Femtosecond®
www.femto-second.com

In the News

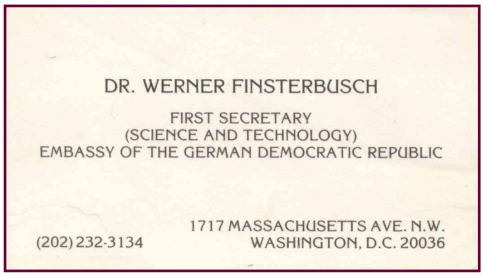
Volume 1 Issue 8

May 18, 2008

Government Sponsored Cyber Attack Capabilities

The US is increasingly under attacked by overseas hackers. Recognizing the potential to use hacker tools for cyber warfare; one Air Force colonel suggested using bot-nets to attack enemies [1]. This leads us into the topic of how various governments look at hacker tools and techniques as potential weapons.

State sponsored interest in hacker tools in not new. In 1998, at the 4th Aerospace Computer Security Applications Conference, in Orlando, Florida, a representative from the Old East German embassy was very interested in computer viruses. This conference took place just after the Morris worm shut down the Internet [2]. Why do you suppose the East Germans were interested in computer viruses?


DR. WERNER FINSTERBUSCH
FIRST SECRETARY
(SCIENCE AND TECHNOLOGY)
EMBASSY OF THE GERMAN DEMOCRATIC REPUBLIC
1717 MASSACHUSETTS AVE. N.W.
WASHINGTON, D.C. 20036
(202) 232-3134

A Former East German Curious About Computer Viruses

Early on, computer viruses were considered as potential weapons. For example, in 1990, there was discussion of using stealth computer viruses as weapons [3]. During the same year, one scenario was published describing to how viruses could be used in attacking military targets [4]. Most viruses primarily attack software. However, there is a more sinister vulnerability where a Trojan horse or other exploit is embedded within the hardware. Once the hardware is deployed, the costs for correcting the problem could be staggering.

Consider the fear expressed by the FBI that counterfeit Chinese network routers and switches, purporting to be Cisco products, found their way into the U.S. government supply chain [5]. Some have blamed the failure on existing procurement practices [6]. However there is a much larger problem in that much of the electronics used within the Government is now built overseas. For example, in examining a Linksys® (by Cisco) WRT54G2 router to see where it was manufactured; sure enough it was made in China. So a question will be, regardless of if the hardware is counterfeit or not, how do you know there are no Trojan horses? The fear of malicious hardware entering Government networks has spawned research from the Defense Advanced Research Projects Agency (DARPA) for ways to finds hardware Trojan horses [7].

The idea that technology manufactured outside of the US poses a risk (Continued on page 2)

Cyber Crime & Terrorism

Global concern for cyber terrorism is resulting in more cooperation amongst countries trying to address the problem. Malaysia will host World Cyber Security Summit with representatives from over 30 countries expected [1]. Within the North Atlantic Treaty Organization (NATO), 7 nations are backing a cyber defense center in Estonia [2]. You may recall that Estonia was subjected to a cyber attack last year that crippled the country [3].

In an expected US response to cyber terrorism, the administration has proposed a $17 billion plan that is being criticized for secrecy [4]. In this world of globalization where our equipment is made overseas, it is hard to imagine how the administration's proposals will solve the problems.

(Continued on page 2)

Inside this issue:

Special points of interest:

- Chinese Hacking against Belgium
- Counterfeiting currency is on the rise

Government Sponsored Cyber Attack Capabilities

(Continued from page 1)

is not new [8]. With China in the news, there are reports their cyber-attack capability is State sponsored [9]. Consider that today no laptop computer is made in the US. Couple this with the following argument: "*There is so much [application development] outsourcing to India and China and other countries. Anyone can put backdoors in there," Khera said. "If you don't do thorough testing for backdoors and other security testing, you have no idea what might be in there. You just don't know what's* in the *code"* [10].

The fake Cisco equipment highlights the following: "*Defense and industry officials describe DOD networks as the Achilles' heel of the powerful U.S. military"* [11]. Perhaps another way to look at the problem: "*you'd have no reason to use counterfeit gear when many of the components for the real stuff are made in factories you can directly or indirectly control"* [12]. Unfortunately, we must hope that the foreign governments that now hold the world's wealth will partner with us in protecting our computing resources.

There is no reason for any individual to have a computer in his home.–Ken Olsen (President Digital Equipment, 1977)

1. Robertson, Jordan, Associated Press Technology, *Colonel suggests using hackers' tool against them*, May 15, 2008.
2. Eisenberg, T., et. al., Communications of the ACM, *The Cornell commission: on Morris and the worm, June*, 1989.
3. Raymond M. Garth, Sr., *Stealth Viruses... Weapon Systems of Tomorrow?*, Defense Computing, May-June, 1990, pp. 34- 36.
4. *Computer Viruses in Electronic Warfare*, Fourth Annual Computer Virus Conference, New York, 1990
5. World Tribune, FBI: *China may use counterfeit Cisco routers to penetrate U.S. networks*, May 15, 2008.
6. Jackson, Joab, GCN, *Fake Cisco gear suggests procurement failure*, MY 14, 2008.
7. Adee, Sally, IEEE Spectrum, *The Hunt for the Kill Switch*, May, 2008.
8. Dupont, Daniel G., Scientific American, *Software Insecurity Outsourcing and Defense of "foreign influence,"* March 13, 2006.
9. Vaas, Lisa, eWeek, *China Prepares for First Strike in Electronic War*, May 30, 2007.
10. Pulley, John, Federal Computer Week, *Weak spots in the fortress*, April 30, 2007.
11. Tiboni, Frank, FCW, *The new Trojan war*, August 22, 2005.
12. Murphy, Paul, ZDNet, *Buying from the Enemy*, May 17, 2008.

Cyber Crime & Terrorism

(Continued from page 1)

Perhaps the old Bob Hope commercials from 1985, *Made in the USA it matters* [5], should be considered for more that the garment industry. In the interim there are a number of technical controls, including smart cards that can be better utilized to reduce overall risk.

The days of the lone hacker boasting about exploits has been replaced by crooks seeking profit [6]. With a trade deficit down to a mere $58.2 Billion [7], we are a debtor nation. As US wealth continues to erode, foreign nations will continue to be in a position to exert undue influence over American security and politics.

1. Jackson, William, DCN, *Major cyberterrorism meeting scheduled*, May 15, 2008.
2. Reuters, *NATO nations back cyber defence centre*, May 14, 2008.
3. BBC News, *Estonian cyber defence hub set up*, May 14, 2008.
4. Olson, Bradley, The Baltimore Sun, *Cyber security plans assailed*, May 18, 2008.
5. Foltz, Kim, The New York Times, *Advertising; Tough New Campaign for U.S. Clothing*, May 18, 2008.
6. Fong, Cherise, CNN, *Fighting the agents of organized cybercrime*, May 9, 2008.
7. Thompson Financial News, *US March trade deficit falls 5.7 pct to $58.2 bln as economy slows*, May 9, 2008.

Hacking in the News

In Chile, a hacker accessed and posted to the Internet government data on 6 million citizens [1]. The reported hacker's reasons were to show how poorly Chile protects personal data [2].

Within the US, 2 hackers using a *packer sniffer*, were charged with stealing credit card numbers at a restaurant chain that caused at least $600,000 in financial institution loss [3]. In India, according to one survey, 30 percent of the top banks admitted to being identity theft victims [4]. Given the reluctance to admit losses, the actual losses may be much higher.

As we look toward the future, we can predict what type of attacks to expect based on the tools that hackers are developing. For example, hackers have developed a rootkit for the Cisco Internetwork Operating System (IOS) [5]. Consider what a hacker could do controlling routers throughout a department network.

1. Associated Press, *Chile probes data theft and posting by hacker*, May 12, 2008.
2. Hulme, George, Information Week, *Hacker Publishes Personal Data Of Six Million Onto Internet*, May 12, 2008.
3. Reuters, *Three accused of hacking Dave & Buster's computers*, May 12, 2008.
4. Prasad, Swait, ZDNet Asia, *Indian Banks Worry about Online Security*, May 9, 2008.
5. McMillan, Robert, IDG News Service, *Hacker Writes Rootkit for Cisco's Routers*, May 14, 2008.

Electronic Passport Security Weaknesses?

The State Department of State (DOS) is issuing electronic passports that include an Radio Frequency ID (RFID) that some are arguing lacks adequate security [1]. One concern cited is the new passports can facilitate identity theft [2].

The DOS has worked with the International Civil Aviation Organization (ICAO) for standardization. Privacy advocates worry that RFID can be captured and later replayed. That is, the RFID device is not an active processor, typical of a contact smart card, but rather a simple storage and retrieve device. Similar in risk to a credit card, if the information can be captured, it can be played back later. The ICAO has defined Machine-Readable Travel Documents (MRTD), which interestingly, are also used in the Personal Identity Verification (PIV) Card [4].

Passports have been the gold standard in verifying the identity of a person. However, counterfeiters are always a risk. For example, over 1,000 fake passports were seized in Thailand last month [5]. Interestingly, the new US passport covers are made at the Thailand Smartrac plant [6].

The Chip Contents

- *The same data visually displayed on the data page of the passport;*
- *A biometric identifier in the form of a digital image of the passport photograph, which will facilitate the use of face recognition technology at ports-of-entry;*
- *The unique chip identification number; and*
- *A digital signature to protect the stored data from alteration [3].*

The MRTD data includes a digital signature for integrity protection. However, if the RFID readers do not verify the signature then any bogus value of the correct length could pass as legitimate. In those limited cases where digital signatures are validated, copied information would limit bad actor use to people with a resemblance to the internal (biometric) picture.

1. Gertz, Bill, The Washington Times, *Passport cards called security vulnerability*, May 16, 2008.
2. Kay, Liz F., Baltimore Sun, *Radio tags raise concern about personal ID theft*, May 14, 2008.
3. http://travel.state.gov/passport/eppt/eppt_2788.html
4. NIST SP, Interfaces for Personal Identity Verification Part 4: The PIV Transitional Interfaces and Data Model Specification, section 2.3.5.
5. Reuters, *Thai police seize more than 1,000 fake passports in raid*, April 27, 2008.
6. Gertz, Bill, The Washington Times, *Fake U.S. passport ring in Thailand busted*, April 28, 2008.

Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away.– Antoine de Saint-Exupery

Financial News

Freddie Mac has set aside $1.2 billion to cover mortgage losses with a quarterly $151 million loss reported [1]. On the bright side, the Treasury secretary said financial markets are calmer [2]. This as more banks are taking record advantage of loans offered by the Fed [3].

In other news, bank fraud continues to be reported with Waukesha Bankshares Inc. indicating a $450,000 loss due to fraud. HSBC appears to have lost a server in Hong Kong that contained information on 159,000 customers [5]. At the same time, HSBC Holding Plc, Europe's largest bank by market value, needed less than the expected $3.2 billion to cover bad loans [6]. Perhaps the worst is over.

1. Zibel, Alan, Associated Press, *Freddie Mac loses $151M in 1Q as home loans falter*, May 14, 2008.
2. Crutsinger, Martin, Associated Press, *Treasury secretary says markets are calmer now*, May 16, 2008.
3. Anstey, Christopher and Matthews, Steve, Bloomberg, *Fed's Direct Loans to Banks Climb to Record Level*, May 16, 2008.
4. Gores, Paul, Milwaukee Journal Sentinel, *U.S. suspects fraud by Sunset Bank customer*, May 8, 2008.
5. Yeo, Vivian, ZDNet Asia, *HSBC loses server with info on 159K accounts*, May 9, 2008.
6. Bloomberg, *HSBC Sets Aside $3.2 Billion for More Bad U.S. Loans*, May 12, 2008.

Prediction is very difficult, especially about the future.

–Niels Bohr

More Chinese Attacks

The latest country to accuse the Chinese of cyber attacks is Belgium [1]. The Belgian justice minister indicated Chinese attacks were being directed against the Belgian Federal Government [2]. There is speculation that China is interested in spying Belgium because the North Atlantic Treaty Organization (NATO) and European Union have headquarters there [3]. Recall that last week, the focus of Chinese attacks was India [4]. The Chinese attacks were such that even the computers at the Indian embassy in Beijing were hacked [5].

1. Information Age, *Belgium reports Chinese cyber attack*, May 8, 2008.
2. Jaques, Robert, ITWeek, *Belgium accuses China of cyber-crimes*, May 7, 2008.
3. InfoZine, *Belgium Accuses Chinese Government of Cyberespionage*, May 12, 2008.
4. Bagchi, Indrani, *The Times of India, China mounts cyber attacks on Indian sites*, May 5, 2008.
5. Gangadharan, Surya, CNN-IBN, *Chinese cyber crawlers hack Indian Govt site*, May 5, 2008.

Counterfeiting

In our paper driven world, technology advances increase the likelihood of counterfeiting. Consider the security controls that go into US currency. Yet we continue to see more cases of counterfeiting. For example, the arrest of 5 people that printed and distributed $7 million in bogus bills [1]. This operation was a home grown operation [2]. In another example, a man pleaded guilty to creating bogus bills in South Carolina [3]. Counterfeiting is on the increase [4]. The question here is how long will it be before digitally signed electronic documents will be more widely accepted than paper currency?

1. Roope, Jim, LiveNews, *US police crack $7 million counterfeit money ring*, May 18, 2008.
2. Glover, Scott, LA Times, *Five arrested after Secret Service probe into Southern California counterfeit ring*, May 14, 2008.
3. Columbia, SC (WIS), *Midlands man pleads guilty to counterfeit conspiracy*, May 14, 2008.
4. KGET, *Authorities say counterfeit money on the rise*, May 7, 2008.