*, November 20, 2007.
5. OMB, M-05-22, *Transition Planning for Internet Protocol Version 5 (IPv6)*, August 2, 2005.

History never looks like history when you are living through it–John W. Gardner

Asia

The softening economy is starting to impact China. The World Bank cut China's 2008 growth estimate to 9.4% [1]. What other country would love to boast such a growth rate? In an effort to improve their economy, the People's Bank of China cut interest rates by more than a percent [2]. Additionally, there are signs of labor unrest emerging. For example, after 500 people lost their jobs at a toy factory, Windows were broken, computers smashed, and 5 police vehicles damaged [3]. China has started providing small subsidies to its domestic airlines [4]. This comes as China told airlines to delay purchases on new aircraft [5]. China's infrastructure stimulus package is expected to increase the Gross Domestic Product by 1 percent [6].

As the rest of the world decides how best to deal with fraudsters, China has its own solution. A man convicted of bilking thousands of investors out of $416 million for an ant breeding scheme, was sentenced to death and was executed [7]. Recognizing the severity of Chinese justice, efforts were made to save a man sentenced to death in a closed Chinese trial for allegedly selling missile drawings to Taiwan [8]. However, outside governments were unsuccessful and China executed the man [9]. This illustrates a real risk in human intelligence over cyber penetrating approaches where conviction is unlikely.

In Japan, signs of a deepening recessions where companies are planning the sharpest production cuts in 35 years [10].

1. Poon, Terence, The Wall street Journal, *World Bank Cuts China's 2008 Growth Outlook to 9.4%*, November 25, 2008.
2. Moore, Malcom, The Telegraph (UK), *China slashes interest rates as panic spreads*, November 26, 2008.
3. Bradsher, Keith, The New York Times, *China's Central Bank Cuts Interest Rates*, November 26, 2008.
4. Ho, Patricia Jiayi, The Wall Street Journal, *China Starts Airline Aid*, November 27, 2008.
5. CNN Money, *China plans fewer aircraft purchases*, November 28, 2008.
6. Wu, J.R., and Back, Aaron, The Wall street Journal, *China Offers Stimulus Plan Details*, November 27, 2008.
7. AP, *China executes man for ant-breeding scheme*, November 27, 2008.
8. Jacobs, Andrews, The New York Times, *Effort Made to Save Man China Convicted of Spying*, November 26, 2008.
9. BBC News, *'Taiwan spy' executed by Beijing*, November 28, 2008.
10. Fujioka, Toru, and Clenfield, Jason, Bloomberg, *Japan's Recession Deepens as Factory Output Slumps*, November 28, 2008.

Once harm has been done, even a fool understands it– Homer

Crime

Mortgage fraud continues to be problematic. For example, a Georgia attorney was sentenced to nearly 5 years in prison and required to pay $4 million in restitution for mortgage fraud [1]. In Florida, a man pleaded guilty in a $5 million mortgage fraud scheme [2].

As the mortgage market struggles, there are cases of identity theft where the homeowner's identity is used to obtain fraudulent home equity loans. For example, arrests and convictions continued for a global identity theft ring that tricked multiple banks and credit unions into wiring more than $2.5 million to accounts outside of the country [3].

1. FBI, *Attorney sentenced to almost five years in federal prison for role in mortgage fraud scheme*, November 25, 2008.
2. WJXT, *Man Pleads Guilty In $5M Mortgage Fraud*, November 25, 2008.
3. Krebs, Brian, The Washington Post, *Thieves Stole Identities to Tap Home Equity*, November 28, 2008.

Oklahoma Bank Robber—FBI