IN THE NEWS

Critical Infrastructure

In California, a commuter train carrying 222 people had a head on collision with a freight train [1]. The death toll continues to rise and the scene is described as total destruction [2]. The suggested cause of the accident was the failure of a Metrolink engineer to stop his train at a red signal [3]. Unfortunately, the engineer in question died in the accident [4]. A retired Amtrak engineer, said the common practice for northbound passenger trains is to pull onto a side track at Chatsworth until southbound freight trains have passed [5]. It will be some time before an official cause is given and if it involves the national security of the U.S., we may not know all details until properly declassified. In the end, it may be that the engineer was neglect or suicidal however, it is still worth considering the role of software. Software that controls utilities such as oil and gas pipelines, chemical plants, transportation (read: railroads), assembly lines and power grids use the supervisory control and data acquisition (SCADA) software. Some have focused on the non-SCADA software product vulnerabilities as significant risk factors [6]. However, following a published SCADA vulnerability discovered earlier an exploit was released [7]. It was pointed out that the exploit only posed a risk to companies with Internet access that lacked adequate firewall protection [8]. So the question to ask, with all the SCADA controls used by the railroads, how is it that two trains have a head on collision while sharing the same track? Up until last Friday, only 47 people were killed in Metrolink trains accidents since 1999; however, less than an hour after the Chatsworth crash, another Metrolink train struck a vehicle and killed a female driver near the Corona station [9]. Police are quoted as saying the driver of a vehicle drove around the lower arms at a train crossing [10]. We hope the Federal investigation will verify the second accident was as reported.

We will continue to track events that could be the result of cyber attacks or illustrate potential consequences of a cyber attack. Sometimes the security of an isolated system becomes compromised when other networked applications are inadvertently added to the isolated network. That is, any device with Internet access added to an otherwise closed network may become a portal

Cyber attacks, also known as computer network attacks, against the U.S. rail industry pose a potentially critical threat, given the dependence of the rail industry on automated control networks, information systems, and telecommunications. The disruption resulting from a cyber attack on control networks, such as Supervisory Control and Data Acquisition (SCADA) systems, which are generally used to automate control processes, could lead to costly power outages, equipment damage, or interruption of safety-related equipment.—DHS, The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System May 24, 2006

Inside this issue:

Special points of interest:

- Head-on collision of Passenger and freight trains sharing the same track

- Less than an hour later, another train accident killed a motorist

- Algos drop United Airlines value by $1 billion in 15 minutes of trading based on outdated story on Google

Algos the Corporate Killers

On Monday (Sept. 8), a six-year old article on United air Lines (UAL) caused a sell-off where the stock lost $1 billion in value in a matter of minutes [1]. What is interesting about this story is the reliance on Google [2]. Moreover, Google products like other commercial products are susceptible to security exploits [3]. The Securities and Exchange Commission has opened an inquiry as to why UAL fell from $12 to $3 in fifteen minutes (before trading was halted) [4]. Before the end of the day, UAL was again trading above $10. The UAL example clearly depicts the opportunity for a rogue to make money by injecting bogus information.

Most large traders rely on computer programs designed to kick in when certain news surfaces. These programs typically run without human interven-

Critical Infrastructure

of entry. There are reports indicating terrorist interest in SCADA and distributed control systems; the simplest of which adjust pipeline valves, close circuit breakers, or throw railway switches [11]. In all likelihood, there were numerous software controlled devices that should have prevented the Metrolink accident. That the accident took place during evening rush hour when the trains were packed with passengers amplifies the damage.

If indeed it turns out that the accident was caused by one person ignoring a signal, this illustrates that a cyber attacker need only change one signal to display green while reporting back that a red signal was displayed. In the Metrolink accident, the engineer would have been exposed to the following options: didn't see the light, saw a red light and ignored it, or saw a green light.

> *Process control and Supervisory Control and Data Acquisition (SCADA) systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wreaked so much havoc on corporate information systems. New research indicates this confidence is misplaced—Turk, Robert J, Idaho National Laboratory, Cyber Incidents Involving Control Systems, October 2005.*

1. KNBC, *Death Toll Continues To Rise In Metrolink Crash*, September 12, 2008.

2. The Los Angeles Times, *'Total destruction': At least 15 die in head-on Metrolink crash*, September 13, 2008.

3. AP, *Metrolink: Engineer error likely train crash cause*, September 13, 2008.

4. Blood, Michael R., and Pritchard, Justin, AP, *Rush to judgment' in deadly LA rail crash?*, September 14, 2008.

5. Weikel, Dan, and Pool, Bob, Chicago Tribune, *Cause of L.A. rail crash remains elusive*, September 14, 2008.

6. Glickenstein, Harvey, and Teumin, David, Railway Age, *Are passenger rail control systems protected from cyberattack?*, January, 2006.

7. Kaplan, Dan, SC Magazine, *Attack code released for SCADA software vulnerability*, September 8, 2008.

8. McMillan, Robert, IDG News Service, *Computer threat for industrial systems now more serious*, September 10, 2008.

9. Weikel, Dan, and Pool, Bob, Los Angeles Times, *Investigators will examine many possible causes of crash*, September 13, 2008.

10. Bermudez, Esmeralda, Los Angeles Times, *Driver dies when Metrolink train hits car in Corona*, September 12, 2008.

11. Gellman, Barton, The Washington Post, *Cyber-Attacks by Al Qaeda Feared*, June 27, 2002.

> *In this business, by the time you realize you're in trouble, it's too late to save yourself. Unless you're running scared all the time, you're gone—Bill Gates*

Algos the Corporate Killers

tion. The programs are referred to as "algos" and accounted for 30 percent of all equity trading last year [5].

Algos use artificial intelligence approaches to quickly execute stock transactions [6]. This presents bad actors with a unique opportunity to make significant money and seriously damage the economy.

What happened to UAL illustrates there are many ways to attack our financial systems independent of actually gaining access to the executing applications. By corrupting the data going into the programs, (read: bogus news stories) chaos can result. Unfortunately, more emphasis goes into reacting to damage rather that prevention. If we fail to address these obvious exploits we may be picking up the pieces down the road.

1. Nizza, Mike, The New York Times, *A Stock-Killer Fueled by Algorithm After Algorithm*, September 10, 2008.

2. Los Angeles Times, *Tribune blames United Airlines article mixup on Google*, September 11, 2008.

3. Keizer, Gregg, Computerworld, *Google issues first patches for Chrome*, September 8, 2008.

4. Scannell, Kara, The Wall Street Journal, *SEC Opens Early Inquiry Into UAL's Stock Decline*, September 11, 2008.

5. Spicer, Jonathan, Reuters, *Automated trading bites some UAL investors*, September 10, 2008.

6. Duhigg, Charles, *The New York Times, A Smarter Computer to Pick Stocks*, November 24, 2006.

Financial Maelstrom

In a sign of continued stress in the banking industry, the Fed auctioned off another $25 billion to ease credit [1]. As we have mentioned before, many times the panic takes over the rational process. For example, Lehman Brothers stock was falling faster than other financial companies worrying shareholders they may lose everything [2]. Lehman, the nation's 4th largest investment bank fell over 40% on Tuesday [3]. As of Thursday, the stock fell another 41% closing at $4.22 per share. On Friday the stock closed at $3.59 per share. The reports on Thursday were that Lehman was in discussions with a potential buyer [4]. Moreover, The Federal Reserve Bank of New York held and Treasury Secretary Henry Paulson met on Friday to discuss Lehman Brothers [5]. Another meeting between Government, Lehman, and industry took place on Saturday [6]. There is fear that if a solution is not reached, the Fed would be powerless to avert other financial institutions from the same fate [7].

Another problem impacting companies is the government bailout of Fannie Mae and Freddie Mac is wiping out those who hold the common and preferred stock [8]. So the other companies that held stock in mortgage giants will likely be taking a charge in the next quarter. For example, Prosperity Banchares Inc. announced a write-down; their Freddie and Fannie stock a book value of $14 million [9].

Another financial stock under pressure is Washington Mutual (WaMu), down to a 17-year low [10]. In 1997, the FDIC sold 14 million shares of WaMu for $665 million [11]. On Wednesday, the stock value of WaMu (market Cap) was $ 3.9 billion.

Some are suggesting that if Washington Mutual fails, the FDIC might need help in the takeover [12]. 77% WaMu $309 billion in assets are mortgages [13]. Assets of the banks on the FDIC's latest watch list are $78 billion [14]. Consequently, WaMu cannot be on the latest list. However, a further reduction in stock price may necessitate a takeover. Additionally, WaMu entered into a memorandum of Understanding with the Office of Thrift Supervision (OTS), the Standard and Poor's Rating Services lowered their outlook to "negative" [15]. On Thursday (Sept 11), WaMU had a recovery at the close of business. However, Moodey's Investors service downgraded the WaMu's senior unsecured debt two notches to junk status [16].

1. Aversa, Jeannine, AP, *Fed auctions another $25 billion in loans to banks*, September 9, 2008.

2. Reuters, *Analysts see Bear Stearns-like fate for Lehman at worst*, September 10, 2008.

3. The Miami Herald, *Lehman Brothers shares plunge*, September 10, 2008.

4. Onaran, Yalman, Bloomberg, *Lehman Said to Be in Discussions About Potential Sale*, September 11, 2008.

5. Crutsinger, Martin, AP, *Emergency meeting held to discuss Lehman Brothers*, September 13, 2008.

6. Aversa, Jeannine, AP, *Emergency meeting on Lehman rescue resumes*, September 13, 2008.

7. Kaiser, Emily, and Somerville, Glenn, Reuters, *Fed's options limited if Lehman talks fail*, September 13, 2008.

8. Gaffen, David, The Wall Street Journal, *Four at Four: A Nation of Bailouts*, September 9, 2008.

9. Barr, Greg, Houston Business Journal, *Prosperity to take Fannie-Freddie charge*, September 10, 2008.

10. Stempel, Jonatha, and Aubin, Dena, Reuters, *Washington Mutual at 17-year low, debt risk soars*, September 10, 2008.

11. FDIC, Press Release PR-5-97, *FDIC Sells Washington Mutual Stock*, January 23, 1997.

12. Gomstyn, Alice, ABC News, *Another Day, Another Bank: Is WaMu Next?*, September 10, 2008.

13. Levy, Ari, Bloomberg, *WaMu Shares Reach Lowest Since 1990, Debt Risk Surges*, September 10, 2008.

14. Ellis, David, and Luhby, Tami, CNN Money, *Problem bank list keeps growing*, August 27, 2008.

15. Lepro, Sara, AP, *Washington Mutual shares plunge to 17-year low*, September 11, 2008.

16. Stempel, Jonathan, Reuters, *WaMu cut to "junk," sees $4.5 billion loss reserve*, September 11, 2008.

Bankruptcy stared me in the face, but one thought kept me calm; soon I'd be too poor to need an anti-theft alarm—
Gina Rothfels

The Cost of Chinese Business

In China, children in seven provinces are suffering from kidney stones and doctors fear it could be due to fake milk [1]. Following this report, 700 tons of the infant formula were recalled due to an industrial chemical, melamine, contamination [2]. The chemical is rich in nitrogen and fools product tests into reporting a high level of protein when there is none [3]. The U.S. Food and Drug administration is warning consumers that contaminated products may have reached the U.S. [4]. As the number of sick babies in China increased to 432, news reports indicate the Chinese government knew of the contamination and ordered the dairy to stop production weeks ago [5].

In July the Trade deficit with China increased to $24.9 billion compared to $24.2 billion that went to OPEC countries [6]. As the trade deficit grows, the Chinese government is still protectionist and will use a new anti-monopoly law in reviewing a bid by Coca-Cola for a popular juice company [7]. Will Chinese protectionism prevail?

1. Martin, Dan, AFP, *Health scare in China over infant milk powder*, September 11, 2008.
2. Bradsher, Keith, The New York Times, *China Recalls Infant Formula*, September 12, 2008.
3. McDonald, Joe, AP, *China vows 'serious punishment' in formula probe*, September 12, 2008.
4. Lawrence, Dune, Bloomberg, *China Says Sanlu Brand Formula Likely Contaminated by Melamine*, September 12, 2008.
5. McDonald, Joe, AP, *Chinese dairy knew milk fault weeks before recall*, September 13, 2008.
6. Palmer, Doug, Reuters, *U.S. trade gap widens to $62.2 billion in July on oil*, September 11, 2008.
7. McDonald, Joe, AP, *China promises review of Coke bid for Huiyuan*, September 11, 2008.

I was seldom able to see an opportunity until it had ceased to be one–Mark Twain

---

Hackers

Last week, the most powerful super collider conducted its first operational test [1]. In an all too familiar story, hackers have since broken into the new Hadron Collider [2].

The threat from botnets continues. According to one group monitoring some of the Internet attacks, the number of PCs infected with botnets increased from 100,000 to 400,000 machines during the past three months [3].

1. Science Daily, *MIT Awaits Data From World's Biggest Physics Experiment*, September 12, 2008.
2. AFP, *Hackers 'find black hole in atom smasher computers'*, September 13, 2008.
3. Hickey, Kathleen, GCN, *Report: Botnets quadruple*, September 8, 2008.
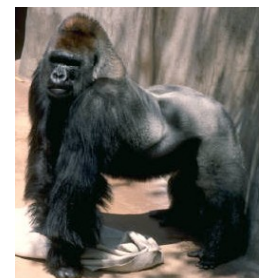
Mortgage 800 Pound Gorilla

The U.S. government seized mortgage giants Fannie Mae and Freddie Mac [1]. The government is pledging $200 billion if needed to help Fannie and Freddie [2].

It is hard to determine what the cost to other organizations will finally be. For example, The Colorado Public Employees Retirement Association held 827,300 shares of Fannie and 541,300 shares of Freddie as of June 30 [3]. One question is did large investor algos result in the collapse of Freddie and Fannie?

Meanwhile, the FHA will be allowed to insure an additional $300 billion of troubled mortgages [4].

1. Crutsinger, Martin and Zibel, Alan, AP, *US government takes on big role in mortgage market*, September 8, 2008.
2. Crutsinger, Martin, AP, *Treasury tries to answer worries about takeovers*, September 11, 2008.
3. Svaldi, Aldo, The Denver Post, *Fannie Mae investor says U.S. didn't keep its word*, September 9, 2008.
4. Der Hovanesian, Business Week, *New Rules Allow the FHA to Buy Troubled Loans*, September 11, 2008.