Banking & Finance in Cyberspace:

Exposure, Risk, and Technology in the Making

By: M.E. Lau

Utica College, Cybersecurity:

Critical National Infrastructure, Spring 2012

Author Note:

Correspondence concerning this paper should be addressed to M.E. Lau.

Email: melau@utica.edu

Abstract

The banking and finance sector, power grid, communications networks, chemicals, energy, defense industrial base, transportation systems, and government facilities have placed sensitive data on computers connected to the Internet.[1] The convenience and accessibility of storing digital data provides a deceiving sense of safety and comfort that no further concerns are necessary. However, threats to computer network security have proven their existence time and again. This paper discusses banking and finance in terms of data security breaches, current security methods, and the newest cybersecurity solutions as of February 2012.

As technology evolves, crime follows suit. Not long after the invention of the computer and Internet, engineers and programmers toyed with network vulnerabilities. In 1971, the Creeper virus would replicate itself, manifesting on displays with the message "I'm the creeper, catch me if you can!"[2] While seemingly inane pranks started out as mischief and one-ups-man-ship, the world wide web and scale-free networks have created an open playground of sitting ducks for criminal enterprises and organized crime networks.

Predictably, the worst data security breaches involved banking or financial data.[3] In July 2007, a fired employee of Fidelity subsidiary Certegy Check Services stole 3.2 million customer records including credit card, banking and personal information. William Sullivan, a senior database administrator who was responsible for defining and enforcing data access,[4] committed theft in May 2007. Sullivan sold the data for $580,000; the data was resold to marketing firms such as Strategia Marketing LLC, also known as Suntasia.

Stolen information included names, addresses, bank account information and credit card information. To avoid detection, Sullivan downloaded the data to a storage device instead of transmitting it over the Internet.[5] Sullivan pled guilty, sentenced to 57 months' imprisonment with $3.2 million in restitution for conspiracy and computer fraud.[6]

Fidelity's security breach is a classic example of the insider threat.

According to a study conducted by the U.S. Secret Service and CERT Coordination Center, perpetrating insiders ranged from 18 to 59 years of age. 42% percent were female; 58% were male. There was a variety of racial and ethnic backgrounds, as well as family situations. 54% were noted as single and 31% married. Insiders were employed in a variety of positions: 31% in service, 23% in administrative/clerical, 19% in professional, and 23% in technical. Only 17% had system administrator or root access prior to the incident.[7]

These statistics show the challenge of profiling a potential insider threat. A preventative solution such as removing access rights prior to termination would not have been effective in Fidelity's breach because Sullivan transferred information well before his termination.

In this case, implementing a monitoring alert system may have communicated attempted breaches immediately. An attempt to transmit, attach, or download sensitive information would have alerted information security personnel. Critical information protection strategies include building secure automated encryption options into sensitive information. Attempts to transmit, attach or download sensitive information may activate automated encryption which obfuscates data and locks the network from sending or receiving.[8]

When information is not encrypted, hackers are able to access information easily upon infiltration. In June 2005, 40 million credit card

accounts were exposed at CardSystems Solutions, a top payment processor for Visa, MasterCard, and American Express. Using an SQL Trojan attack, hackers broke into CardSystems' database. The SQL Trojan inserted code into the database via the website every four days, placing data into a zip file and sending it back through an FTP. CardSystems failed to encrypt information, and gave hackers access to names, accounts numbers, and verification codes to more than 40 million card holders.[9]

A paper written in September 2007 discusses the evolving nature of SQL Trojan attacks and its two-pronged nature: the attack, and the evasion of threat detection systems.[10] Traditionally, SQL injection attacks were prevented using pattern-matching techniques against signatures and keyword-based stores to identify potentially malicious requests.

Similar to the Trojan Horse of Greek lore, dangerous code is hidden inside a valid request and deploys after it has been accepted inside the walls of the data center. Threat prevention products such as Intrusion Prevention Systems (IPS)[11] and application firewalls have evolved to detect hidden attacks using pattern matching.

Nevertheless, hackers mutated their code into a “Trojan Zebra,” each packet with a unique signature, like a unique set of stripes, which evaded pattern matching detection techniques. Furthermore, Trojan Zebras’ code may imitate

legitimate patterns. Along with high volumes of signature permutations that resemble good code, the Zebra has outsmarted pattern matching detection.

Throughout 2010, VeriSign, the company responsible for authenticating more than half the world's websites, had been hacked multiple times. In response to updated U.S. Securities and Exchange Commission (SEC) guidelines on reporting security breaches to investors, the VeriSign attacks were revealed in a 2000-page disclosure a year after the breach (2011). [13]

Although VeriSign reported no critical systems including DNS or certificate servers were compromised, "access was gained to information on a small portion of our computers and servers."[14] Described as “the web’s core,” VeriSign’s 50 billion daily queries ensures visited websites are legitimate via digital certificates. An article expounded on the potential implications of the threat, stating,

> *“It's possible that the VeriSign hackers could turn the Web upside down and create an Internet where nothing would be what it seems. A hacker website could look and act just like your bank's website. Your PC could easily be tricked into downloading automatic software updates that would appear authentic but actually contain viruses. And no matter what web address you typed into your browser, you could be redirected to a criminal's website half-way around the world.”* [15]

In December 2006, an estimated 94 million TJX credit cards were exposed due to zero encryption and no firewall, according to reports. TJX is the parent company of T.J.Maxx, Marshalls, HomeGoods and A.J. Wright in the

U.S., Winners and HomeSense in Canada, and T.K. Maxx in Britain. With a total of 46 million customer records compromised, the TJX case outranks CardSystems' 2005 hack in which hackers accessed accounts of 40 million card holders.[16]

TJ Maxx's thousands of brick and mortar locations, millions of customers, and high-profile brand resulted in more immediate disclosures and an increased level of accountability. The cascade of post-breach events involved credit card companies contacting 28 banks to report millions of accounts as compromised and untrustworthy. To step up security efforts, Visa incentivized merchants and transaction service providers to comply with the Payment Card Industry (PCI) Data Security Standard, requiring limits on data storage and encryption.[17]

In December 2008, 134 million credit cards on Heartland Payment System's servers were exposed through an SQL injection. Heartland processes approximately 100 million payment transactions for over 250,000 businesses, mostly restaurants. The forensics teams hired by Heartland found software planted on "its payment processing network that recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients."

The stolen data included names, credit, debit card numbers and expiration dates – but thankfully, social security numbers, PIN numbers, addresses and

telephone numbers were left intact. Hackers did, however, access the digital information encoded onto the magnetic stripe built into the backs of credit and debit cards. With this data, thieves are able to create counterfeit credit cards by imprinting identical stolen information onto fabricated cards.

Since credit card numbers may easily be replaced, stealing such data may become obsolete. Lesser breaches occurred at other card payment systems such as RBS Worldpay and Hannaford Brothers.[18]

As evidenced, the financial services sector is a priority for online criminal enterprises, which include data breaches and using the data for monetary gain. One company, ForeScout, provides comprehensive network security solutions through CounterACT, a technology in a box that contains multiple solutions and runs on a network, instead of through a client or agent.

CounterACT's abilities include data security, network access control, mobile security, threat prevention, endpoint compliance, BYOD security, regulatory compliance, and agent-less visibility. Agent-based data security strategies utilize encryption, firewalls, host attack prevention (anti-virus), and data access policies – all of which address cybersecurity needs.

ForeScout also addresses the problem of how agent-based data security may be turned off or bypassed, citing an investigation in 2007 that "over 50% of their own computers had a problem with their security agents or

configuration." Thus, ForeScout designed CounterACT to surveille and control managed and unmanaged endpoints. By operating over the network and not relying on host-based software, CounterACT is able to detect all wireless and wired devices including smart phones, printers, tablets, laptops and traditionally networked computers.

Device interrogation and network access controls are part of CounterACT's services that enable an operator to accept or reject a device's request to connect to a company's network, based on the device interrogation information provided. CounterACT mitigates risk by filtering devices and users through five layers of protection.

1. A physical layer allows only authorized users on the network.
2. A network layer blocks attacks within the network.
3. A system layer ensures security agents including antivirus, encryption, and DLP are deployed while confirming OS patches.
4. An application layer detects which computers have outdated, vulnerable applications.
5. A user layer educates users with real-time notifications when they violate security policies and prevents use of unauthorized applications or USB devices by automatically disabling them.

CounterACT's network layer is said to be armed with the ability to pre-empt zero-day attacks, suppress propagating worms, stop low and slow attacks, and reduce advanced persistent threat (APT) risks. ForeScout addresses the problem of unmanaged devices, and the boundary-less network perimeters that

create vulnerable holes in a network. [19]

ForeScout's ActiveResponse patented technology is said to have detected and blocked attacks such as Zeus and Stuxnet on day-zero, "before any security company anywhere had developed a signature for these attacks." ActiveResponse operates by detecting and blocking any attack that "goes over the network and relies on reconnaissance to identify possible targets." ForeScout boasts "ActiveResponse does not rely on signatures, updates, or a learning period to detect day-zero attacks."

In addition, tens of thousands of worms such as Conficker are mentioned to have been suppressed by ActiveResponse. Conficker, the most successful computer worm since the 2003 SQL Slammer worm, infected more than seven million government, business and home computers. While traditional IPS and antivirus systems had trouble blocking Conficker, ActiveResponse is said to have been able to block Conficker "with extreme efficiency and accuracy."

ForeScout claims that ActiveResponse "doesn't need to perform deep packet inspection on either the network traffic or the payload file." For insider threats and APTs like Stuxnet, ForeScout says ActiveResponse is capable of blocking both.[20]

The innovative nature of ForeScout's technologies have gained the attention of Frost & Sullivan, a global research consulting firm which monitors more than 300 industries and 250,000 companies.

A nine-page report details the decision to give ForeScout a 2012 technology innovation award for network access control. Five criteria were judged: uniqueness of technology, impact on new products and applications, impact on functionality, impact on customer value, and relevance of innovation to industry. ForeScout scored between 9 and 10 on all five criteria on a scale of 1-10. Frost & Sullivan concludes the report mentioning "…ForeScout security solutions are easy to deploy, unobtrusive, intelligent and scalable, they have been chosen by more than 1,000 of the world's most secure enterprises and military installations for global deployments spanning 37 countries."[21]

ForeScout's achievements are a protective win for healthy economies. Nonetheless, domestic and international cyber-crime continue to recruit. According to Joseph Menn, keynote speaker and author of *Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet*, cyber-crime is just another career opportunity.[22] Crime happens, and for some countries, cybercrime is the only job that pays. An American political statement from the last decade of the 20th century comes to mind: "It's the economy..."[23]

Footnotes:

[1] Department of Homeland Security. (2009). National Infrastructure Protection Plan. P.3
[2] http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms#1960.E2.80.931969

[3] Amerding, Taylor. "The 15 Worst Data Security Breaches of the 21st Century." CSO Online. February 15, 2012. http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century

[4] Gradijan, Dave. Millions of Records Stolen from Fidelity Subsidiary. July 3, 2007. http://www.csoonline.com/article/216597/millions-of-records-stolen-from-fidelity-subsidiary

[5] Gradijan, Dave. Millions of Records Stolen from Fidelity Subsidiary. July 3, 2007. http://www.csoonline.com/article/216597/millions-of-records-stolen-from-fidelity-subsidiary

[6] United States Attorney's Office, Middle District of Florida, "Largo Man Sentenced for Stealing Consumer Information", July 10, 2008, News Release. See: www.cybercrime.gov/sullivanSent.pdf

[7] U.S. Secret Service and CERT Coordination Center. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." August 2004. www.cert.org/archive/pdf/bankfin040820.pdf

[8] Ideas and suggestions from author's own thought process while writing this paper.

[9] Amerding, Taylor. "The 15 Worst Data Security Breaches of the 21st Century." CSO Online. February 15, 2012. http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century

[10] Vittie, Lori Mac. "SQL Injection Evasion Detection." F5 Networks. September 2007. www.f5.com/pdf/white- papers/sql-injection-detection-wp.pdf

[11]Newman, Robert C. (19 February 2009). *Computer Security: Protecting Digital Resources*. Jones & Bartlett Learning. pp. 273–. ISBN 9780763759940. http://books.google.com/books?id=RgSBGXKXuzsC&pg=PA273. Retrieved 25 June 2010. Also see: http://en.wikipedia.org/wiki/Intrusion_prevention_system

[12] http://www.businesswire.com/news/home/20111102005558/en/F5-BIG-IP-Application-Security-Manager- Awarded-Five-Star. Press News Release November 2011.

[13] Brenner, Bill. Salted Hash. VeriSign Hit By Hackers. 2/2/2012. http://blogs.csoonline.com/data- protection/2013/verisign-hit-hackers

[14] Amerding, Taylor. "The 15 Worst Data Security Breaches of the 21st Century." CSO Online. February 15, 2012. http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century

[15] Sullivan, Bob. VeriSign, at web's core, is hacked: What does it mean to you? The Red Tape Chronicles on MSNBC.com. February 2, 2012. http://redtape.msnbc.msn.com/_news/2012/02/02/10302393-verisign-at-webs-core- is-hacked-what-does-it-mean-to-you

[16] Jewell, Mark. TJ Maxx theft believed to be largest hack ever. Associated Press. 3/30/2007. http://www.msnbc.msn.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack- ever/

[17] Evers, Joris. TJ Maxx hack exposes customer data. CNET news. 1/18/2007. http://news.cnet.com/T.J.-Maxx- hack-exposes-consumer-data/2100-1029_3-6151017.html

[18] Krebs, Brian. Payment processor breach may be largest ever. The Washington Post. 1/20/2009. http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html

[19] http://www.forescout.com/solutions/data-security/

[20] http://www.forescout.com/solutions/threat-prevention/

[21] Frost & Sullivan. Best Practices Research. "2012 Technology Innovation Award Network Access Control." 2012. See: http://blog.forescout.com/Landing-FS-Award/

[22] Brenner, Bill. Salted Hash. VeriSign Hit By Hackers. 2/2/2012. http://blogs.csoonline.com/data- protection/2013/verisign-hit-hackers

[23] http://en.wikipedia.org/wiki/It%27s_the_economy,_stupid