Security Absurdity: The Complete, Unquestionable, And Total Failure of Information Security.

A long-overdue wake up call for the information security community.

by Noam Eppel
Vivica Information Security Inc.

Boiling Frog Syndrome

They say if you drop a frog in a pot of boiling water, it will, of course, frantically try to scramble out. But if you place it gently in a pot of tepid water and turn the heat on low, it will float there quite complacently. As you turn up the heat, the frog will sink into a tranquil stupor and before long, with a smile on its face, it will unresistingly allow itself to be boiled to death. The security industry is much like that frog; completely and uncontrollably in disarray - yet we tolerate it since we are used to it.

It is time to admit what many security professionals already know: We, as security professionals, are drastically failing ourselves, our community and the people we are meant to protect. Too many of our security layers of defense are broken. Security professionals are enjoying a surge in business and growing salaries and that is why we tolerate the dismal situation we are facing. Yet it is our mandate, first and foremost, to protect.

The ramifications of our failure are immense. The success of the Internet and the global economy relies on trust and security. Billions of dollars of ecommerce opportunities are being lost due to inadequate security. A recent survey of U.S. adults revealed that three times the number of respondents believed they were more likely to be victimized in an online attack than a physical crime. A recent Gartner survey that indicated that 14% of those who had banked online had stopped because of security concerns, and 30% had altered their usage. People are simply losing trust in the Internet.

The security community is not just failing in one specific way, it is failing across multiple categories. It is being out innovated.

It is losing the digital battle over cyberspace.

Failing? Says Who?

Today we have fourth and fifth generation firewalls, behavior-based anti-malware software, host and network intrusion detection systems, intrusion prevention system, one-time password tokens, automatic vulnerability scanners, personal firewalls, etc., all working to keep us secure. Is this keeping us secure? According to USA Today, 2005 was the worst year ever for security breaches of computer systems. The US Treasury Department's Office of Technical Assistance estimates cybercrime proceeds in 2004 were $105 billion, greater than those of illegal drug sales. According to the recently released 2005 FBI Computer Crime Survey,

nearly nine out of 10 U.S. businesses suffered from a computer virus, spyware or other online attack in 2004 or 2005 despite widespread use of security software. According to a Federal Trade Survey, approximately 9.9 million were victims of identity theft in 2003 alone - which is approximately 27,000 victims of ID theft per day! And companies like IBM are putting out warning calls about more targeted, more sophisticated and more damaging attacks in 2006.

Something is seriously wrong.

One only has to open a newspaper and view current headlines documenting the almost constant loss of personal and financial data due to carelessness and hacking. It isn't just careless individuals that are leaking confidential information - it is large, multinational corporations with smart, capable I.T. departments with dedicated security professionals and huge security budgets.

Credit Card Breach Exposes 40 Million Accounts
Bank Of America Loses A Million Customer Records
Pentagon Hacker Compromises Personal Data
Online Attack Puts 1.4 Million Records At Risk
Hacker Faces Extradition Over 'Biggest Military Computer Hack Of All Time'
Laptop Theft Puts Data Of 98,000 At Risk
Medical Group: Data On 185,000 People Stolen
Hackers Grab LexisNexis Info on 32000 People
ChoicePoint Data Theft Widens To 145,000 People
PIN Scandal 'Worst Hack Ever'; Citibank Only The Start
ID Theft Hit 3.6 Million In U.S.
Georgia Technology Authority Hack Exposes Confidential Information of 570,000 Members
Scammers Access Data On 35,000 Californians
Payroll Firm Pulls Web Services Citing Data Leak
Hacker Steals Air Force Officers' Personal Information
Undisclosed Number of Verizon Employees at Risk of Identity Theft

Just How Bad Is It?

In some cases, even our best recommended security practices are failing.

In a recent experiment, AvanteGarde deployed half a dozen systems in honeypot style, using default security settings. It then analyzed the machines' performance by tallying the attacks, counting the number of compromises, and timing how long it took an attack to successfully hijack a computer once it was connected to the Internet. The average time until a successful compromise was just four minutes!

A person can go to his/her local computer store and purchase an expensive new computer, plug it in, turn it on and go get a coffee. When he/she returns the computer could already be infected with a trojan and being used in a botnet to send out spam, participate in phishing attacks, virus propagation, and denial-of-service attacks, etc.

The first thing most consumers do with a new computer is surf the Internet, play games, send emails - not install patches. However, even if a person was security-aware and even if the person followed SANS Incident Response Center's recommendations for Surviving the First Day of Windows XP, they will still be left vulnerable as the process of downloading and installing the latest Microsoft patches which may be as small as 70 megabytes (MB) or as large as 260 MB, takes longer than the time it takes for an unpatched computer to be compromised. "In some instances, someone had taken complete control of the machine in as little as 30 seconds," said Marcus Colombano, a partner with AvanteGarde.

The Failures Are Everywhere

The effects of our failure can be seen everywhere.

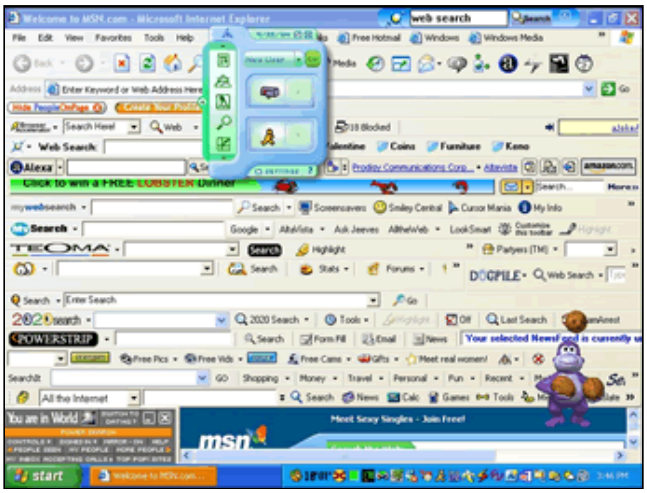
SPYWARE

The average user's computer is absolutely crawling with spyware and popups. According to the National Cyber Security Alliance a staggering 91 percent in the study have spyware on their computers. According to a report from EarthLink and Webroot Software, a scans of over 1 million Internet-connected computers found there's an average of almost 28 spyware programs running on each computer. Spyware can cause extremely slow performance, excessive and unsolicited pop-up advertisements, hijacked home pages, theft of personal information (including financial information such as credit card numbers), monitoring of Web-browsing activity for marketing purposes, routing of HTTP requests to advertising sites, etc. Sometimes Spyware can cross the line when it expose adult pornography to children.

Eric Howes, a renowned security researcher at the University of Illinois at Urbana-Champaign, found that many of the best-performing anti-spyware scanner "fail miserably" when it comes to removing spyware from infected computers, with some missing up to 25% percent of the critical files and registry entries installed by the malicious programs. Recovering from malware is becoming impossible, according to Microsoft.

PHISHING

Phishing scams now exceed 40 million attempts per week. Phishing attacks started as poorly written email messages in broken English that only the most gullible would fall for. Today Phishing attacks are sophisticated operations with emails and fake websites that appear almost identical to the real thing. In June 2004, the Gartner Group reported that online bank accounts had been looted of $2.4 billion just in the previous 12 months. It estimated that 1.98 million adults in America had suffered losses with Phishing attacks which usually impersonate well known brands such as eBay, PayPal, Visa, SouthTrust Bank, KeyBank, AOL, Comcast, Earthlink, Citizen Bank, Verizon, etc.



Look familiar? The average user's computer is crawling with spyware and popups.

George Ou revealed that many large American financial institutions are not using SSL to verify their identity to the customer. This makes it more easy for a phishing attacker to intercept and spoof a financial web site. Financial institutions that were identified as not using SSL properly include: American Express, Bank of America, Chase, Countrywide, DCU, Georgia Telco Credit Union, Keybank, NationalCity, NAVY Federal, PSECU, US Bank, Wachovia, and Washington Mutual.

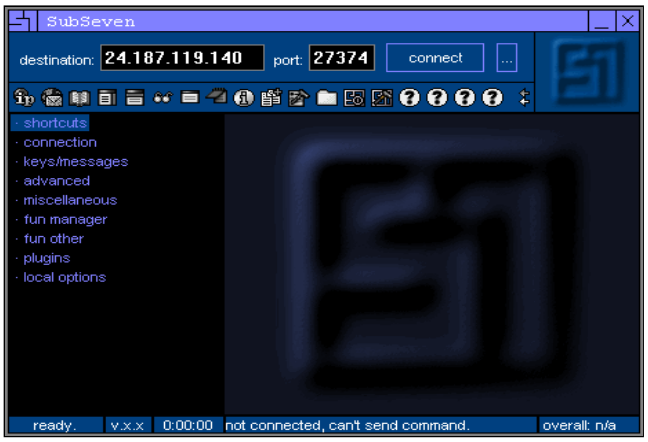
TROJANS & VIRUSES & WORMS

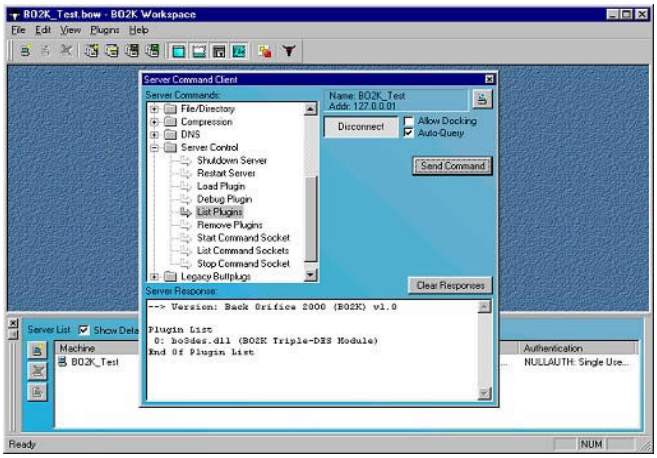
There are literally thousands of new trojans, viruses and worms created each and every month. In the past, where as malware-creation was done mostly out of curiosity, entertainment or in search of notoriety, today they are being driven by financial returns and profits. Previously, the greatest potential danger was the deletion of computer files. Nowadays, your money and confidential information is at risk.

The U.S. Federal Bureau of Investigation (FBI) estimates that computer crime costs American companies a staggering $62 billion a year—with computer viruses, worms or Trojan horses plaguing 84 percent of the 2,066 respondents to the agency's 2005 security survey. Microsoft has had over two billion downloads of its malicious software removal tool in the last year, which tells us something about the overall size of the malicious software problem.

Malware is becoming ever more dangerous and sophisticated. A new class of cyrpto-viruses such as Ransom.A.Trojan and Zippo.A, infects a computer and encrypt documents on the hard drive. These viruses then demands the user to send money via paypal or Western Union to a designated account in order to reveal the password needed to decrypt the files. These "ransomware" viruses usually demand a relatively small amount of money (From 10.99 to a few hundred dollars) in exchange for the password which increases the likelihood that the ransom will be paid.

New generation of rootkits are becoming increasingly difficult to detect. Microsoft Research labs created the first proof-of-concept prototype for virtual machine-based rootkits called SubVirt. VM Rootkits drops a virtual machine monitor underneath an operating system, which makes the rootkit virtually impossible to detect from the host operating system because its state cannot be accessed by security software running on the target system.





Powerful hacker tools such as Sub7 and BOK2 are easy for anyone to use with point-and-click graphical interfaces..

Today's malware propagation strategies are overwhelming and exploiting the weakness in the industry-standard, signature-based detection method of most anti-virus software.

The conventional signature-based approach, which involves maintaining a library of characteristics of each and every malicious attack, is fast falling behind. It is completely reactive. The speed of attack and propagation is such that patches simply cannot be issued quickly enough. In 2001, the infamous Code Red Worm was infecting a remarkable 2,000 new hosts each minute. Nick Weaver at UC Berkeley proposed the possibility of a "Flash Worm" which could spread across the Internet and infect all vulnerable servers in less than 15 minutes. A well engineered flash worm could spread worldwide in a matter of seconds.

Another method to bypass signature-detection methods is custom-designed trojans such as Trojan.Mdropper.B and Trojan.Riler.C that are being created to target a specific company or industry. On June 16, the United Kingdom's incident response team, the National Infrastructure Security Co-ordination Centre, warned that stealthy Trojan-horse attacks were targeting specific U.K. companies and government agencies.

"I think it would be very, very naive for any company to ignore these attacks. The lack of instances makes this more insidious, because it's likely that that no one is detecting the attacks. People may only notice it months later--by then, it is too late." said Mark Sunner, chief technology officer, MessageLabs.

SPAM

Bill Gates, the co-founder and chief software architect of Microsoft predicted the Death of Spam by 2006. Spam activity has increased 65% since January 2002 according to Postini. And as of April 2006 they report that 70% of all emails - or 10 out of 14 emails - are spam which includes unsolicited commercial advertisements, stock scams, adult content, financial hoaxes, etc.

Not surprisingly, spam is predicted to get much worse. At the 2006 European Institute for Computer Anti-Virus Research conference in Hamburg, John Aycock and Nathan Friess from the University of Calgary presented a paper on how spam can bypass even the best spam filters and trick experienced computer users who would normally delete suspicious email messages. The new technique relies on a new generation of spam zombies that monitor and mine email they find on infected machines, using this data to automatically forge and send improved, convincing spam to others. The next generation of spam could be sent from your friends' and colleagues' email addresses – and even mimic patterns that mark their messages as their own (such as common abbreviations, misspellings, capitalization, and personal signatures) – making you more likely to click on a Web link or open an attachment.

BOTNETS

When the U.S. Justice Department stepped up its investigation of cybercrime, it found spam originating from an unexpected source: hundreds of powerful computers at the Department of Defense and the U.S. Senate. The machines were "zombies" that had been compromised by hackers and integrated into bot networks that can be remotely controlled to send spam or launch distributed denial of service attacks. Botnets consisting of 100,000 and 200,000 nodes are not uncommon. There's even a case where a real botnet was found with about 1.5 million machines under one person's control.

According to data from PandaLabs, in 2005 more than 10,000 examples of bots were detected, representing an increase of more than 175 percent with respect to the previous year. Bots represented more than 20 percent of all malware detected in 2005. The number of variants of each bot could stretch into the thousands, a figure far too high for signature-based protection to cope with. For example, in the prolific Gaobot family, more than 6000 new variants were found in 2005 alone.

WEB APPLICATION VULNERABILITIES

Mercedes Benz, Fuji Film, Panasonic, US Navy, US Army, Greenpeace, Coldwell Banker, Microsoft, Google, Standford Electric, the National Oceanic & Atmospheric Administration, The SCO Group, the National Weather Service, Stanford University, SANS Institute, Symantec, Mcdonalds, Sandia National Laboratories, the U.S. Geological Survey, Bottom Line Technology, Association of Chief Police Officers, Midwest Express Airlines, the Space and Naval Warfare Systems Command, the Office of Secretary Defense, the Defense Logistics Agency, NASA Jet Propulsion Laboratories.... what do all these have in common? Their web site were recently defaced.

Zone-h.org keeps a digital archive of web site defacements, documenting hundreds of new defacements every day of corporations, organizations, and governments around the world. The majority of these compromises were compromised using an admin configuration mistake (19.4%) or a known vulnerability to which a patch is available (15.3%) or other programming errors. In other words - entirely avoidable. The same insecure programming methods and same programming mistakes are being used over and over - even in web applications developed by tech-savvy corporations such as Google, Yahoo, Hotmail, eBay, Etc.

- October 2005 - A vulnerability in Google's Gmail's authentication and session management discovered allowed a cybercriminal the ability to potentially take complete control of a victim's Gmail account without requiring any involvement of the victim.
- February 2006 - A Hotmail vulnerability allowed cross-site-scripting attacks.
- February 2006 - An Ebay vulnerability was being actively exploited.
- April 2006 - An vulnerability in Yahoo Mail was actively exploited for targeted phishing.
- April 2006 - Phishers were using a Ebay vulnerability discovered April 2006 to trick victims.
- April 2006 - A Myspace vulnerability allowed malicious scripts to be inserted anywhere on the site.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

A Distributed Denial Of Service attack is one in which a multitude of compromised systems flood a single target with data which drains computational resources, such as bandwidth, disk space, or CPU time, thereby causing denial of service for valid users of the targeted system. The attacking computer hosts are often zombie computers with broadband connections to the Internet that have been compromised by viruses or Trojan horse programs that allow the perpetrator to remotely control the machine and direct the attack. With enough such slave hosts, the services of even the largest and most well-connected websites can be denied.

Gaming sites, blogs, payment gateways, gambling sites, domain registrars advertising services, media organizations, large software companies, security vendors, security professionals and researchers, regularly face intimidation, extortion attempts and downtime caused by DDoS attacks. The extortion works by an attacker shutting down a site using a DDoS attack, and then follow-ups with an email saying, "Pay us or else we will shut down your site again."

"It's happening enough that it doesn't even raise an eyebrow anymore." says Ed Amoroso, chief information security officer at AT&T. Paying an extortionist a few thousand dollars to leave your network alone might make bottom-line business sense if the alternative is enduring a distributed denial-of-service attack that could cost your company millions in lost revenue and public relations damage. And many companies do pay.

"Six or seven thousand organizations are paying online extortion demands. The epidemic of cybercrime is growing. You don't hear much about it because it's extortion and people feel embarrassed to talk about it." said Alan Paller, director of research for security organization SANS. "Every online gambling site is paying extortion." Paller claimed.

ACTIVE-X

The security weaknesses of Active-X controls have long been known. Yet they are still highly popular. And its about to get worse. Research by Richard M. Smith, suggests that as much as 50 percent of all Windows computers might contain one or more flawed Active-X control that could allow remote compromises. Smith used a tool to checks for "buffer overflows" in common Active-X controls. Smith found dangerous security problems in Active-X controls distributed by dozens of other major companies, including PC manufacturers and even some of the nation's largest Internet service providers. In some cases, these insecure Active-X controls come pre-installed on Windows PC from the factory!

The Yankee Group is quite clear about their opinion on Active-X when they say "Retire Active-X—now."

PASSWORDS

One-factor authentications using passwords is still the most common form of authentication. New password cracking tools based on Faster Time-Memory Trade-Off Technique which uses pre-generated hash tables can crack complex passwords in a matter of days. While many employees and even executives are still using passwords such as "password" and "12345", a very respectable password (by today's standards) of "Aq42WBp" can be cracked easily using free, downloadable tools. Ophcrack can recover 99.9% of alphanumeric passwords in a Windows SAM database in SECONDS. Two-factor authentication would do a lot to improve user security (such as prevent some forms of phishing attacks) and the industry would benefit to see greater adoption, yet some of the most popular email sites such as Hotmail and Gmail don't support it leaving users with no option.

And while two-factor authentication does have benefits, Bruce Schneier is correct to state that, "Two-factor authentication isn't our savior." In response to the increased adoption of stronger authentication, cybercriminals are already proactively changing their tactics. Recent bank-stealing Trojans wait until the victim has actually logged in to their bank and then it just transfers the money out completely bypassing any authentication controls.

PATCH MANAGEMENT

Too often, software vendors are slow releasing patches to fix critical flaws in their products, leaving their customers exposed. Oracle, which likes to claim its software is "Unbreakable", took an astonishing 800 days to fix two flaws, and last year took more than 650 days to publish a fix for another security flaw. Perhaps a good indication of the poor state of information security; the day Oracle announced the Unbreakable campaign, David and Mark Litchfield discovered 24 holes in Oracle products.

Often critical patches released by Microsoft which are intended to protect their customers, instead causes system hangs and crashes.

The security company Scanit recently conducted a survey which tracked three web browsers (MSIE, Firefox, Opera) in 2004 and counted which days they were "known unsafe." Their definition of "known unsafe": a

remotely exploitable security vulnerability had been publicly announced and no patch was yet available. Microsoft Internet Explorer, which is the most popular browser in use today and installed by default on most Windows-based computers, was 98% unsafe. Astonishingly, there were only 7 days in 2004 without an unpatched publicly disclosed security hole. Read that last sentence again if you have to.

ZERO-DAYS

On Dec. 27, 2005 a Windows Metafile (.WMF) flaw was discovered affecting fully patched versions of XP and Windows 2003 Web Server. Simply by viewing an image on a web site or in an email or sent via instant messenger, code can be injected and run on the target computer. The vulnerability was in the Windows Graphics Rendering Engine which handles WMF files, so all programs such as Internet Explorer, Outlook and Windows Picture and Fax viewer which process this type of file were affected.

> *"There were only 7 days in 2004 without an unpatched publicly disclosed security hole." -- According to a survey by security company Scanit*

Within hours, hundred of sites start to take advantage of the vulnerability to distribute malware. Four days later, the first Internet messenger worm exploiting the .wmf vulnerability was found. Six days later, Panda Software discovers WMFMaker, an easy-to-use tool which allows anyone to easily create a malicious WMF file which exploits the vulnerability.

While it took mere hours for cybercriminals to take advantage of the vulnerability, it took Microsoft nine days to release an out-of-cycle patch to fix the vulnerability. For nine entire days the general public was left with no valid defenses.

The WMF Flaw was a security nightmare and a cybercriminal dream. It was a vulnerability which (a) affected the large majority of Windows computers (b) was easy to exploit as the victim simply had to view an image contained on a web site or in an email, and (c) was a true zero-day with no patch available for nine days. During those nine days, the majority of the general population had no idea how vulnerable they were.

Most disturbingly, the WMF vulnerability was auctioned off to the highest bidder, and reportedly was sold for $4,000 more than a month before Microsoft issued a patch and two weeks before virus hunters started noticing the potential flaw.

Yes, Zero-day exploits are now a reality. If you aren't scared yet about your online security, you should be.

WIRELESS ACCESS POINTS

Millions of wireless access points are spread across the US and the world. According to a FBI presentation at a 2005 Information Systems Security Association (ISSA) meeting in Los Angeles, about 70% percent of these access points are unprotected and left wide open to access by anyone near that location. The rest are protected by Wired Equivalent Privacy (WEP) defined as a security protocol in the IEEE 802.11 standard. Only a small portion are using the new, more secure, WPA standard.

The problem is that the WEP standard is completely broken. Today, easily accessible tools can crack a 128 bit WEP key in minutes. One reason for the low adoption of the new WPA standard is that product manufactures and computer stores continue to make and sell devices which only support the insecure WEP protocol. So even if the average consumer takes the unusual step of attempting to enable security protection, he/she is still left highly vulnerable.

INTERNAL ATTACKS

Internal attacks cost U.S. business $400 billion per year, according to a national fraud survey conducted by The Association of Certified Fraud Examiners, and of that, $348 billion can be tied directly to privileged users. And according to the 2005 Global Security Survey, internal attacks on information technology systems are surpassing external attacks at the world's largest financial institutions.

VULNERABILITIES IN SECURITY SOFTWARE

Rather than just focus on operating systems, cybercriminals are now also targeting and exploiting anti-virus and security software - the very security software that's supposed to protect PCs. According to a Yankee

Group research paper, in a 15-month period ending March 31 2005, 77 separate vulnerabilities have been discovered in products from security vendors Symantec, F-Secure and CheckPoint Software Technologies and others.

For example, in May 2004 a critical remote vulnerability affected almost the entire line of Symantec firewall product line (including versions of Symantec Norton Internet Security, Symantec Norton Personal Firewall,Symantec Client Firewall, and Symantec Norton AntiSpam) which allowed remote kernel access to the system - even with all ports filtered, and all intrusion rules set. In March 2004 the W32/Witty.worm damaged tens of thousands of computers by exploiting computer systems and appliances running security gateway software from network protection firm Internet Security Systems causing an unstable system and corrupted files.

MOBILE VIRUSES

We are discovering that no technology is immune from cybercriminals looking for ways to exploit it. Simply by using a cell phone, or personal digital assistant people can be a walking, talking security risk. There are currently dozens of viruses which target the popular Symbian phone operating system, however many of these are low-risk. While the problem is not yet widespread, it is only a matter of time before malware writers start to write more destructive mobile viruses. From a virus that will dial 1-900 numbers all day long, to the one that automatically buys a hundred ring tones that get added to your phone bill, there is money to be made and therefore there will be cybercriminals looking to exploit the technology.

THREATS EVERYWHERE - EVEN IN MUSIC CDS

Seemingly innocuous objects such as music CDs are now attack vectors which can leave you vulnerable. On Oct. 31, 2005 Mark Russinovich of Sysinternals discovered that Sony distributed a copy-protection DRM with music CDs that secretly installed a rootkit on computers. Once a CD is placed in the computer, the software tool is run without your knowledge or consent. The Sony code modifies Windows so you can't tell it's there - a process called cloaking which is a tactic usually used by virus writers - and It acts as spyware, surreptitiously sending information about you to Sony. And trying to remove it can damage Windows. Virus writers begin to take advantage of the Sony rootkit's cloaking features, making their viruses undetectable by anti-virus software.

Under intense pressure by the media, Sony created an uninstaller program. However, the uninstaller didn't remove the rootkit - it only removed the cloaking features. It was then discovered that the uninstaller had a vulnerability which allowed any web page you visit to download, install, and run any code it likes on your computer. More than half a million networks, including military and government sites run were infected. The rootkit has even been found on computers run by the US Department of Defense.

ENCRYPTION

There has been significant advances and cryptography research against security algorithms. In 1999, a group of cryptographers built a DES cracker, effectively killing off the Data Encryption Standard. It was able to perform 2^56 DES operations in 56 hours. The machine cost $250K to build, although duplicates could be made in the $50K-$75K range. A similar machine built today could perform 2^60 calculations in 56 hours, and 2^69 calculations in three and a quarter years. Or, a machine that cost $25M-$38M could do 2^69 calculations in the same 56 hours. In 2004 Eli Biham and Rafi Chen, of the Israeli Institute of Technology and separately Antoine Joux, announced some pretty impressive cryptographic results against MD5 and SHA. Collisions were also demonstrated in SHA. In February 2005, Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu from Shandong University in China showed that SHA-1 is not collision-free by developing an algorithm for finding collisions faster than brute force.

What does this mean for the average person? While these developments are big news for cryptographers, they present little real-world risks to the average user at the moment. However, what these developments make clear is that its time for a new standard.

Jon Callas, PGP's CTO, said it best: "It's time to walk, but not run, to the fire exits. You don't see smoke, but the fire alarms have gone off."

Come On In... The Water's Fine!

This is no doubt an information security pandemic occurring. We are passed rising temperatures and hot waters - the pot is boiling!

Yet, SANS's Internet Storm Center's Infocon Threat Level is rarely at any level other than a consistent Green; the lowest threat-level rating. While the pot is boiling, the Infocon Threat Level is telling us, "Everything is normal. No significant new threat known." Symantec's ThreatCon is most often at l, which is the lowest threat-level rating. Panda's Software Virusometer is usually at Green - "Normal".

	Description	Status	What is Means
SANS's Internet Storm Center's Infocon Threat Level (at time of writing, May 1st 2006.)	The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity.		"Everything is normal. No significant new threat known."
Symantec ThreatCon (at time of writing, May 1st 2006.)	"The Symantec ThreatCon rating is a measurement of the global threat exposure, delivered as part of Symantec DeepSight Threat Management System."		"This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted."
Panda Virusometer (at time of writing, May 1st 2006.)	"The Panda Virusometer measures the probability of users being affected by a virus at any given time."		"There are no signs of viruses or hoaxes that represent a threat. Low risk of being infected by a virus or malicious code, as long as the usual precautions are taken."

To steal a line from Arthur Dent in The Hitchhiker's Guide to the Galaxy: "Ah, this is obviously some strange use of the word "safe" that I wasn't previously aware of." It is as if many in the information security community are so used to zero-days, 100,000-node botnets, daily virus threats, spam-clogged email boxes, organized-crime-funded aware, massive identity thefts, etc, that they look at this situation and believe this is "normal." Business as usual.

This attitude is dangerous.

And it must change.

Why Are We Failing?

We operate in a hostile environment. Cyberspace's digital battlefield heavily favors the cyber criminal. A cyber-criminal only needs to identify a single vulnerability in a system's defenses in order to breach its security. However, information security professionals need to identify every single vulnerability and potential risk and come up

with suitable and practical fix or mitigation strategy. Furthermore, the freedom, privacy and anonymity cyberspace offers, gives cybercriminals the opportunity and confidence to target victims around the world with little chance of being caught.

Cybercrime no longer requires exceptional technical skills. This perfectly innocuous device is actually a hardware keyboard logger which silently and undetectably captures key strokes! They can be bought online for less than $100 US.

Cybercriminals are simply out innovating us. The technology and information security landscape is in a constant state of change and security is a digital arms race with both exploits and defenses continuously improving. While the cyber criminals have adapted and modified their attack and exploit techniques, the security community struggles to modify and adapt not simply their defenses, but their mind set.

For example, when Microsoft wanted to limit Windows Updates to registered copies of Windows, they developed their "Genuine Advantage" system. In less than 24 hours, the it was cracked. Sony spent millions developing a DRM technology called key2audio for their music CDs to prevent unauthorized music duplication, track ripping and piracy. Shortly after CDs with key2audio started hitting store shelves, it was discovered that the DRM technology could be defeated - by a $0.99 cent pen by simply scribbling around the rim of a CD! Tsutomu Matsumoto, a Japanese cryptographer, recently discovered that many advanced biometric fingerprint scanners used for authentication can be bypassed 4 out of 5 times using Gummi Bears and $10 worth of equipment!

Computer users attempting to sign up for an email account or blog are now faced with a mishmash of letters and numbers that they have to try to decode. This system is called CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) - the security community's answer to bot impersonating humans to register for computer services (such as free email accounts used to send spam) which is now in use on sites like Yahoo, Paypal, and Hotmail. However, computer software devoted to circumventing CAPTCHA is becoming so effective, sites have been forced to generate CAPTCHAS that are even difficult for humans to solve! And spammers have already engineered methods to bypass CAPTCHA. This system only serves to frustrate legitimate users and does little to hamper illegitimate bots.

Is this image a CAPTCHA or a digital representation of our failure? You decide. Chances are that computer software would have more success decoding this than a human!

Cybercrime is accessible to anyone. Whereas once one had to possess extraordinary computer skill to become a cybercriminal, today you don't need special skills or knowledge to become a successful cybercriminal. Exploits and detailed vulnerability information are available to anyone on the Internet. Point-and-click wizards, virus generators, and hacking tools dramatically reduce the skill level required to attack a target. For $15 to $20, hackers can buy a "Web Attacker Toolkit" from a Russian web site which sniffs for seven unpatched vulnerabilities in Internet Explorer and Firefox, then attacks the easiest-to-exploit weakness. The toolkit then places a trojan on the victims computer which can be used log keystrokes, download additional code, or open backdoors. You don't even have to participate - armies of coders are available to code custom spyware for money, or perform denial of service attacks for hire such as the one a CEO of a web-based satellite T.V. retailer ordered against his competitors which caused outages as long as two weeks at a time and $2 million in losses.

The "Biggest Bank Heist in History" did not involve technological geniuses breaking encryption algorithms and cracking firewall defenses. In fact, the heist was so simple only the most basic of technological skills were required. Thieves masquerading as cleaning staff installed hardware keystroke loggers on computers within the London branch of Sumitomo Mitsui. Hardware keystroke loggers are tiny devices which are physically installed on the back of a computer between the keyboard and CPU which silently and undetectably records every single key typed on the computer. They can be bought online for less than $100 US. They then

attempted to transfer more that $440 million to various accounts in other countries but the plan was foiled by the UK National High Tech Crime Unit.

The number of PC users is expected to hit or exceed 1 billion by 2010, up from around 660 million to 670 million today. As the internet expands, it increases the number of opportunities and potential targets of cybercriminals.

Security isn't accessible. Security is a full time job which requires hiring skillful and dedicated security professionals and purchasing a deluge of costly technology systems and devices. For example, purchasing anti-DDoS services to protect against the costly distributed denial-of-service attacks can cost around $12,000 per month from carriers such as AT&T and MCI, according to John Pescatore, Gartner security analyst.

Individuals and most companies simply do not have the time, money, skill and resources required to effectively manage all of today's risks and threats.

Complexity is the enemy of security. As technology becomes more powerful and advanced, the complexity often increases too which only serves to benefit cybercriminals. Today, simple office printers now come equipped with built-in services like Telnet and SMTP, SNMP, Bluetooth, etc. The security of an entire network can be compromised by a printer with a remotely exploitable vulnerability.

How can we fix this?

Solving the security absurdity is a daunting challenge and there is no simple, easy fix. It requires creativity, insight, persistence, adaptation, co-operation, action and support across the entire Internet industry and community. This document is not intended to contain all the answers. Instead it is written to raise awareness of the problem which too many people seem to not want to acknowledge. Through increased awareness can there be new dialogs and discussions on solutions. Because what is clearly missing is more dialog to come up with solutions to today's security challenges.

No one can deny the Internet's immeasurable benefits to our lives. This only heightens the need to confront and stop the overwhelming security threats. These threats are putting at risk the very benefit and value of the Internet. While the Internet opened up new means of communication and data sharing, security threats are closing doors and preventing opportunities. The pot is at a boiling point and action must be taken!

Part Two of this article will contain a list of what we must do to address our current failure. It will incorporate your comments and feedback.

What do you think? How can we stop the failure? Your comments are most welcome.

Comments

Thank to everyone who has written in with comments and questions.

Read the comments and post your own by clicking here..

This article is an opinion of the author(s) and does not necessarily represent the views or policy of their employers. All information and statistics contained in the article is correct to the best of the author(s) knowledge and has been linked to the original source where possible. If any information contained herein is inaccurate, kindly notify the author(s). Links contained in this article to external sources should not imply a relationship between this site and the external resource. Thank you for reading. Your comments and feedback is most appreciated.

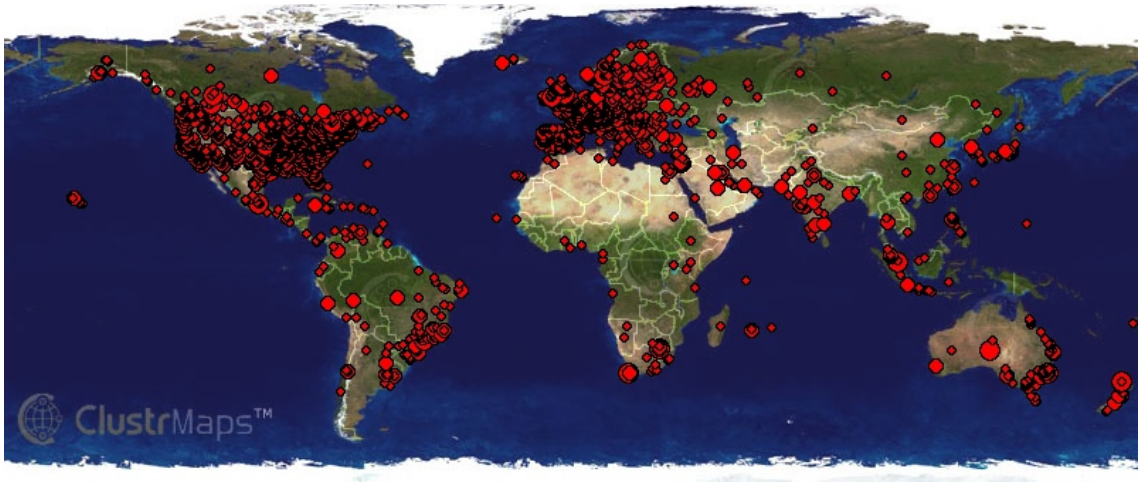
Community Comments & Feedback to Security Absurdity Article

by Noam Eppel
Vivica Information Security Inc.

Community Comments & Feedback

When I decided to write and publish Part One of my Security Absurdity article, I had no idea what the response would be. My largest concern was that the article would receive little or no attention. As the author of the article, let me state that I am genuinely interested in encouraging and promoting discussion on possible solutions to our current security challenges. The article was written to spark off dialogue, discussion and debate. Thankfully the article received quite a bit of attention and generated discussion on various sites, blogs and forums.

In a 24 hour period after the Security Absurdity article went online, it generated about 20,000 hits.



If one is going to write an article claiming a "total failure" of information security, one should expect some strong feedback. I was not sure what to expect - total disregard, complete agreement, outrage, or indifference. Thankfully, the majority of responses have been very positive. Whether or not you believe there has been a "total failure", there seems to be almost unanimous agreement that things are pretty bad out there, and the security community faces some significant challenges. It has been six months since my article was posted and sadly the security situation is only getting worse. The Cyberworld has progressed merely from the Wild West to the 1920s mob-controlled urban centers. Shortly after my Security Absurdity article was posted online, we witnessed a remarkable series of events when cybercriminals forced Blue Security, an innovative anti-spam security

company, out of business. This incident demonstrated quite dramatically that cybercriminals are indeed currently winning the battle.

The opinion that we are failing is not new or unique. I am not the first or only person to say security is failing:

- Financial Cryptographer Ian Grigg starts his April 2006 article in the Journal of Internet Banking and Commerce by saying, "It is slowly dawning on the world that Internet security isn't working."
- Jon Oltsik, Senior Analyst at Enterprise Strategy Group wrote a May 2006 article saying it's, "Time to face the truth about data security". He writes, "When it comes to confidential and private data security, the tired tech industry buzz phrase of 'people, process and technology' is truly in play. Each of the three areas is badly broken and in dire need of repair."
- Brent Huston wrote a September 2002 article for ITWorld titled, "Why Current Internet Security is Failing Us". In it he wrote, "Face it, the system is broken. Internet security is in a state of decline, and if present trends continue, it will be an abysmal failure within five years."
- David D. Clark of MIT In the Technology Review's December/January 2006 cover story, "The Internet Is Broken" where he claims the Internet's lack of security has decreased the ability to accommodate new technologies. And he delivers a strikingly pessimistic assessment of where the Internet will end up without dramatic intervention. "We might just be at the point where the utility of the Internet stalls -- and perhaps turns downward".
- Ken Birman of Cornell University wrote an article for the IEEE computer society in February 2006 where he said we are experiencing a, "profound failure in the area of security." And Birman says that, "For all the hype about more secure versions of the major platforms and popular products, and the heavy investment in safeguarding the Internet, security has been a catastrophe.
- Bruce Schneier, founder and Chief Technology Officer at Counterpane Internet Security Inc, commented on my article saying, "It sounds like something I would write." In fact, Schneier has been claiming security has been failing us for years such as when he told the US Senate's Subcommittee on Science, Technology and Space that, "Every year, the problem gets worse. Security is failing us." At this year's Hack in the Box Security Conference (HITB) in Kuala Lumpur, Malaysia, Schneier repeated the message saying, "I don't think, on the whole, we are winning the security war; I think we are losing it."
- Professor Eugene H. Spaffords, who is one of the most senior and recognized leaders in the field of computing, stated during the keynote address at the recent AusCERT 2006 conference that, "Trends over the last 10 years indicate nothing related to overall information security is getting better."
- Marcus Ranum has long spoken about our security failures. During a June 2005 interview he stated, "I believe we're making zero progress in computer security, and have been making zero progress for quite some time."
- Bruce Sterling claims in an article for PCWorld that, "the Internet is now in a golden age of criminal invention" and that, "the Internet's running amok. We're in a dark period for law and order."

- Richard Forno, consultant for KRvW Associates argues that we are failing to acknowledge or fix an infrastructure plagued with problems and instead we are simply placing more complexity on top of existing (and flawed) complexity, in his article titled, "Why Internet security continues to fail".

- Abe Kleinfeld, CEO of nCircle wrote in a May 2004 article, "For many reasons, network security is failing and corporations need to undergo a fundamental shift in how they approach security..."

- Tim Wilson, Site Editor of the Dark Reading Security site says that despite various government initiatives and organizations attempting to fight cybercrime, "computer criminals are winning the war. Phishing, spam, and identity theft are at all-time highs. There are more than enough gaps in our defenses to be exploited, and there are enough loopholes in the laws to make these vulnerabilities attractive lines of business for both casual hackers and organized crime."

- Eugene Kaspersky stated, "We're losing this game with computer criminals. There are just too many criminals active on the Internet underground, in China, in Latin America, right here in Russia. We have to work all day and all night just to keep up."

- Dan Hubbard, vice president of security research at Websense recently stated in a talk at Defcon 2006 that, "We are getting our butts kicked, there is no doubt about it".

I am not even the first to write about our tolerance of the current situation (a.k.a. the Boiling Frog Syndrome). Mark Burnett wrote in a column at SecurityFocus.com in June of last year that, "We have been well conditioned to recognize and delete the endless stream of spam, phishing attempts, Nigerian scams, and virus attacks we get every day in our inboxes. We have been so far behind for so long in the battle with computer security that we have almost forgotten some of the most basic insecurities that we put up with day after day." David D. Clark also observed that sometimes the worst disasters are caused not by sudden events but by slow, incremental processes -- and that humans are good at ignoring problems. "Things get worse slowly. People adjust. The problem is assigning the correct degree of fear to distant elephants." Today Clark believes the elephants are upon us.

David D. Clark also stated that, "We are at an inflection point, a revolution point." I hope so too. And I hope this Security Absurdity article has helped to fuel this revolution. There are significant challenges ahead but with the right discussions, solutions can be found.

I want to highlight some of the comments that the article generated - the Good, the Bad and the Ugly.

The Good

Professor Eugene H. Spafford, Center for Education and Research in Information Assurance and Security (CERIAS):

> *"This is a great blog posting: Security Absurdity: The Complete, Unquestionable, And Total Failure of Information Security. The data and links are comprehensive, and the message is right on. There is a tone of rant to the message, but it is justified. I was thinking of writing something like this, but Noam has done it first, and maybe more completely in some areas than I would have."*

Marcus Ranum:

> *"Apparently I'm not the only person who feels that computer security has been accomplishing relatively little, in return for a large amount of money expended. ... Eppel's completely right about every one of the points he raises, and I highly recommend his article."*

Jon R. Kibler, CTO Advanced Systems Engineering Technology, Inc:

> *"This is probably the best article that I have read recently about the state of information security. It mirrors my thinking on the subject. And, deservedly, it isn't too kind to us security pros either. A great wakeup call (as if we really needed one)."*

Martin McKeay, ComputerWorld:

> *"I've been arguing that we're losing the battle against hackers for a while, but Noam Eppel argues that we, the security community, have already suffered a 'complete, unquestionable and total failure of information security'. While I don't agree with the severity of the judgement that Noam puts forth in the article, I do agree that we are losing ground and are one major vulnerability away from an Internet meltdown."*

Dan Morrill, Senior Security Engineer:

> *"I think he is right, I have been involved in information security for 18 years, and it is the right job for me, it suits my personality and beliefs quite well, and I find it overall very exciting to be in this industry. I believe that there are things seriously wrong with the current state of affairs in information security, but I also believe that they are addressable, and in many ways fixable. Noam does a good job of laying out the fundamentals of the issue, that even for all of our vaunted systems and programs and technologies companies are still getting hammered by the hackers and criminals..."*

Rick Wanner, Corporate Security at SaskTel:

> *"I'd like to point you to an article by Noam Eppel and the subsequent followup by Marcus Ranum. Both of these people are not unknown in the security community, and I would have to believe that Marcus is probably as close to a household name as there is in this industry. I'd like to disagree with them, but unfortunately their is a lot of truth in what they say. The security vendors make and so called security professionals keep deploying technology that is ill-conceived, flawed, and overly complex. Why? To attempt to satisfy protecting application technologies that are ill-conceived, flawed, and overly complex. The solution is not easy, but as long as this arms race continues, the attackers will continue to hold the upper hand."*

Financial Cryptographer Ian Grigg:

> *"Mark points to Noam Eppel. If you haven't subscribed to the "total collapse of security and humanity as we know it" theory, then I'd encourage you to read "Security Absurdity: The Complete, Unquestionable, And Total Failure of Information Security." Even just skimming the list of headline failures will help :) [...] You may not agree with the central claim, but at least the article clearly lays out the evidence, from top to bottom. It is*

> *important to understand the claim and its foundations, even if you don't agree, because much of the new work that is being done is based on the complete replacement of large chunks of old wisdom. This only makes sense if we can claim that the old ways were wrong."*

Kenneth Searl, Prodigen:

> *"Noam's article is right on. I believe a significant part of the issue with regard to security is the lack of acceptance of innovative products by the security professionals. Best Practices have not worked as Noam is suggesting. In 2002 I was new to the security space and looked at security as an outsider. As Noam states on insider threats, traditional perimeter solutions just don't work. There are better ways of looking at security and I'm sure there are many creative innovations in other areas, but until the security professional can take the chance on a solution beyond "Best Practices" The bad guys will continue to win. Walls just don't work!"*

Chris Kendall:

> *"I have to agree with what he's saying about this. I work for a major web hosting company and though we are very secure security wise we are on a daily basis getting DOS attacks. No matter what we do we are constantly under attack and unfortunally there isn't enough information on how to stop it. As individual's in various computer related field's I feel it is essential that we all need to figure out how to be ahead of the game instead of behind like it is now. Otherwise we'll never get out of this loop we're in."*

Jimi Loo:

> *"This is probably the single most compelling article I have read on the topic/issue. Well done. I personally like to think of the Internet as a parallel universe, a cyber-world as opposed to the real-world. In cyber-world people do thing much the same as in the real-world, such as chat, work or go shopping. And as in the real-world, there are dangers. In the real-world we spend years as children learning about this world and all its dangers before we can safely go out on our own. This is not the case in cyber-world. People wonder into cyber-world as cyber-toddlers or even cyber-infants. How can these people are expected to look after themselves in this strange new world? I know I'm reiterating some other people's comments, but I believe education must be the first step to computer security. Cyber-world is too complex and dangerous to jump into without understanding the dangers."*

Rob Lewis:

> *"I liked your article; it was readable and you said things that need to be said, even though they are perceived differently by different people. I know you got push back. Ranum did for his "6 dumbest mistakes in computer security" piece as well. Entrenched vested interest groups always get defensive with change because they like to protect their learning investment and revenue stream. How do you think the whole industry would handle it if a new model of IT security arrived on the scene that made status quo technologies obsolete? Are they going to be happy? Not likely."*

Phil Becker, ZDNet:

> *"A big clue to why current security approaches were doomed from the start is found in the sports cliche that no game is ever won by defense alone. The best a perfect defense can accomplish is a 0-0 tie, and eventually this will break down under sustained pressure from the other side. Slowly this is dawning on the security industry.... So how can security *win* its game of protecting networked computing and those who use it from threats that will never cease? To win, a way must be found to go on the offense, not just respond to each new symptom as it pops up. When the strategy used to protect things is shown a failure, winning requires changing the rules of the game...."*

Wes Kussmaul, Chief Instigation Officer, The Village Group:

> *"..The fact is that the foundations of both our operating systems and the internet were built from naive assumptions that must be revisited. In doing so, the means of establishing authenticity must be imported from centuries old processes of establishing authoritative certification. These processes have very little to do with technology. The irony of the term "certification authority" says it all. It refers to a piece of technology, with zero genuine authority, yet we trust it to put the lock icon on our browsers. No wonder we're hosed. We went on the assumption that authenticity could come from technology. Would you occupy a building whose plans were signed by xyz.com, attested to by Gopapa.com certification authority? Me, I'd rather see a structural engineer's professional license on the line, with the occupancy permit signed by city hall."*

Rlmarchant:

> *"Very entertaining and enjoyable paper... I think, however, from a universal user (e.g. the home user) perspective, security and security tools need a witch doctor more than a security professional. The ritual and dogma surounding security tools, the advertisements filled with bovine fecal matter, and the layer upon layer of redundant firewalls, scanners, filters, detectors, alert mechanisms.....ad nauseum leave users realing from security tools shock. We as security professionals need to stop trying to come up with tools and techniques that protect the end user without their involvement and spend a little time trying to understand exactly what this user is capable of understanding. Then provide tools that match that capability. I believe most users ignore or improperly configure security mechanisms out of contempt or dismay, not lack of ability. Our failure (as professionals) is in failing to understand the users capability and matching our user interface to that level of understanding."*

Tim:

> *"Scale is the reason the problem is so bad. Scale is an inherent feature of the Internet: millions of (flawed) applications, millions of potential victims, millions of potential attackers - all of which can interact with full capability from distant locations. The effect is that a security flaw in an application is not at all like a safety flaw in a power tool; it's likely that only one hand is lost at a time in that faulty table saw, but a typical security flaw allows the attacker to exploit millions of people at nearly the same cost as exploiting just one."*

P Scotty:

> *"When we needed to get goods to the West Coast of the US, the railroads expanded. When we needed to expand our markets to the mideast using the expansion of democracy to do so, we built the Great White Fleet. When Europe ran out of places to sell their trinkets, they went to China and sailed the Atlantic ocean. The innovations of tanks, nuclear weapons, jet aircraft and other tools of 'security' were driven by the mass disruptions of economic freedoms. Economy drives innovation. Nothing else."*

NoticeBored:

> *"The first part of your article is already part of the solution - it's an excellent summary of current information security risks. The sheer breadth of issues we face is an eye-opener, and that to me is the first step towards finding a workable solution. People who don't appreciate the risks are unlikely to even address them, let alone solve them."*

NRH, StupidSecurity.com

> *"If you want to scare the Hell out of a pointy-haired boss, make him run to a tropical island retreat and cut off contact with the rest of the world, this would be the url to hand him!"*

The Bad

1) Using The FUD Card...

There was a lot of good criticism of the article. The most common complaint was that the article was spreading FUD - "Fear, Uncertainty and Doubt." The term originated to describe misinformation tactics in the computer hardware industry to appeal to customer's fear in order to prevent them from switching to competitors' equipment. The term is now used more broadly to describe any scare tactics designed to sell a product or point.

FUD is simply complaining about problems - without any care for actually finding solutions or improving the problem. Many people seemed to miss that fact that only Part One of the article has been posted. I wrote in the article that, "Part Two of this article will contain a list of what we must do to address our current failure. " And that, "It will incorporate your comments and feedback." As the author of the article, let me state that I am genuinely interested in encouraging and promoting discussion on possible solutions to our current security challenges. Encouraging and promoting discussion can only be called productive and not FUD.

Unfortunately, labeling something FUD has now become a FUD tactic itself with the sole purpose of preventing further discussion.

2) But It's Not My Fault!

The second most common complaint relates to where the blame lies. Most people agree that things are pretty bad at the moment, yet many argue that Security Professionals can't be blamed because *other* causes are at fault such as ignorant users, vendors that write insecure software, insufficient laws to prosecute cybercriminals, and various other factors.

"Security Professional" wrote:

> *"Great article. However, I think you need to be careful on whom you place the blame. The article at first glance faults on the thousands of security professionals whose job it is to stem the tide of vulnerabilities and threats. However, these professionals are not the ones writing the swiss cheese software. The fact of the matter is that if applications and operating systems were designed securely form the start, then the majority of these issues wouldn't exist."*

Marcus Ranum previously commented on this blame game:

> *"Whenever security people look at the state of the industry, they invariably seem to latch on one of the potential blame-targets above, and they assume that, if only we could apply sufficient pressure on one key aspect of the problem, it would all be OK. This is what I call "a circular dependency of lameness" - at each point in the broken process, it's so easy to think "if I just fix it really well here it'll all be OK." But it won't."*

There were a number of people who responded to the article who were in complete agreement that we are currently witnessing a dramatic security failure, but were greatly opposed to the idea that security professionals were to blame. They were quick to blame Microsoft, software developers, or ignorant users. Let me ask then, who then is best able to correct the current failures? Who can drive the fundamental changes required to improve the security landscape? Techno-illiterate politicians and law makers who have zero security experience? Police agencies that lack the resources and expertise required to fight cybercrime? Software vendors who are rewarded for meeting deadlines, not writing secure software? Managers? Teachers? Parents? Consumers? Media?

Security Professionals are in the best position to create change and that is why we are responsible for this situation. If we lack certain laws then it is Security Professionals that can help politicians understand this and advocate for better laws. If software vendors are producing insecure products then it is Security Professionals that can assist (or pressure) them to improve their coding practices. If Universities lack security courses then it is Security Professionals that can raise awareness and promote security education at Universities.

Let's say the local police department has been given a report which shows a large crime increase over the previous year. Imagine them claiming it's not their responsibility - "The media is to blame!", "It's the fault of video game developers!", "Bad parenting and bad teachers are the cause!".

These factors may play a large part in the crime increase. However, it's not the duty of police to prevent crime ONLY if there are no bad parents, teachers or video games. Its the police's duty to prevent crime DESPITE these factors. Its unproductive to simply avoid the blame. Its more productive to recognize the problem and find solutions.

I think the security community needs to redefine their definition of success. And I think they need to understand the unique position they are in to improve security and to accept that responsibility.

The truth is, there is enough blame for everyone: end users, software vendors, managers, Microsoft, hackers, etc. But you can either play the blame game or you can actively work to improve the situation.

For example, if police currently don't have the tools, resources, skills or knowledge to fight cybercriminals then the security community and technology industry need to step up and fill in the gaps. Toronto Police Detective Sergeant Paul Gillespie was overcome with the flood of internet child abuse and emailed a plea for help to Microsoft chairman and Chief Software Architect Bill Gates. Gates read the email and tasked Microsoft Canada to work closely with the Toronto Police in developing a solution. The result is that today police have free access to Child Exploitation Tracking System (CETS), a powerful internet investigative software without equal in the world which is being used by twenty-five police forces across Canada.

The nCirlce blog has some entertaining comments on the need to take responsibility for those that blame "swiss cheese software":

> *"You can't blame the butcher for selling what people are buying. You aren't doing anything to change the world and make it a better place by yelling "Oh poor me! The vendors make crap! They're so evil - damn them!". Well guess what - YOU, THE HORDES OF COMPLAINERS, are the ones to blame. Until we learn to suffer and do without, rather than buy the crap for sale, the situation is not gonna change. Until you learn that some stuff you should do yourself rather than fork out cash, it's not gonna change. Here's one area where Open Source shines. Until you vote with your feet and your dollars, THINGS ARE NOT GONNA CHANGE. Take responsibility for yourself."*

3) Best Practices Will Solve All!

The third most common complaint was that if Best Practices were followed, none of the failures in the article would have happened.

Ben Ricker commented:

> *"There seems to be a bit of a non-sequitor going on here: you go through a laundry list of new technologies to protect data and implement security, then say "But look at all the break-ins!" You seem to be arguing that all these new technologies are not protecting us. Logically, however, the question is: are the companies USING these technologies and out of those, how many of them are still getting popped? You are mixing up the classes of everyone and everyone WHO FOLLOWS GOOD SECURITY PRACTICES. In the laundry lists of incidents, I know that a couple of them were within areas that had poor security practices. They were NOT using all these new technologies in the right manner."*

Jack Jones, who won the, "Excellence in the Field of Security Practices" award this year at the RSA conference, wrote a paper titled, "An Introduction to Factor Analysis of Information Risk (FAIR)". He writes, "...while we would like to believe that Best Practices are generally effective (as we tend to reuse what has been successful in the past), this may be a dangerous assumption. Best Practices are often based on long-held shamanistic solutions, tend to be one-size-fits-all, may evolve more slowly than the conditions in which they're used, and can too often be used as a crutch - e.g., "I can't explain why, so I'll just point to the fact that everyone else is doing it this way."

For example, how often have you heard Security Professionals advise that users should change their passwords every few months? This "best-practice" is based on recommendations made 30 years ago regarding non-networked mainframes in a DoD environment! It is completely outdated by today's technology and changing passwords every few months has minimal impact on improving security.

Some security professionals claim that if people just follow the acceptable computer behavior then they will remain safe. However, the problem is that the security community has set a tight, strict and constantly changing limit as to what is now acceptable computer behavior. Here are some actual security recommendations and advice which the security community expects the average user to follow:

- Don't click on links in email messages. Type the URL in your browser manually.
- Disable the preview pane in all your inboxes.
- Read all email in plain text.
- Don't open email attachments.
- Don't use Java, JavaScript, and ActiveX.
- Don't check your email with Microsoft Outlook or Outlook Express.
- Don't display your email address on your web site.
- Don't follow links in web pages, email messages, or newsgroup without knowing what they link to.
- Don't let the computer save your passwords.
- Don't trust the "From" line in email messages.
- Never Use Internet Explorer and instead Switch to Firefox.
- Never run a program unless you know it to be authored by a person or company that you trust.
- Read the User Agreement thoroughly on all software you download to ensure it is not spyware.
- Don't count on your email system to block all worms and viruses.
- Get a Mac

And in the event a computer user gets hit by any of the myriad of threats or has their privacy or confidential information compromised, we say to them, "Oops, you should have followed the latest Best Practices!". In order for Best Practices to be relevant, they need to be attainable, practical, implementable and manageable. Today's security Best Practices are counterintuitive, difficult to implement, quickly outdated by new threats, and are constantly changing.

Augusto Paes de Barros, CISSP-ISSAP, MCSE, CCSE, CCSA commented:

> *"I have a friend that is a penetration test specialist. His approach gives him almost 100% success rate, even in companies that have advanced security programs. What is happening is that the main sources of information for the CSO, with their indications about most common threats, don't drive to solutions that could stop my friend's approach. The "by the book" CSO will be a easy prey for him. I believe that we need a deeper technical discussion about what we understand as "Best Practices", making them more effective and clear."*

Security is a process to be evaluated on a constant basis. There is nothing that will put you into a "state of security" - no best practice, no security guideline, no security checklist.

4) Damn, Lying Statistics

Unfortunately, statistics in information security can be unreliable due to various reasons. Cybercriminals conceal their successful attacks. Companies often do not reveal their security breaches or report them to the authorities. Security vendors can often exaggerate the risk in order to promote their own products. These factors make understanding and measuring the state of security (or insecurity) difficult. We have not yet developed commonly accepted analysis frameworks or methodologies to measure, analyze and understand trends or to critically examine our own performance.

The security industry is occupationally immature - a point Robert W. Beggs of DigitalDefence.ca made in his response to my article:

> *"The information security community is occupationally immature - as a group, we have not yet been able to develop cohesive common security practices, we are not sharing security duties very well, and we have not yet advanced to the point of having predictable plans that can be followed by all members of an organization. Instead, security professionals are still in a highly reactive mode. Our focus is, on tactical responses ("putting out the fires"), and we will not be able to ponder why there are fires in the first place until we can develop a common framework for analysis."*

Evaluating the methodology of the studies and surveys was obviously beyond the scope of the article, however, the reason I provided links to the original sources is exactly so people can evaluate them on their own. Certainly, while statistics can be debated, judging by the majority of the comments and discussions around the article, people agree that things are in pretty bad shape and there is no doubt that the security industry is facing a number of significant challenges.

No individual contributed more to the debate then Robert Beggs of Digital Defence and I applaud his effort. In his follow-up paper to my article Beggs writes:

> *"This paper is not an attack on Noam Eppel's Security Absurdity paper; I think that I speak for many in our profession when I state that there is a feeling that things could be "done better" to create a more secure environment for our information. I disagree with several of the points made by Noam, as I am certain he will disagree with many of mine. This is not only to be expected, but the clash of ideas is the goal - I take a "Hegellian approach" to the subject of security.... My analysis of Noam's paper basically see a very worthwhile thesis (security is failing) that is hindered by the lack of support that is required to produce a strategic direction... Noam has already achieved success by getting the community to talk, share ideas, and focus on how to make itself better. My goal is to help Noam push the Security Absurdity paper to the next level, and support the analysis that will achieve strategic success, not just small tactical victories."*

In Beggs' "antithesis", rather than explaining how we are winning by showing that cybersecurity is not failing but indeed getting safer, Beggs attempts to discredit the theory by discrediting the statistics presented in the article. There is a fallacy to this in that people don't need to rely on statistics to be convinced that security is failing; they experience it daily as they try to navigate through dozens of spam messages and phishing emails, as they struggle to regain control of their computers from spyware, or as they attempt to eradicate worms that are constantly bombarding their computers. Statistics are not required to make the argument that security is failing - you simply have to talk to any home user or system administrator struggling to keep their systems protected against daily threats.

Chris Kendall wrote:

> *"I have to agree with what [Noam's] saying about this. I work for a major web hosting company and though we are very secure security wise we are on a daily basis getting DOS attacks. No matter what we do we are constantly under attack and unfortunately there isn't enough information on how to stop it. As individual's in various computer related field's I feel it is essential that we all need to figure out how to be ahead of the game instead of behind like it is now. Otherwise we'll never get out of this loop we're in."*

People like Chris Kendall do not need to rely on any statistic to believe security is failing - they experience the effects of that failure daily!

However, even after Rob Beggs' analysis, it seems the statistics do hold up pretty well. Here are some example of statistics which Beggs believes are false:

1) *Beggs questions if nearly nine out of 10 organizations really did experience a computer security incident in a year's time:*

> *"Noam makes the statement that "nearly nine out of 10 US businesses suffered from a computer virus, spyware, or other online attack in 2004 or 2005". The author attributes this statement to the 2005 FBI/CSI study. This statement is simply not true. In fact, the closest that the survey comes to such a claim is the statement that: The percentage of respondents answering that their organization experienced unauthorized use of computer systems in the last 12 months increased slightly from 53 percent last year to 56 percent this year."*

The FBI released two major cybercrime reports in 2005, the CSI/FBI Computer Crime and Security Survey and the larger, more comprehensive 2005 FBI Computer Crime Survey. I attributed the statistic to the CSI/FBI survey instead of the FBI survey. The link was wrong but the statistic is true; we can go straight to the source to the FBI web site at <http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm> where they state that, "Nearly nine out of 10 organizations experienced computer security incidents in a year's time".

2) Beggs questions the claim that billion of dollars are being lost due to security threats:

> *"..where are the billions of dollars being lost due to inadequate security? DigitalDefence does not doubt that security fears are having a negative impact; however, we would like to see rational analysis supporting Noam's argument, rather than sensationalist claims that are not supported by the cited reference."*

In the article, I wrote that, "Billions of dollars of ecommerce opportunities are being lost due to inadequate security." This statement was linked to a Gartner study which reported that people were using online banking less due to security concerns. This study did NOT show that billions of dollars were being lost due to inadequate security. The link was the exact same link I used later on when discussing the Gartner survey. I had simply used the wrong link for that reference.

Beggs is correct in finding that the sentence does not link to a reference which supports that claim, however, I am not sure why Beggs takes issue with the claim that billions are being lost. Further on in the article there are many referenced statistics which show that billions of dollars are being lost, and furthermore, a quick search on Google would have revealed many more sources to support the claim:

- Thomas Noonan, chairman and CEO of security firm Internet Security Systems stated at a 2006 RSA Security conference that, "financial losses are estimated at nearly $50 billion dollars a year by corporations and businesses grappling with security. And it's growing at a rate of three times the investment."

- According to the 2005 FBI Computer Crime Survey, cybercrime robs U.S. businesses of $67.2 billion a year. The 2005 FBI Computer Crime Survey is the largest survey on these issues to date according to the FBI. The survey was developed and analyzed with the help of leading public and

private authorities on cyber security and is based on responses from a cross-section of more than 2,000 public and private organizations in four states.

- According to research carried out by Computer Economics, total losses in 2004 from virus writers, hackers and spammers were close to $18 billion, with a trend towards a 30 - 40% annual growth rate.

- The Federal Trade Commission (FTC) says that during a one-year period, nearly 10 million people had discovered that they were victims of identity theft. Estimated losses translated into $48 billion for businesses and $5 billion to consumers.

- A report by Ferris Research, "The Global Economic Impact of Spam" says that lost productivity and other expenses associated with spam cost U.S. businesses $17 billion in 2005. They estimated that worldwide costs could be as high as $50 billion.

- According to a Gartner survey, in 2006 alone retailers lost almost $2 billion because of consumer security fears, with about one-half of those losses ($913 million) coming from people who avoided sites that seemed to be less secure and the rest (about $1 billion) came from consumers who were too afraid to conduct e-commerce business at all.

3) Beggs questions the claim that 91 percent of computers in a study really did have spyware:

> *"Other citations that 'feel' believable are soon proved wrong when the source is evaluated. For example: "According to the National Cyber Security Alliance a staggering 91 percent in the study have spyware on their computers". Actually, if you read page 6 of the cited report, only 61% were of the study were found to have spyware after a scan of their system was completed."*

That statistic was taken directly from Ken Watson, who is chairman of the National Cyber Security Alliance - the organization which conducted the survey. Watson stated that, "About 91 percent of PCs today are infected with spyware programs that send information from your PC to an unauthorized third party". Cindy Bates, General Manager of the Microsoft U.S. Small Business Group, stated the exact same figure.

Other survey's have produced similar results, such as the CNET Networks/Trend Micro nationwide survey of spyware and its impact on U.S. corporations, which found that 93 percent of companies have seen an increase in the amount of spyware on their networks in the past three months and 95 percent of companies report that adware is frequently found within their organization. The latest 2005 National Spyware Study, prepared by The Ponemon Institute, found that 84 percent of respondents report that they have been spyware victims. The most recent Webroot Software State of Spyware Report claim that 89 percent of consumer PCs are infected with spyware.

To argue that we are not failing is to show that we are indeed winning the battle and that the overall state of security for corporations and individuals is improving. It is not to simply point out that statistics on cybersecurity can be unreliable.

However, where I disagree most with Beggs is where he takes issue with my statement that, "it is our mandate, first and foremost, to protect." He writes:

> *"Rubbish! The hypertext reference is to the SANS IT Code of Ethics, published in 2004. I had to look it up, because I've never seen this Code, nor have I ever subscribed to it. In fact, I have not met any others who particularly endorsed this series of statements either,*

> *so it is unfair to ascribe this Code of Ethics to the industry as a whole. After reviewing the Code, I determined that the first mandate is NOT to protect - it is to "strive for technical excellence in the IT profession by maintaining and enhancing my own knowledge and skills". In fact, the word "protect" is not used at all in this general Code of Ethics - the closest we come to Mr. Eppel's meaning is the 11th mandate: I will report on the illegal activities of myself and others without respect to the punishments involved. I will not tolerate those who lie, steal, or cheat as a means of success in IT".*

SANS is the largest source for information security training and certification in the world. Beggs is correct that there is no single, unifying Code for the entire security industry. I linked to SANS's IT Code of Ethics as one example. However, while Beggs does not like SANS voluntary code of ethics since "he has never subscribed to it", perhaps I should of linked to the mandatory (ISC)2 Code of Ethics which all CISSP applicants must subscribe to. The very first Code of the Ethics Canon is to, "Protect society, the commonwealth, and the infrastructure."

My point was that security professional must look beyond the limited scope of what must be done to protect ourselves, our careers, our networks, our employers, and start to look to protect our society. (More on this topic later).

The Ugly

I believe a number of people reacted to the article with shock and complete disagreement to the very suggestion that information security could be failing, but were completely unable to provide any arguments to show how we are not.

Thomas Ptacek at Matasano seems utterly convinced that security is NOT failing, but utterly unable to explain why I am wrong. Instead he humorously accuses me of "eating bugs" and completely misrepresents what I wrote and the statistics in my article. For example, he claims that I believe, "Phishing would be solved if banks just required SSL at login." Nowhere in my article did I say that. What I did say was that banks not using SSL, "makes it more easy" for a phishing attacker to intercept and spoof a financial web site.

He also claims I believe that, "Anti-Spyware is a total failure because a report from 2004 said Giant missed 34 registry settings." What I actually said is, "Eric Howes, a renowned security researcher at the University of Illinois at Urbana-Champaign, found that many of the best-performing anti-spyware scanners 'fail miserably' when it comes to removing spyware from infected computers, with some missing up to 25% percent of the critical files and registry entries installed by the malicious programs."

In fact, Howes rated the Giant AntiSpyware product as the BEST of the twenty scanners tested - even though it missed numerous critical files and registry entries. I am not sure why Ptacek appears to have ignored the entire anti-spyware test - and more importantly Howes' conclusions - and instead focus on the one anti-spyware product which performed the best of the 20 products tested.

While Ptacek is evidently okay with anti-spyware products leaving malware on a PC, Mike Danseglio, Microsoft Program Manager in the Security Solutions group recently concluded that anti-spyware products are mostly useless when attempting to clean up malware, and that recovery from malware is becoming impossible:

> *"When you are dealing with rootkits and some advanced spyware programs, the only solution is to rebuild from scratch. In some cases, there really is no way to recover without nuking the systems from orbit... We've seen the self-healing malware that actually detects that you're trying to get rid of it. You remove it, and the next time you look in that directory, it's sitting there. It can simply reinstall itself," Danseglio said. He conceded that the cleanup process is "just way too hard." "Detection is difficult, and remediation is often impossible."*

Ptacek seems completely shocked that I would claim that insider attacks cost U.S. Businesses $400 billion per year. As mentioned in my article, that figure is taken directly from a national fraud survey conducted by The Association of Certified Fraud Examiners. The actual report can be found here which states, "Fraud and abuse costs U.S. organizations more than $400 billion annually." My article links to a CSO Online article which repeats the same statistic when they say, "Internal attacks cost U.S. business $400 billion per year".

However, I don't think anyone was able to so accurately illustrate the boiling frog syndrome as Russ Cooper, who writes:

> *"According to the author of this article, our attempts at securing the Internet have totally failed and every idea we have to do better is worthless. Anyone remember that we recently stated that using PHP on a public Web site, particularly one that allows users to post their own commentary, is a scary proposition? Here we have a security professional decrying the failure of our own business, while ignoring the risks himself. Mr. Eppel's lengthy description of how every form of eBusiness is going to fail by the end of 2006 is nothing short of amazing FUD. From his perspective, nothing works, nor will work, in terms of computer security. Unfortunately many of the "facts" he cites are out and out wrong, and others are spun to drive his theory. If there's much to be gleaned from this work its that there is far more reporting of breaches and issues than in the past...that's it, as there's certainly no reliable statistics to prove that people are actually being affected more than before. Finally, it's worth pointing out that Mr. Eppel falls short of providing any sort of suggestion as to what must be done in the future, beyond presumably us just giving up. He leaves that for what he says will be his "part 2" story...ah, yet again, someone hyping FUD with no viable solutions to offer. Where have we seen that before?"*

The fact that simply using PHP to create a web site where users can post comments is now "scary" only strengthens my argument! If the current state of cybersecurity is so poor that we can't even use a programming language to implement a basic feature such as user comments without "scary" consequences then clearly we are in a state of dramatic insecurity! Cooper actually advocates that people no longer use PHP to allow visitors to post comments - and he sees nothing wrong with that suggestion?! (PHP is only the most popular server-side scripting language that powers some of the most popular web sites.) What other technologies should we throw out and avoid due to security risks? Email? Blogs? Web Sites?

Cooper attempts to discredit my arguments by completely misrepresenting what I said, such as claiming I believe, "every form of eBusiness is going to fail by the end of 2006", "every idea we have is useless", and "nothing works, nor will it." Nowhere did I make such statements. If anyone was confused over what FUD is, Cooper provides a perfect demonstration.

Cooper claims that many of the facts in my article are out and out wrong and "spun" to drive my theory, yet doesn't provide a single example of an incorrect fact.

He also criticizes the article because it didn't contain any quick-fix solutions:

> *"Mr. Eppel falls short of providing any sort of suggestion as to what must be done in the future, beyond presumably us just giving up. He leaves that for what he says will be his "part 2" story...ah, yet again, someone hyping FUD with no viable solutions to offer."*

Presumably us just giving up? I clearly wrote in the article that, "This document is not intended to contain all the answers. Instead it is written to raise awareness of the problem which too many people seem to not want to acknowledge. Through increased awareness can there be new dialogues and discussions on solutions. Because what is clearly missing is more dialog to come up with solutions to today's security challenges. No one can deny the Internet's immeasurable benefits to our lives. This only heightens the need to confront and stop the overwhelming security threats." And I wrote that, "Part Two of this article will contain a list of what we must do to address our current failure... It will incorporate your comments and feedback."

Why then, with such a clear statement on the purpose of the article, and the need to confront and stop the overwhelming security threats, and that a follow-up article on solutions will be forthcoming, is Cooper criticizing the article for not providing solutions? I suppose some people just want quick-fix solutions.

Cooper argues that security isn't failing or getting worse, its just that more people are reporting their breaches. He writes:

> *"If there's much to be gleaned from this work its that there is far more reporting of breaches and issues than in the past...that's it, as there's certainly no reliable statistics to prove that people are actually being affected more than before."*

Cooper alludes to the fact that statistics can be unreliable, yet from the lack of reliable statistics Cooper has concluded that we are not failing and that there is simply more reporting of breaches then in the past! How can anyone possibly make this conclusion from a body of unreliable statistics?

Organizations are increasing the sheer amount of access to once-isolated applications, servers and databases at an unprecedented rate. The number of PC users is expected to hit or exceed 1 billion by 2010, up from around 660 million to 670 million today. There is no question that as more of our critical data becomes internet-accessible more people are being affected by cybercrime. Scale is what makes the issue of cybersecurity so challenging, a point Tim made:

> *"Scale is the reason the problem is so bad. Scale is an inherent feature of the Internet: millions of (flawed) applications, millions of potential victims, millions of potential attackers - all of which can interact with full capability from distant locations. The effect is that a security flaw in an application is not at all like a safety flaw in a power tool; it's likely that only one hand is lost at a time in that faulty table saw, but a typical security flaw allows the attacker to exploit millions of people at nearly the same cost as exploiting just one."*

With the claim that security is failing so common among some of the most respected names in the industry, why then is this so shocking to people like Russ Cooper? Where have they been?

Enjoying the water perhaps..

But what is failure?

While many people are claiming security is failing, we do not have the metrics yet to define what "failure" or "success" actually is.

My idea of security is that a user should be free to conduct, "normal and common" activities and not have to expect that he/she will be a victim of crime. If a man parks his expensive car in a bad neighborhood in the middle of the night and leaves it unlocked with the windows rolled down and with a $100 bill on the dashboard of the car, then that is irresponsible behavior and it is likely a crime will happen. However, if the man carries out what is considered normal activities - i.e., parks in the daytime on a busy street and locks it with a good security system - then that is normal and common behavior and a crime should not be expected.

Today, computer users can use their computers for, "normal and common" activities - such as reading email, browsing the web, using instant messaging, searching for and downloading a screen saver - and still easily fall victim to viruses, trojans, and spyware. Leading anti-virus companies have an 80-percent miss rate, and malware is so prevalent and invasive that occasionally products are shipped straight from vendors which contain viruses and spyware!

Some security professionals claim that if people just follow the acceptable computer behavior, they will remain safe. However, security professionals instruct that acceptable computer behavior now includes, "Never open any email attachment!", "Never click on links in email!", "Never browse untrustworthy web sites!", "Never download any games or screensavers!", "Never use PHP to allow users to submit comments!" A home user can't even use the web browser installed on his computer - he/she is told to "Never Use Internet Explorer." and instead to switch to Firefox! That is like telling the man to be free to use his car, but only on certain roads, between 3:00AM - 1:00PM, to only make right-hand turns, and with only a specific brand of tires and gas!

The average user simply can't keep up with the constantly changing Best Practices and security advise. Today we REQUIRE that individuals that just want to do their jobs, communicate with colleagues or play games online (i.e., normal and common behavior) have to become advanced computer users in order to do so.

When a man can't even park a car in the middle of the day without it being damaged or stolen, or a user can't even use their computer for normal and common things such as reading email or sharing a video with friends without being exposed to malware, then that is evidence of security failure.

But what is success?

Susan Brenner, a law professor who specializes in cybercrime, states it best:

> *"Our goal is to keep crime on line to manageable proportions, to maintain the necessary baseline of order for cyberspace to function as an analogue of the real-world. In the real-world, we maintain a baseline of order which allows societies to carry out the functions they must if they and their constituents are to survive and prosper. We cannot eliminate real-world crime, but we control it."*

Scott Pinzon, Editor-in-Chief of WatchGuard's LiveSecurity Service commented in the cisspforums:

> *"I don't think Information Security is failing, for the simple reason that today more online commerce is occurring than ever in history, and for the most part, it works. Info Sec is far from perfect; we all know that. But you can't point at a bunch of bad drivers and say "the national highway system is failing!" or a few crime-ridden cities and say "our entire culture is crashing into chaos!" The fact that we all go about our day banking, buying, and investing proves that Info Sec is not failing."*

Clearly there are people still using the internet despite the dangers. Just as the existence of a security incident does not automatically mean security is failing (the goal is not 100% security because we can never eliminate all online crime), the evidence of people banking and buying online does not automatically mean we are succeeding.

The second critical measure which will indicate success is that our technology must be securable - meaning that people (from System Administrators to home users) should be able to take **reasonable**, **straight-forward** and **practical** measures to achieve an effective level of security. Today's reality of insufficient security software and outdated and inadequate Best Practices, simply means that achieving an effective level of security is beyond the reach of most people and companies today. Security is simply not accessible.

A Note On Vista...

Microsoft has a virtual monopoly on the computing operating system market. Over 90% of computers are running some form of Windows, and cybercriminals primarily target the security weaknesses of Windows. Due to Microsoft's poor record on security, many security professionals think of Microsoft as the enemy of information security. Microsoft should not be blamed. Windows is being attacked by exploit techniques that weren't even invented while Windows was being developed.

While clearly Microsoft has contributed a lot to today's dismal security situation, it can't be blamed for all today's problems. Similarly, it is in perhaps one of the best positions to help improve the situation. Security professions need to work with Microsoft, not against it. The "blue hat" security conferences, which brings security experts and Microsoft together to share the latest exploit techniques, is a great example of how the security industry and Microsoft can work together to benefit security.

Microsoft's work in training developers company-wide in secure coding practices is virtually unparalleled among major software vendors, and has resulted in their Security Development Lifecycle (SDL), a formalized process for incorporating secure coding and security testing into every phase of a product's lifecycle. Their Trustworthy Computing initiative so far looks like a success; one that has transformed Microsoft's and much of the industry's thinking about security in just four years.

Microsoft has also gone on the offensive against phishers that attempt to steal personal financial information. Microsoft has filled 129 lawsuits to date against phishers in Turkey, Germany, France, Italy, UAE, The Netherlands, Morocco and the UK as part of their "Global Phishing Enforcement Program". Under this program, which was launched in March this year, a total of 253 Web sites have been investigated. Out of the 129 lawsuits, 97 are criminal complaints filed in cooperation with local authorities.

Within a few weeks, Microsoft will be releasing the latest version of their Windows operating system. There is much debate on whether or not Vista will have any effect on improving the overall state of security.

When firewalls were introduced people claimed there would be no more hackers. When anti-virus software was created people claimed there would be no more viruses. When personal firewalls were created people claimed there would be no more spyware. No technology alone can or will solve the current security challenges. It is only part of the solution.

However, Vista is different. The Windows operating system is the foundation of the large majority of computers, workstations and servers. It is the common denominator of nearly every single user across the Internet. Every single application (including security software) relies and depends on the security of the host operating system.

The National Security Agency (NSA) recently published, " The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments". One of the authors, Stephen Smalley, described the paper to me as:

> *"It is essentially a call to action itself, specifically focused on filling the critical gaps in the protection mechanisms provided by today's mainstream operating systems, in particular mandatory security and trusted/protected paths. Without those mechanisms, we cannot make any serious headway in solving the higher level security problems plaguing current systems, as argued in the paper. The NSA SELinux project was motivated by this challenge, and has succeeded in getting a flexible mandatory access control mechanism into a mainstream OS (Linux) and in providing a reference implementation from which others can learn (e.g. ported to FreeBSD as SEBSD, port to Darwin underway as SEDarwin). Much work still remains to be done to enable this foundation to be fully leveraged and to extend the same guarantees to higher levels (middleware and applications) and across the network (among a collection of potentially disparate systems), some of which is already work in progress, but we now have the basic building blocks we need to work toward that end."*

As the NSA argues, failure is inevitable and we will not start to solve today's security challenges without first filling the critical gaps in the protection of today's mainstream operating systems.

Vista goes a long way in bringing protection mechanisms such as User Access Control, Kernel Patch Protection, Mandatory Driver Signing & Address Space Layout Randomization to mainstream computer users.

If there is going to be any improvement of the current cybersecurity situation, it has to start with the operating system. In this regard, if Microsoft delivers on their promise to produce a secure operating system, it will be an important milestone for cybersecurity, and quite possibly a start to a security revolution.

Vista also launches Microsoft's entry into the security space with anti-malware products and services such as Windows Defender, OneCare, and Forefront. The insufficiencies of today's anti-malware software have long been known. Microsoft's entry into the security space will force security vendors to innovate or be pushed out of the market.

I, for one, applaud Microsoft's recent efforts and results. I predict that Vista will have quite a positive effect on the overall state of computer security and we may see a Vista Ripple Effect throughout the industry. However, technology alone will not solve the security challenges and how well Microsoft has implemented the security features in Vista is still yet to be determined.

So Where Do We Go From Here?

There are a growing number of people adding their voice to the claim security is failing. There is now more awareness - and acceptance - that we are currently failing and are facing significant challenges ahead. This awareness is what will produce discussion and through discussion we can formulate solutions.

Many in our industry still choose to ignore the problem and believe the current situation of zero-days, 100,000-node botnets, rampant DDOS extortion, and spam-clogged email accounts is "business as usual" and "normal".

Our failure is not something to fear. It is not something to be ashamed of. This is no time to lose focus or shrink from our responsibilities. These are exciting times for Security Professionals. We face formidable adversaries, but challenges are what will drive real innovation and progress in our industry.

No one can deny the Internet's immeasurable benefits to our lives. This only heightens the need to confront and stop the overwhelming security threats. While I have no doubt in my mind that we are currently failing, I am equally convinced that we will ultimately win.

Ravi Char commented:

> *After reading this article, I was reminded about a quote from Martin Luther King, JR.: "The ultimate measure of a man is not where he stands in moments of comfort and convenience, but where he stands at times of challenge and controversy."*

Comments

Thanks to everyone who has written in with comments and questions. Have something to say? Read the comments and post your own by clicking here...

Thank you for your continuing comments and feedback. Special thanks to Wes Kussmaul, Marcus Ranum, Eugene H. Spaffords, Stephen Smalley, Ian Ferguson & Robert Beggs. Part Two is forthcoming. Stay tuned... Lots more to come.

Recommended Readings:

Quiet Enjoyment: Bring Security With Privacy to Your Networks and Your Life
http://search.barnesandnoble.com/bookSearch/isbnInquiry.asp?r=1&isbn=1931248125

The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments
http://www.nsa.gov/selinux/papers/inevit-abs.cfm

2004-2005 PITAC Reports to the US President: Cyber Security: a Crisis of Prioritization
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

An Introduction to Factor Analysis of Information Risk (FAIR)
http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf

The Six Dumbest Ideas in Computer Security
http://www.ranum.com/security/computer_security/editorials/dumb/

Making the Case for Replacing Risk-Based Security Donn B. Parker, CISSP
http://www.issa.org/journal_archive.html

Digital Defense's Response to Security Absurdity
http://www.digitaldefence.ca/mydocs/media/pdf/wp-securityabsurdity2062306_165519.pdf

---

November 22, 2006

This article is an opinion of the author(s) and does not necessarily represent the views or policy of their employers or their employees. All information and statistics contained in the article are correct to the best of the author(s) knowledge and has been linked to the original source where possible. If any information contained herein is inaccurate, kindly notify the author(s). Links contained in this article to external sources should not imply a relationship between this site and the external resource. Thank you for reading. Your comments and feedback is most appreciated.