Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 32

November 2, 2008

Technology

There is a lot of reliance placed on the outcome of a polygraph; but can the polygraph be trusted? Three ATF agents trained to defeat a polygraph test successfully hid their identities when the Mongols motorcycle club administered a polygraph test [1]. Having bad actors pass the polygraph is not new. Consider the Aldrich Ames, employed by the CIA was spying for the KGB [2]. The FBI had their day in the news with Robert P. Hanssen who provided the Russians classified information for over 15 years [3]. As with biometrics in general, the polygraph has false positive and false negative results.

Polygraphs are not the only technology that is error prone. Last spring, in an unmanned underground nuclear launch site, an undetected (for five days) fire broke out causing $1 million in damage [4]. There was no radiation leak, no chance of accidental launch, and the fire burnt itself out after a few hours [5]. The fire started at the nuclear ICBM located at F.E. Warren Air Force Base in Wyoming following a thunderstorm that temporarily knocked out power [6]. The incident took place on May 23 and there was no mention of the incident prior to the accident investigation report at Peterson Air Force Base [7].

Today, when we hear pirates, we think of someone making illegal copies of copyright material, a football team, or perhaps a Disney movie. However, there are still sea faring pirates that are seizing ships today. Readers may recall back in 1975 when the US flag ship, the Mayaguez, was seized by pirates and later freed by us forces [8]. Somali pirates recently seized a Turkish freighter on Africa's east coast between Somalia and Yemen [9]. The Turkish ship, the Neslihan, sent out distress signals but was still boarded by pirates [10]. The pirates use fast moving skiffs, pull alongside the ship, and hold the crew at gunpoint [11]. So in a world with radios and other forms of communication, how is it that pirates can still operate in the open?

At the University of California at San Diego, computer scientists demonstrated the capability to generate a physical lock key from a photograph [12]. So it is possible that we may see exploits where bad actors can recreate door keys from a telephotograph.

(Continued on page 2)

Security News

Following last week's out of sequence emergency security patch, Microsoft has release another [1]. The latest emergency patch does not appear to have a active exploit just a vulnerability [2]. Microsoft was not alone; Google started distributing a security patch to its Android mobile phone operating system [3].

In other news, the *Sinowal* Trojan is reported to have stolen 300,000 bank logins [4]. Apparently, researchers from RSA uncovered a site with compromised stolen bank account information going back to 2006 [5]. The Trojan infects the master boot record and triggers when users enter one of 2,700 specific Web addresses [6]. The data retrieved indicates the Trojan has been collecting bank accounts since February, 2006, or over 2 1/2 years [7]. Researchers suspect the source of the Trojan may have a Russian origin because none of the 2,700 banks the Trojan looks for are located in Russia [8].

(Continued on page 2)

Inside this issue:

Special points of interest:

- Three ATF agents trained to lie passed polygraph test
- A $1 million fire at ICBM silo that burnt itself out went undetected for five days
- The Sinowal Stealth Trojan stole 300,000 bank logins
- Freedom Bank becomes 17th bank failure

Technology

(Continued from page 1)

Technology can sometime be crucial in solving a crime. Case in point, in 2006, due to an embedded GPS device, 4,500 stolen phones in a cargo trailer were tracked to their final destination leading to a Maryland man pleading guilty to receiving stolen cell phones [13]. In this case, the GPS device was placed in the trailer following the theft of other cell phone shipments.

1. Watkins, Thomas, AP, *Polygraphs tested mettle of agents in biker case*, October 27, 2008.
2. Johnston, David, The New York Times, *How the F.B.I. Finally Caught Aldrich Ames*, January 27, 1995.
3. Risen, James, The New York Times, *Ex-F.B.I. Man Said to Accept Spy Case Deal*, July 4, 2001.
4. Elliott, Dan, AP, *Air Force: Nuke missile silo fire went undetected*, October 30, 2008.
5. Peters, Mike, Greeley Tribune, *Air Force: Nuclear missile silo burned*, October 31, 2008.
6. Hoffman, Michael, Air Force Times, *May fire damaged cables leading to nuclear ICBM*, October 30, 2008.
7. Roeder, Tom, Colorado Springs Gazette, *Silo fire casts another cloud over U.S. nukes*, October 30, 2008.
8. Kraft, Joseph, Pittsburgh Post-Gazette, *Lessons we can learn from Mayaguez affair*, May 21, 1975.
9. Bright. Arthur, Science Christian Monitor, *Somali pirates seize Turkish ore freighter*, November 1, 2008.
10. CNN, *Turkish ship 'distressed' in pirate waters*, October 30, 2008.
11. Schneiderman, R. M., The New York Times, *Somalia's Pirate Economy*, October 31, 2008.
12. UCSD Jacobs, *Keys can be copied from afar, Jacobs School Computer Scientists show*, October 30, 2008.
13. FBI, *Annapolis man pleads guilty to receiving stolen cell phones*, October 30, 2008.

And, after all, what is a lie? 'Tis but the truth in masquerade–Lord Byron

Security News

(Continued from page 1)

The master boot record contains information located on the hard drive that is amongst the first information loaded when the computer starts up. As the infection loads before the anti-virus software, it has the opportunity to defeat protection software. This stealth technique is one reason this particular Trojan was able to operate for so long without detection. So how many other Trojans are in full operation that has yet to be detected? With the current financial crisis and growing cyber-crime, perhaps the time has come to finally tighten up Internet security. PKI enabled smart cards offer a proven technology against password grabbing Trojans.

1. O'Reilly, Dennis, Cnet News, *Check your Windows Update history*, October 28, 2008.
2. Hulme, Georgem Information Week, *Microsoft Issues Emergency Advisory*, October 27, 2008.
3. Prince, Brian, eWeek, *Stealthy Trojan Swipes Bank Log-ins, Financial Data From Thousands*, October 31, 2008.
4. Markoff, John, The New York Times, *A Huge Cache of Stolen Financial Data*, October 31, 2008.
5. Keizer, Gregg, Computer World, *'Ruthless' Trojan horse steals 500k bank, credit card log-ons*, October 31, 2008.
6. Krebs, Brian, The Washington Post, *Virtual Heist Nets 500,000+ Bank, Credit Accounts*, October 31, 2008.
7. Goodin, Dan, The Register (UK), *Undetectable data-stealing trojan nabs 500,000 virtual wallets*, October 31, 2008.
8. Shankland, Stephen, Cnet News, *Google patches Android security flaw*, November 1, 2008.

Technology Use

To better predict the future, we can look to the present and see what is popular. Entertainment has always been a big industry from football games to broadcast media (radio and television). With the advent of computers and the Internet, new forms of entertainment have emerged. Case in point, there are now over 11 million subscribers, paying $13–15 per month to subscribe to the on-line game *World of Witchcraft* [1]. There are a number of on-line games world-wide and the numbers are increasing. It has gotten to the point where two Dutch teenagers were convicted of stealing virtual (computer game) items [2].

The value of something can be determined by what someone is willing to pay for the item. Virtual reality games are providing a valuable observation into computing trends. In another trend, the Christian Science Monitor will stop printing newspapers and offer only on-line service [3]. This follows continued declines in most newspaper circulations [4]. At the same time, the newspaper web sites are experiencing growth 68.3 million visitors in the third quarter of 2008 [5]. This comes as CBS reported a $12.5 billion loss [6]. In other news, the Washington Post reported earnings 86% below the same quarter last year [7]. The paper's daily circulation fell by 2.4%; with Sunday down 3.6%; however on-line publishing increased by 13% [8]. Overall, weekday newspaper circulation has dropped 4.6% in the past year [9].

1. Snow, Blake, MacWorld, *Blizzard: World of Warcraft subscribers equal population of Ohio*, October 28, 2008.
2. Telegraph (UK), *Dutch court finds youths guilty of 'virtual theft'*, October 22, 2008.
3. Clifford, Stephanie, The New York Times, *Christian Science Paper to End Daily Print Edition*, October 28, 2008.
4. Seattle Times/AP, *Sharp circulation drops for Times, P-I, other daily newspapers*, October 28, 2008.
5. Robertson, Ken, *Tri City Herald, Newspaper website growth no myth*, October 28, 2008.
6. James, Meg, Los Angeles Times, *CBS reports $12.5-billion loss on another write-down*, October 31, 2008.
7. Plumb, Tierney, Washington Business Journal, *Washington Post earnings fall 86%*, October 31, 2008.
8. AFP, Washington Post profits plummet, October 31, 2008.
9. Rabil, Sarah, Bloomberg, Newspaper Weekday Circulation Drops 4.6%, ABC Reports, October 27, 2008.

A cunning fox cannot outsmart a skilled hunter–

Anonymous

Financials

In a troubling sign of further financial problems, dozens of hedge funds have refused to return investor's money [1]. For example, the Knight Capital Group, halted redemptions from two of their hedge funds citing the need to protect investors [2].

In Florida, the Freedom Bank became the 17th bank closed in 2008 [3]. The closing is expected to cost the FDIC's insurance fund between $80 million to $104 million. Banks continue to struggle through the financial crisis. For example, in Washington, the AmericanWest bank posted a $97 million quarterly loss [5]. Likewise, the Great Florida Bank reported a $13.9 million loss [6]. In Oregon, the Columbia Bancorp reports a quarterly loss of $14.1 million [7].

1. Herbst-Bayliss, Svea, Reuters, *Hedge funds working to limit redemptions*, October 31, 2008.
2. Reuters, *Knight Capital's Deephaven halts fund redemptions*, October 30, 2008.
3. Shwiff, Kathy, The Wall street Journal, *Fifth Third Bancorp Takes Over Assets in 17th Bank Failure*, November 1, 2008.
4. Vekshin, Alison, and Mildenberg, David, Bloomberg, *Florida's Freedom Bank Is 17th in U.S. to Be Closed This Year*, November 1, 2008.
5. Puget Sound Business Journal, *AmericanWest bank posts $97M Q3 loss; closing six branches*, October 31, 2008.
6. Bandell, Brian, South Florida Business Journal, *Great Florida posts $13.9 million loss*, October 31, 2008.
7. Manning, Jeff, The Oregonian, *Columbia Bancorp records $14 million loss*, October 31, 2008.

Global Trade

During this election year, free trade is making the news. In particular, the slumping economy, stagnating wages for many workers and unease about the rise of China as an economic powerhouse are contributing to voter angst [1].

The news from China's food quality remains bad. It seems that animals were fed melamine tainted products that have now entered the food chain [2]. Earlier in the week, melamine tainted chicken eggs from China were found [3]. Melamine is rich in nitrogen and gives low-quality food and feed artificially high protein readings thereby making more profit for bad actors [4].

If the food people eat is tainted, what assurances do we have that the electronics are not tainted? Consider, the Port of Los Angles recently awarded a contract to purchase a mobile X-ray machine to the low bidder using a device made in China [5]. The Chinese manufacturer, NUCTECH, is run by 37 year old Hu Haifeng, the son of PRC President and Communist Party General Secretary Hu Jintao [6].

1. Hitt, Greg, and Haynes, Brad, The Wall street Journal, *Mood Shift Against Free Trade Puts Republicans on Defensive*, October 31, 2008.
2. UPI, *China goes after tainted feed producers*, November 1, 2008.
3. Reuters, *China urged to halt melamine in eggs*, October 26, 2008.
4. Wong, Gillian, AP, *Melamine already in global food chain: experts*, October 31, 2008.
5. Goodwin, Jacob, GCN, *Port of L.A. buys Chinese X-ray scanning system with U.S. taxpayer money*, October 16, 2008.
6. Defense Industry Daily, *Port of LA Buys Security Scanners from Chinese Firm*, October 21, 2008.

The essence of lying is in deception, not in words– John Ruskin

Crime

Last year, the IRS alone issued over $1 billion in fraudulent checks [1].

In Missouri, 17 people were indicted in a $12.6 million mortgage fraud scheme [2]. In Texas, a man was sentenced for bilking $107 million from a taxpayer-funded bank [3]. In Connecticut, a 31-year old man pleaded guilty to a $1.8 million credit card scam at Foxwoods Resort Casino [4]. In New Orleans, an attorney pleaded guilty to stealing $30 million from his law firm and a casino operator [5]. In Oregon, twin brothers are facing counterfeiting charges for having $15,000 in bogus $100 bills [6]. A federal jury convicted Lance Poulsen, the former National Century Financial Enterprises CEO, of conspiracy, fraud and money laundering that cost investors nearly $2 billion [7]. A former product marketing manager and her husband were accused of stealing $millions from McAfee [8]. Finally, the Department of State has notified 383 people that their passport files have been illegally accessed and used to open fraudulent credit card accounts [9].

Department of State

1. Abrams, Jim, AP, *Report: IRS issued $1B in bad refunds in 2007*, October 30, 2008.
2. FBI, *Missouri real estate agent, loan officers among those indicted for $12.6 million mortgage fraud*, October 29, 2008.
3. AP, *Businessman sentenced in $107M bank fraud*, October 28, 2008.
4. AP, *Mass. man guilty in Foxwoods Casino scam*, October 29, 2008.
5. KATC, *La. lawyer pleads guilty to charges he stole $30M*, October 31, 2008.
6. AP, *Twins charged with counterfeiting*, November 1, 2008.
7. Market watch, *Former National Century Financial Enterprises CEO Convicted of Conspiracy, Fraud and Money Laundering*, October 31, 2008.
8. KPIX (CBS 5), Couple Accused Of Stealing Millions From McAfee, October 31, 2008.
9. Le, Matthew, AP, *State Department warns passport applicants of possible identity theft*, October 31, 2008.