Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 20

August 10, 2008

Hacker Conventions

The cost of cyber crime is high and by one estimate up to $100 billion per year [1]. So hacker conferences draw large crowds. Consider that a black hat is considered a bad guy and today refers to hackers. Last week, a large hacker conference took up most of the third and fourth floors of the Las Vegas convention hall at Caesars Palace [2]. It is estimated that 5,000—7,000 people attend the conference [3]. At the conference, security researcher Dan Kaminsky detailed the recent Domain Name System (DNS) vulnerability and how it could be used to bypass firewall and SSL security [4]. During his presentation, Dan detailed 15 other ways the vulnerability could be exploited [5]. Separately, one Russian physicist demonstrated that a DNS emergency fix was exploitable [6].

Additionally at the Black Hat conference, there are a number of Government participants. For example, the newly created National Cyber Security Center chief suggested we must determine how much our networks are worth and how must to spend protecting them [7]. Not surprisingly, French reporters were caught hacking other reporters accounts and were booted from the conference [8].

With the move toward wider adoption of Web 2.0 technology, it was no surprise that this would be a topic of discussion. For example, while discussing Google Gadget, Web-based applets that could steal data were demonstrated [9]. It would appear that hackers are targeting feature rich social networking sites such as Facebook, MySpace and LinkedIn [10]. Hackers at the DefCon conference discussed an exploit where a hacked iPhone could be shipped to a non-existing employee and hope it sits in the mail room scanning for wireless networks [12]. The rush to market will continue to push products that have not been fully security vetted. This year also features free legal consultation for speakers from the Electronic Frontier Foundation (EFF) [11].

1. Acohido, Byron, USA Today, *Meet A-Z: The computer hacker behind a cybercrime wave*, August 5, 2008.
2. Vamosi, Robert, cnet news, *Black Hat 2008 promises to be big*, August 4, 2008.
3. Bosak, Steve, Newsfactor, *Security Geeks, Hackers Convene in Vegas*, August 6, 2008.
4. Los Angeles Times, *Internet security flaw described as worst in 10 years*, August 6, 2008.
5. Shiels, Maggie, BBC News, *Net address bug worse than fear*, august 7, 2008.
6. Markoff, John, The New York Times, *Patch for Web Security Hole*

(Continued on page 2)

Identity Theft

We recognize the risk of using credit cards could result in someone capturing our card information. To this end, eleven people have been charged with hacking into nine retailers, stealing, and selling 41 million credit and debit card numbers [1]. The hardest hit, T.J. Maxx and Marshalls discount clothing chains, took $197 million in charges to cover losses from this security breach [2]. Apparently, the hackers installed sniffer software to capture card numbers and passwords [3]. The U.S. alleges that the group decrypted PIN numbers, made new cards, and got cash from ATMs [4]. What's more, there are suggestions the vulnerabilities exposed are far from being fixed [5]. The question here is how many other organizations are vulnerable to the same exploits?

(Continued on page 2)

Inside this issue:

Special points of interest:

- Black Hat Hacker Conference
- 11 Hacker Charged in Theft of 41 Million Credit and Debit Cards

Hacker Conventions

(Continued from page 1)

Has Leaks of Its Own, August 8, 2008.

7. Robertson, Jordan, AP, *New US cyber defense coordinator hints at plans*, August 7, 2008.
8. Robertson, Jordan. AP, *Reporters booted from Black Hat conference for hacking*, August 8, 2008.
9. Brandt, Andrew, InfoWorld, *Web 2.0, DNS flaws revealed at Black Hat*, August 7, 2008.
10. Krebs, Brian, Washington Post, *Hackers' Latest Target: Social Networking Sites*, August 9, 2008.
11. Robertson, Jordan, AP, *Hackers mull physical attacks on a networked world*, August 8, 2008
12. McMillian, Robert, IDG News Service, *Now at Black Hat: a Lawyer to Vet Your Hacking*, August 7, 2008.

New Technology

A new fingerprint device not only checks for past history but also looks for traces of other substances including explosive and drug residue [1]. This is another example of technology that on the surface helps law enforcement.

With the new tests available, we should refine our definition of what is a false positive.

One report suggests that most of the $20 bills in circulation, except brand new currency, have traces of cocaine residue [2]. It has been suggested that U.S. currency contains the highest trace amounts of cocaine and drug users often roll the paper currency to sniff the drug [3]. So in all likelihood, if a person is handling paper money, they will be in contact with drug residue. So how will the new technology be used such that honest citizens will not be subjected to false positives? One constant challenge with new technology is an appreciation of the consequences.

1. Chang, Kenneth, International Herald Tribune, *Fingerprint test tells much more than identity*, August 7, 2008.
2. Skelton, Chad, Vancouver Sun, *There's cocaine in your wallet, probably*, June 10, 2005
3. Totten, Sanden, Minnesota Public Radio, *Our currency may be sinking, but it's "higher" than any other money in the world*, August 5, 2008.

You cannot escape the responsibility of tomorrow by evading it today—

Abraham Lincoln

Identity Theft

(Continued from page 1)

Department stores are not the only place hackers have struck. Rogues have installed hard to detect credit card skimmers at gas stations where every gas pump is equivalent to a checkout counter [6].

To provide more protection for consumers, laws continue to evolve. For example, the Senate unanimously approved a bill that allows identity theft victims to seek restitution in federal court for time and money lost restoring credit [7].

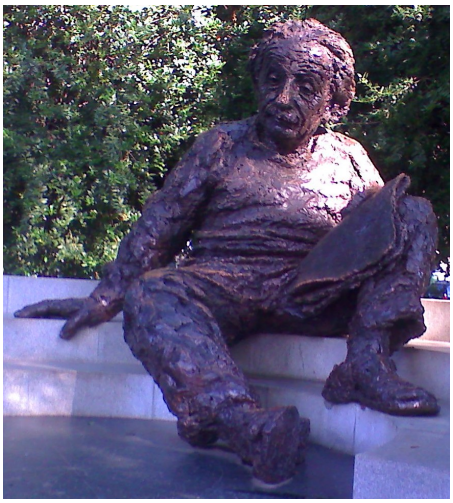
1. Ngowi, Rodrique, and D'Innocenzio,Anne, AP, *11 charged in connection with credit card fraud*, August 6, 2008.
2. Robertson, Jordan, AP, *Data-breach indictment unlikely to dent identity theft underworld, security researchers say*, august 6, 2008.
3. Harris, Andrew, and Burke, Heather, Bloomberg, *U.S. Indicts 11 in Largest U.S. Identity Theft Case*, August 6, 2008.
4. Thibodeau, Patrick, Network World, *DOJ: Credit card thefts helped by 'well designed' software*, August 7, 2008.
5. Raphael, JR, PC world Blog, *Massive Identity Theft Exposes Troubling Trend*, august 6, 2008.
6. Lackey, Katharine, USA Today, *Thieves skim credit card data at fuel pumps*, August 6, 2008.
7. Mark, Roy, eWeek, *Bill Would Allow ID Theft Victims to Sue in Federal Court*, August 5, 2008.

Mortgage News

The manager of the world's largest bond fund, Bill Gross, is estimating the U.S. Treasury will purchase up to $30 billion in Fannie Mae and Freddie Mac preferred shares to shore up capital [1]. This occurs at a time when Freddie Mac reported a loss of $821 million, three times larger than expected [2]. Fannie Mae reported a loss of $2.3 billion for the quarter [3]. This is the fourth consecutive quarterly loss for Fannie Mae and was worse than expected [4]. Given the potential U.S. Treasury support, some in Washington are questioning the wisdom in allowing Freddie and Fannie to lobby lawmakers [5]. In a sign that mortgage losses continue, the insurance company AIG suffered a $5.36 billion 2nd quarter loss primarily due to the mortgage market investments [6]. One of the consequences of the mortgage crisis is that rates are starting to rise [7].

On the positive side, Fannie Mae indicated they may have opportunistic modest mortgage portfolio growth [8]. Perhaps more importantly, the price of oil fell $5 a barrel to $115.20 last Friday [9]. Given almost all industry relies on energy a drop in oil process should improve profit.

1. Hays, Kathleen, and Harrington, Shannon D., Bloomberg, *Pimco's Gross Says U.S. Will Rescue Fannie, Freddie*, August 6, 2008.
2. Elphinstone, J.W., AP, *Freddie Mac swings to 2Q loss*, August 6, 2008.
3. Zibel, Alan, AP, *Fannie Mae loses $2.3B in quarter as defaults rise*, August 8, 2008.
4. Desmond, Maurna, Forbes, *Up To Its Fannie In Trouble*, August 8, 2008.
5. Holzer, Jessica, The Wall Street Journal, *Fannie, Freddie's Right To Lobby Lawmakers Is Questioned*, August 7, 2008.
6. Read, Madlen, AP, *AIG's huge 2Q loss shows credit market woes linger*, august 7, 2008.
7. Bernard, Tara Siegel, The New York Times, *Mortgage Rates, Down for So Long, Are Creeping Back Up and Crimping Affordability*, August 8, 2008.
8. Reuters, Fannie Mae says modest mortgage portfolio growth possible, August 8, 2008.
9. Orlando Sentinel, *Finally, A Little Good News*, August 9, 2008.



It has become appallingly obvious that our technology has exceeded our humanity–Albert Einstein

Bank News

Big banks are puzzling regulators by suggesting that the purchasers of complex financial products be limited to the all but the wealthiest retail investors [1]. Moreover, during the second quarter, mortgage bankers spent $1.2 million lobbying [2].

In other news, Morgan Stanly informed thousands of clients whose properties have lost values, that they will not be allowed to withdraw money on their home-equity credit lines [3].

Elsewhere, reports continue to highlight exploits to bank security. For example, one researcher argues that stolen bank account information placing accounts at risk were discovered on a hacker database [4]. Finally, now that Bank of America owns Countrywide, the SEC has launched a formal investigation [5].

1. van Duyn, Aline, Financial Times, *Big banks seek to limit their own risks*, august 6, 2008.
2. AP/Boston Globe, *Mortgage bankers group spent $1.2M lobbying in 2Q*, August 7, 2008.
3. Harper, Christine, Bloomberg, *Morgan Stanley Said to Freeze Home-Equity Credit Withdrawals*, August 6, 2008.
4. Keizer, Gregg, Network World, *Russian hacker gangs steals with impunity, researcher*, August 9, 2008.
5. AP, SEC now conducting formal probe into Countrywide, August 8, 2008.

Fraud

As there is more financial stress, we are learning of more instances of fraud. For example, in Los Angeles, a hospital CEO was arrested in a scheme where homeless people were recruited to bill the government for $ millions in unnecessary services [1].

In banking, to settle state and federal claims that it fraudulently sold auction-rate securities, UBS the largest Swiss Bank, may pay more than Citigroup Inc. or Merrill Lynch & Company [2]. Additionally, UBS has agreed to pay $150 million in fines [3]. Meanwhile, the French chip maker STMicroelectronics sued the second largest Swiss bank, Credit Suisse, for investing $450 million in auction-rate securities without permission [4].

Citigroup agreed to pay a $100 million fine to settle charges it fraudulently misled investors [5]. Together, Merrill and Citigroup have agreed to buy back $17 billion in questionable fixed-income investments [6]. Moreover, another large bank, the Bank of America, received subpoenas from federal and state regulators related to sales of auction-rate securities [7]. One of the objectives for the bond buy-back is to try to get past the auction -rate trouble and restore the bank's image [8].

In Connecticut, a man pleaded guilty to defrauded banks and his clients of more than $8 million [9].

1. Mohajer, Shaya Tayefe, AP, *FBI: Hospital CEO arrested in health care scheme*, August 6, 2008.
2. McDonald, Michael, and Freifeld, Karen, Bloomberg, *UBS Costs in Auction-Rate Accord May Top Citigroup's*, August 8, 200.
3. McDonald, Michael, and Freifeld, Karen, Bloomberg, *UBS Fined $150 Million, Agrees to Buy Auction Debt*, August 8, 2008.
4. Ram, Vidya, Forbes, *UBS: The ARS Are Ours*, August 8, 2008.
5. McCool, Grant, and Stempel, Reuters, Jonathan, *Citigroup and Merrill to buy back auction-rate debt*, August 8, 2008.
6. Hamilton, Walter, Los Angeles Times, *Citigroup, Merrill to buy back $17 billion in auction-rate securities*, August 8, 2008.
7. Dash, Eric, The New York Times, *2 Banks Will Buy Back $17 Billion in Securities*, August 6, 2008.
8. Farell, Greg, USA Today, *Citigroup, Merrill to buy $20B in bonds*, August 8, 2008.
9. FBI, *Wilton Man Admits Mortgage Fraud Scheme*, August 5, 2008.

There is more real pleasure to be gotten out of a malicious act, where your heart is in it, than out of thirty acts of a nobler sort—

Mark Twain

Security Incidents

In one survey indicated that 89% security incidents go unreported [1]. From this we can infer that the actual loss due to computer crime is most likely much higher than reported.

At Black Hat, one instance of an Estonian financial firm was described where they executed an exploit and thereby received advanced information and profited $8 million before the SEC discovered and halted the activity [2]. Pointing out the obvious ethical issue, IBM criticized researchers and indicated that 16 percent of the vulnerabilities disclose were zero-day exploits [3]. During this window of vulnerability, significant loss can result with few options available for the victims. More exploits are becoming available within 24 hours of announcing the vulnerability [4]. Consider the DNS flaw was described in the detail necessary for exploiting the vulnerability while fixes are still being applied [5]. Cybercriminals are using automation techniques to enable them to rapidly exploit announced vulnerabilities [6]. So why does a security researcher find it necessary to provide a detailed how-to exploit a vulnerability before fixes have been applied? Who wins and who loses?

1. Claburn, Thomas, Information Week, *Most Security Breaches Go Unreported*, August 1, 2008.
2. Greene, Tim, *Network World, Business hacks reap money from e-commerce sites*, August 8, 2008.
3. Tung, Liam, ZDNet, *IBM chides security researchers*, July 30, 2008.
4. Robertson, Jordan, AP, *Online threats materializing faster, study shows*, July 28, 2008.
5. Menn, Joseph, Los Angeles Times, *A flaw in the domain name system allows hackers to steer traffic and steal information*, August 7, 2008
6. Poremba, Marquette, SC Magazine, *X-Force at mid-year: Cybercriminals get faster*, July 30, 2008.