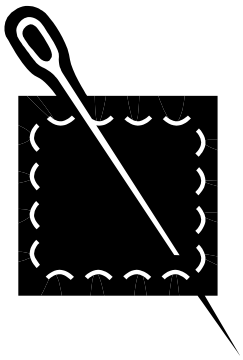
Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 21

August 17, 2008

Patch Management



When software products are introduced we often wonder how many security holes might be part of the product. As the product matures, we can learn much from the types of patches needed to fix various problems. We are seeing a number of zero-day exploits where the pressure to release patches is increasing. Moreover, configuration management and version control must keep track of the patches installed. Readers may recall the original word processor documents were flat files. They never executed and didn't allow for running under an interpreter. Thus, the old files were not suited for propagating viruses. Then came the introduction of macros. Small pieces of executable code that provided features for the users. At that point, the documents were fertile for viruses. By the time the security weaknesses were discovered, many had invested significant resources in developing powerful macros. So a logical fix of disabling macros was not an option. The rush by vendors to provide more features and consumers to purchase these products sets the stage for future exploits. A patch was once considered a temporary fix not necessarily a permanent solution. Unfortunately, vendors continue to add more exploitable functionality and many don't support older product versions. Strategically, there is a lesson learned that should be included as part of strategic risk assessments.

Case in point, last week, Microsoft released 12 patches, three of which try to keep hackers from stealing information [1]. Consider the types of attacks that the Microsoft security patches fix. One patch fixes a vulnerability that allows an attacker to remotely execute arbitrary code on a system if a user visits a specially crafted web page [2]. So if a web server you frequent gets compromised, this could have a serious impact on your machine. There were six critical patches fixing 26 problems. The six critical updates address code injection risks involving Access, Excel, Microsoft Office and Internet Explorer [3]. Two of the vulnerabilities are actively being used by hackers [4].

What this one example illustrates is that patch management is lagging the onslaught of active exploits. Years ago, when the Chaos Computer Club (CCC) took over the NASA Headquarters VAX Cluster, they made sure they could get back in by installing additional back doors corrected with the next operating system upgrade. So once your machine is compromised, short of a

(Continued on page 2)

Congress Eyes Privacy

The value of information that could aid marketers in selective advertisement is increasing. For this reason, congress is gathering information for possible new legislation to address personal information gathering [1].

A question here is will new laws protect privacy, especially regarding hacker attacks? Consider the example where an MIT student received a court order not to discuss vulnerabilities with the Massachusetts Bay Transit Authority's (MBTA) Boston fare cards [2]. On the surface, it would appear that current laws were applied thereby preventing unnecessary exploits. However, the bulk of vulnerability information was posted to the Web [3].

As technology advances, new privacy issues will continue to emerge. For example, much research has been done in the

(Continued on page 2)

Inside this issue:

Special points of interest:

- Russia Cyber-Attacks Georgia
- FDIC Many Need Cash

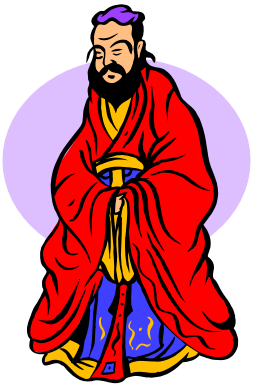
Patch Management

(Continued from page 1)

known clean install, there is a chance it may never be fully safe again. For security controls to be effective, privileged programs should start from a known good state. For example, once the files were downloaded in the background, the latest Microsoft patch required a reboot to complete installation. This necessitated a two minute delay in computer availability as the patch installation completed.

1. Barney, Doug, Redmond Report, *Patch Times 12*, August 11, 2008.
2. Espiner, Tom, ZDNet, *Microsoft Patch Tuesday brings six critical updates*, August 13, 2008.
3. Leyden, John, The Register (UK), *Bumper Patch Tuesday plugs multiple Office flaws*, August 13, 2008.
4. Clayburn, Thomas, Information Week, *Microsoft Stages 'Mammoth Patch Tuesday'*, August 12, 2008.

Success depends upon previous preparation, and without such preparation there is sure to be failure.– Confucius



China

With the Olympics fresh on everyone's mind, it is worth looking at the new economic powerhouse. It is estimated that China will surpass the U.S. as the largest manufacturer in the world, four years sooner than expected [1].

As China moves into a dominant position in the world theater; there are signs of internal challenges. During the first 2 days of the Beijing Olympics there were bombings in the Xinjiang region of far western China [2]. This is a part of China new we seldom learn of.

China is working to make the Olympics a showcase example of their emergence as a world power. One of the approaches they are using to reduce bank card fraud is the central bank is blacklisting foreign bankcards found involved in fraud cases [3].

1. Marsh, Peter, Financial Times, *China to overtake US as largest manufacturer*, August 10, 2008.
2. Cody, Edward, Washington Post, *Early in the Games, Glimpses Of China's Security Struggles*, August 10, 2008.
3. China View, *China central bank to blacklist foreign bankcards involved in fraud*, August 13, 2008.

Congress Eyes Privacy

(Continued from page 1)

area of genetics. People were concerned that based on their genetic markers, insurance companies or employers would use this information. A new law, the Genetic Information Nondiscrimination Act (GINA), took 13 years and went through several iteration before becoming law on May 21, 2008 [4].

At some point, the Congress will likely look at many of the emerging regulatory enforcement approaches in place. For example, if you forget, lose, or have you ID stolen and discover it missing while passing through TSA security, your name will be included in the TSA database for 15 years [5]. The TSA news comes at a time when reports indicate the Government Accountability Office (GAO) found that TSA follow-up of their screening practices lacking [6].

1. Clifford, Stephen, The New York Times, *Web Privacy on the Radar in Congress*, August 11, 2008.
2. Calburn, Thomas, Information Week, *MIT Students Ordered To Withhold Boston's MTA Hack Details*, August 11, 2008.
3. Raphael, JR, PC World, *Silenced Subway Hackers, Silenced No More*, August 11, 2008.
4. Platt, John R., *U.S. Law Bans Genetic Discrimination*, August 8, 2008.
5. Frank, Thomas, USA Today, *Lack of ID put fliers on TSA List*, August 13, 2008.
6. Frank, Thomas, USA Today, *Oversight of airport screening 'a waste'*, August 14, 2008.

Mortgage News

Fannie Mae and Freddie Mac were originally Government creations (1938 and 1968 respectively). Both were converted to publicly traded corporations. With the current mortgage crisis, they both reported large losses for the second quarter. So far, the Treasury Secretary, Henry Paulson, has no stated plans to infuse cash into these lending giants [1]. However, Treasury capital may be required to shore up foreign demand for Freddie Mac and Fannie Mae issued debt [2]. Indeed, economists are betting on U.S. Government money to prop up the two mortgage lenders [3]. There are commentaries suggesting mortgage giants are in serious trouble and therefore should be nationalized [4]. Former Fed Chairman Alan Greenspan suggested they be nationalized and then broken up into small companies [5].

The mortgage industry has been under the microscope since losses started to grow into a serious crisis. Continuous reports of fraud are highlighting a systemic problems now being investigated. Not unlike many of the phishing attacks promising great returns on wealth; mortgages were sold with the argument that property prices only go up. However, now one third of new home mortgages are for more than the house is worth [6]. In perhaps the most extreme example yet, a foreclosed house in Detroit took 19 days to find a buyer and sold for one dollar [7]. Most likely, the financial institution wanted to cut additional losses from property taxes.

1. Brinsley, John, Bloomberg, *Paulson Says He Doesn't Plan to Add Cash to Fannie, Freddie*, August 11, 2008.
2. Adler, Lynn, Reuters, *Fannie, Freddie debt faces confidence crisis overseas*, August 15, 2008.
3. Izzo, Phil, The Wall Street Journal, *Economists Bet in U.S. Aid for Fannie and Freddie*, August 15, 2008.
4. Newmark, Evan, The Wall street Journal, *Mean Street: Fannie and Freddie– They Shoot Horses Don't They?*, August 15, 2008.
5. Matthews, Steve, Bloomberg, *Greenspan Tells WSJ Fannie, Freddie Deserved Breakup*, August 13, 2008.
6. Ivry. Bob, Bloomberg, *One Third of New Owners Owe More Than House Is Worth*, August 12, 2008.
7. French, Ron, The Detroit News, *Foreclosure fallout: Houses go for a $1*, August 13, 2008.

The four most dangerous words in investing are 'This time it's different'– Sir John Templeton

Bank Insurance to Increase

The stress of bank failures, especially IndyMac, is putting a strain on the FDIC fund and will likely require rate increases charged to banks [1]. The problem is likely to get worse as the top 100 banks subprime loss approaches $ 510 billion [2]. Some are suggesting that globally, the loss may reach $1 trillion [3]. Some are critical of the regulator's delay in closing hundreds of troubled banks suggesting additional losses will result [4]. If true, this will certainly add additional stress to the insurance fund.

The biggest unknown leading to bank failures is the run on a bank. This is controlled by depositors and ensuring confidence in the bank is critical. To this end, confidence in the U.S. Banks has fallen 9 percent to 32 % [5]. Perhaps this is why the FDIC also revised the estimate of uninsured deposits at IndyMac downward from $1 billion to $600 million [6].

1. Vekshin, Alison, Bloomberg, *FDIC Fund Strained by Bank Failures May Lift Premiums*, August 11, 2008.
2. Onaran, Yalman, Bloomberg, *Banks' Subprime Losses Top $500 Billion on Writedowns*, August 12, 2008.
3. Bruno, Jow, AP, *Breaking up big banks questioned as losses mount*, August 16, 2008.
4. Appelbaum, Binyamin, The Washington Post, *Bank Failures Rise but Critics Say Not Fast Enough*, August 13, 2008.
5. Niemela, Jennifer, Minneapolis / St. Paul Business Journal, *Banks work to calm depositors*, August 15, 2008.
6. Reckard, E. Scott, Los Angeles Times, *FDIC slashes estimate of IndyMac's uninsured deposits*, August 12, 2008.

Georgia Cyber-war

The Russian military has been fighting their neighbor, Georgia [1]. For years, many worried that a shooting war would be accompanied with a cyber-attack. Indications are that such a scenario is currently playing out. Case in point, Georgia experienced a denial of service attack from sources within Russia [2]. The attacks centered on Georgia Government, media, communications and transportation companies [3].

Even after the shooting cease fire, Russian hackers were continuing to attack Georgian web sites, including at least one hosted in the U.S. [4]. Georgia was subjected to distributed denial of service (DDOS) attacks starting on July 20 [5]. Recall the news broadcasts during the start of Desert Storm, when all communications were jammed by coalition forces. Perhaps the Russian military is showing us what to expect in future conflicts. Especially since so many countries depend on the Internet for communication. What we are seeing is confirmation that cyber-warfare is integrated into a military strike [6]. Cyber-warfare is no longer a hypothetical scenario. Georgia relocated some of their servers in other countries that were less immune to the cyber-attacks [7]. However, in a larger unrestricted conflict, this would not be a likely option. The Russian-Georgia conflict was completely one sided. The Russians appear to have achieved their objectives of reclaiming two semi-independent regions and showing the West is powerless to stop them [8]. In an interesting development, the Pentagon has decided to put a hold on the Air Force Cyber effort [9].

1. Baer, Robert, Time, *The Russian Empire Strikes Back*, August 12, 2008.
2. Shachtman, Noah, Wired Blog, *Georgia Under Online Assault*, August 10, 2008.
3. Markoff, John, The New York Times, *Cyberspace Barrage Preceded Russian Invasion of Georgia*, August 12, 2008.
4. Stevenson, Peter, AP, *Russian hackers continue attacks on Georgian sites*, August 12, 2008.
5. Markoff, John, The New York Times, *Before the Gunfire, Cyberattacks*, August 12, 2008.
6. Gorman, Siobhan, The Wall Street Journal, *Georgia States Computers Hit By Cyberattack*, August 12, 2008.
7. Hart, Kim, The Washington Post, *Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar*, August 14, 2008.
8. Jackson, David, USA Today, *Russian actions send message to region, West*, August 13, 2008.
9. Hess, Pamela, *AP, Pentagon puts hold on USAF cyber effort*, August 13, 2008.

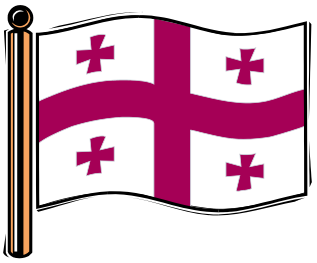
History never looks like history when you are living through it–John W. Gardner

Financials

Investment banks have been trying to cut their losses and avoid any negative publicity from the mortgage crisis. For example, Morgan Stanley, the third largest auction-rate municipal bond underwriter is being pressured by the New York Attorney General (AG) and is offering to buy back $4.5 billion in auction-rate securities. The New York AG is expanding the auctions-rate securities probe to include JPMorgan Chase & Co., Morgan Stanley and Wachovia Corp [2]. This at a time when JPMorgan reported a quarterly loss of $ 1.5 billion in its mortgage-backed securities [3]. What is interesting is this is the loss since July of this third quarter [4].

The large banks are continuing to cut back. Case in point, Wachovia is cutting thousands of jobs and just increased the number by an additional 600 [54].

1. Giannone, Joseph A., Reuters, *Morgan Stanley eyes deal, N.Y. widens auction-rate probe*, August 11, 2008.



2. Bernard, Steven, AP, *NY AG expands auction-rate securities probe*, August 11, 2008.
3. Lepro, Sara, AP, *JPMorgan shares tumble on widening 3Q losses*, August 12, 2008.
4. Reuters, *JPMorgan has $1.5 bln in Q3 mortgage asset losses*, august 12, 2008.
5. AP, *Wachovia to cut 600 more jobs than earlier planned*, August 11, 2008.