Femtosecond®
www.femto-second.com

# In the News

Volume 1 Issue 9

May 25, 2008

## On-line Medical Records

What if you are out of town and become ill. Having access to your medical records would help physicians prescribe proper treatment. However, this capability should be predicated on having adequate security. Advertising a service as an *on-line vault* implies a secure solution, but is it? The latest to offer such a service is Google [1]. Google Health is completely free. As noted by the Google Frequently asked Questions: *There is no cost to sign up. All you need is a username and a password. And if you already have a Google account set up then you are set* [2]. So on the surface, your medical records would be protected by a user ID and password. Do you believe this is sufficient security? Before Google, Microsoft's HealthVault and WebMD's Health Manager, both outside of HIPAA, were available on-line applications for user access to medical records [3]. One report raises two issues with HealthVault launched in October 2007, can it be trusted and is it relevant [4].

You may recall a few weeks ago, a hacker server was discovered that contained 1.4 GB of information, including Health Insurance Portability and Accountability Act (HIPAA) information [5]. Since HIPAA information is leaking to the hacker community, what are adequate security controls?

Looking at medical record security breaches provides a look at hacker interest. For example, hundreds of patent records disappeared from a Montgomery, Alabama psychiatric hospital [6]. In Monterey, California, an Identity Theft victim started receiving maternity bills originating from the person using her ID [7]. In this last case, the cause is believed to be a lost wallet. How did a HIPAA compliant system allow a woman with a fake identity to receive maternity services? This is perhaps a good reason for stronger identification and authentication, such as using smart cards. In another case, California health regulators identified 14 people at the UCLA Medical Center who were improperly viewing medical records of celebrities [8]. Further, reports indicate that 60 celebrity medical records were stolen and sold to the media [9]. A security breach at the University of California San Francisco exposed 6,000 patent's records for three months [10]. In April, a former hospital employee was arrested for and identity theft scheme involving 50,000 patent records [11]. As hospitals and medical centers continue moving away from paper, data breaches are on the rise [12]. Consistent with the problems of other industries, backup tapes containing 2 million medical records being transported for the University of Miami's medical school, were stolen [13]. What is the value of those 2 million records? Would proper encryption have helped?

1. Metz, Rachel, AP Business, *Google makes health service publicly available*, May 19, 2008.
2. https://www.google.com/health/html/faq.html

(Continued on page 2)

## Cyber Crime News

An international cyber criminal ring with ties to organized crime has been broken with 38 people charged [1]. The ring used phishing (1.3 million emails were sent) attacks to steal personal financial data [2]. In other international news, Eugene Kaspersky, founder and CEO of Russian-based anti-virus experts Kaspersky Lab, said the number of cyber-criminals increased over tenfold since last year [3]. Cyber crime is finding its way into communities large and small. For example, in Tennessee, some criminals are using unsecured wireless connections to cover their tracks [4]. What happens is that a wireless routers can be used by bad actors. When law enforcement traces the source of the criminal, it originates as some person's home that is using an unse-

(Continued on page 2)

**Inside this issue:**



**Special points of interest:**

- Man convicted defrauding $350,000 (from Enron)
- NSA Web and email out for several hours due to improper DNS configuration

# On-line Medical Records

(Continued from page 1)


3. Scherzer, Lisa, Smaryt Money, *How to Choose a Personal Health Record*, May 1, 2008.
4. Chappell, Les, Wisconsin Technology Network, *DHC 2008: EMRs stimulate interest in personal health records*, May 8, 2008.
5. Miller, Chuck, SC Magazine, *Massive hacker server discovered*, May 7, 2008.
6. WSFA 12 News, *Patient Information "Disappears" from Montgomery Psychiatric Hospital*, May 17, 2008.
7. Mitchell, Eve, Media News (The Herald, Monterey County), *ID Theft: Bigger Threat Offline*, May 21, 2008.
8. Omstein, Charles, Los Angeles Times, *More tied to UCLA snooping*, May 13, 2008.
9. Whitcomb, Dan, Reuters, L.A. woman accused of stealing stars' medical info, April 29, 2008.
10. UPI, *Hospital data left open online,* May 3, 2008.
11. Appleby, Julie, USA Today, *Identity thieves prey on patients' medical records*, May 7, 2008.
12. Poremba, Sue Marquette, SC Magazine, *Medical data breaches on the rise*, May 14, 2008.
13. Fonseca, Brian, Computer World, *Thieves pilfer backup tapes holding 2M medical records*, April 24, 2008.


# Critical Infrastructure

*I think there is a world market for maybe five computers.*

*~ Thomas Watson, chairman of IBM, 1943*

For some time, there have been concerns that the critical infrastructure could be vulnerable to cyber attack. Congress is concerned that the electric industry group, North American Electric Reliability (NERC) is painting a rosy picture to a serious problem [1]. Similarly, the GAO found cyber security vulnerabilities with the Tennessee Valley Authority that could impact 8.7 million consumers [2].

Much of the current security philosophy is based on prevention. For example, at a recent NSA versus West Point cyber attack exercise, only one NSA attack was successful and one participant pointed out: "You can't make one mistake. It has to be perfect." [3] However, in the world of zero day attacks, this may be unrealistic. Another approach is to build a second defense that assumes an attack will get through. Proper technology separate from the various operating systems, such as smart cards, can provide security and tripwire detection alerting security personnel that a breach occurred.


1. Goss, Grant, IDG News, *Lawmakers See Cyber Threats to Electrical Grid*, May 21, 2008.
2. Mansfield, Duncan, Associated Press, *TVA system vulnerable to cyber attacks, GAO says*, May 22, 2008.
3. Howe, Kevin, Montery County Herald, *One Breach is One Too Many in Cyber Warfare*, April 29, 2008.


# Cyber Crime News

(Continued from page 1)

cured wireless configuration. One report indicates that Washington police trying to arrest a suspected pedophile were greeted by an innocent elderly lady [5]. The home user is a weak link in Internet security and it is unrealistic to expect the average user to fully understand computer security. For example, new routers include strong encryption that when turned on can mitigate the wireless piggyback threat described.


1. Claburn, Thomas, Information Week, *International Cybercrime Ring Busted*, May 19, 2008.
2. Mahony, Edmund H., Hartford Courant, *Dozens Charged With Running Computer Crime Ring*, May 20, 2008.
3. AFP, *IT chiefs warn of cyber-terrorism threat*, May 20, 2008.
4. Green, Josh, WJHL, *Cybertheft: The Crime Of The Future?*, May 23, 2008.
5. Ashwell, Rob, The Guardian (UK), *The wireless gateways to cybercrime*, May 22, 2008.

# Domestic Intelligence Gathering

While debate rages as to how much power to give domestic intelligence gathering, it is worth looking at how other countries are addressing counter terrorism. Brittan is planning a database to maintain records on every cell phone call and email [1].

Domestically, the house is working on a law that would update the 1979 Foreign Intelligence Surveillance Act [2]. Concurrent with the arguments pro and con on domestic cyber spying, the DHS indicates that Government agencies reported 12,986 cyber attacks in 2007 compared with 3,569 the year earlier [3].

As DHS tries to address the increasing threat, the debate will continue as to the best approaches. Readers may recall that in 1994 the Communications Assistance for Law Enforcement Act (P.L. 103-414) was enacted into law. The law provided funding and required telecommunications vendors to "dumb down" their equipment to facilitate wiretaps. Now, 14 years later, does anyone believe the Government should fund weakening security controls to make it easier for law enforcement monitoring?


1. Ford, Richard, Times on Line, *'Big Brother' database for phones and e-mails*, May 20, 2008.
2. Gorman, Siobhan, The Wall Street Journal, Lawmakers Near Agreement On Domestic Surveillance, May 23, 2008.
3. Joch, Alan, Federal Computer Week, Homeland security's cyber eyes, April 28, 2008.


# Bank Fraud

Up to $50 million was stolen using a fraudulent refund check scam [1]. Lou Pearlman, responsible for the Backstreet Boys and 'N Sync, was sentenced to 25 years in prison for swindling over $300 million from investors and banks [2]. A data breach at Bank of New York Mellon Corp. may have compromised customers at other banks [3]. The NY Mellon bank lost a tape containing records on 4.5 million people [4]. The ex-100 meter world record holder, Tim Montgomery, received jail time for his part in a $1.7 million bogus check bank fraud scheme [5]. Fake documents allowed a man to bilk two Kentucky banks out of $8 million [6]. Remember Enron? In addition to $2.2 million in bank and wire fraud, a jury in Delaware convicted a Canadian of stealing $350,000 from Enron [7]. So what other crimes might have contributed to the downfall of Enron? What is the true impact on US banks?

In other news, one report indicates the $7 billion loss at Société Générale was due in part to lax management [8]. The Société Générale fraud is unusual due to its size and that it was reported. In general, as one report depicts: "*But banks and other major companies are reluctant to release any figures about the losses they sustain, for fear of scaring off customers*" [9]. In other news overseas, approximately one million euros was stolen from 300 bank accounts in Ireland [10].


1. Duggan, Paul, Washington Post, *Former Bank Manager Pleads Guilty in D.C. Tax Fraud Case*, May 21, 2008.
2. Associated Press, *Boy band creator sentenced to 25 years in prison*, May 21, 2008.
3. AP, Conn. *subpoenas 2 banks over data loss*, May 22, 2008.
4. Podsada, Janice, Hartford Courant, *Customer Info From More Banks May Be On Lost Tape*, May 23, 2008.
5. BBC News, US sprinter jailed for bank fraud, May 16, 2008.
6. WTVW– IN, *Beaver Dam Bank Fraud*, May 21, 2008.
7. O'sullivan, Sean, The News Journal (Delaware), *Man sentenced for defrauding Enron*, May 22, 2008.
8. Vandore, Emma, AP Business, *Societe Generale cites lax management in $7B fraud*, May 23, 2008.
9. BBC News, *What makes a cyber criminal?*, May 19, 2008.
10. Belfast Telegraph, *One million euro stolen in bank card scam*, May 21, 2008.

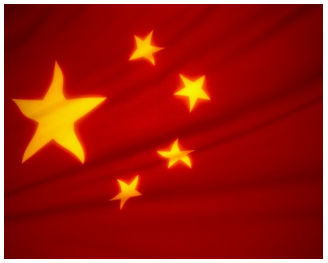

*640K ought to be enough for anybody.– -Microsoft Chairman Bill Gates, 1981 (discussing computer RAM)*

# China in the News

Reports indicate there is a server farm in China that is using an SQL injection attack against other servers in China and Taiwan [1].

US military sources are concerned that China is becoming a significant space and cyber threat [2]. Consider the impact if the Global Positioning System (GPS) and communications satellites were shot down. What would the US response be?

In other news, countries continue to blame China for hacking [3]. There is a report that fake credit cards from China are responsible for significant losses within Pakistan [4].




1. Lemon, Sumner, IDG News Service, Mass SQL Injection Attack Targets Chinese Web Sites, May 19, 2008.
2. Wolf, Jim, Reuters, *U.S. military cites growing China space*, cyber threat, May 20, 2008.
3. Baluni, Akshay, International Business Times, *Nations blame China for recent cyber hackings*, May 20, 2008.
4. Sharif, Shafiq, Dailey Times Pakistan, *Counterfeit credit cards main source of cyber crime*, May 21, 2008.


# DNS News

The Domain Name System (DNS) is critical for relying Internet applications that need to resolve a numeric address from a name. If you were trying to reach the National Security Agency (NSA) May 15, their web server and email was down for several hours due to an improper DNS configuration [1]. Recognizing the need to protect DNS, the DHS has awarded a contract to add DNS Security Extensions (DNSSEC) [2]. This follows OMB's announcement that agencies will be required to strengthen their DNS [3].

*Any sufficiently advanced technology is indistinguishable from magic.–Arthur C. Clarke*


1. Carr, Jim, SC Magazine, *NSA's website outage due to lack of topological "diversity"*, May 16, 2008.
2. Campbell, Dan, GCN, *DHS moves to strengthen domain name servers*, May 22, 2008.
3. Rendleman, John, Federal Computer Week, *OMB plans domain name security measures*, May 14, 2008.


# Security Tools

Is it reasonable to expect software based security products to offer complete security? We now live in a world where you go to a web site or open a email message and get infected. Many organizations rely on single products to protect computer and network assets. The threats originating from malware are such that software only solutions will have a difficult time. Consider the case of a new host-based firewall and anti-spam product that was silently infected during product testing [1]. Other products such as HackerSafe also exhibits zero day attack vulnerabilities [2].

The threat environment continues to grow with no end in sight. Trend Micro is reporting more than two million malicious code patterns during the first four months of 2008 [3]. Against this onslaught, those responsible for IT security must think more innovatively. The formula for protection is constantly changing.


1. Grimes, Roger A., Info World, *ZoneAlarm ForceField: Compromised in sixty seconds*, May 21, 2008.
2. McFeters, Nathan, ZDNet blogs, *More bad news for McAfee, HackerSafe certification*, May 1, 2008.
3. Oltsik, Jon, Cnet news blog, *Scary security numbers from Trend Micro*, May 8, 2008.