SecurityAbsurdity.com >

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 tolerated it since we are use to it.

It is time to admit what many security professional already know: We as security professional 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 is 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 forth 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/CSI Computer Crime and Security 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 the FBI, every day 27,000 have their identities stolen. 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 then 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.

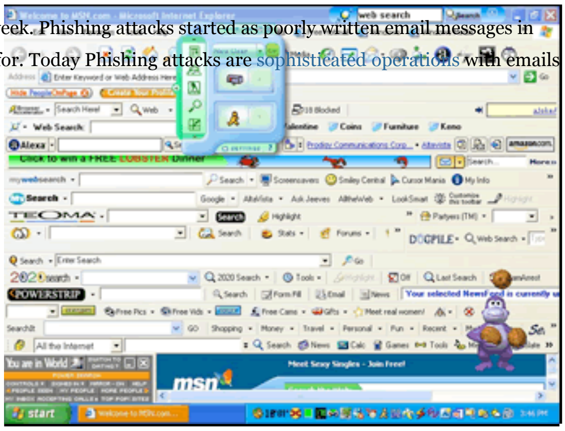
SPYWARE

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.

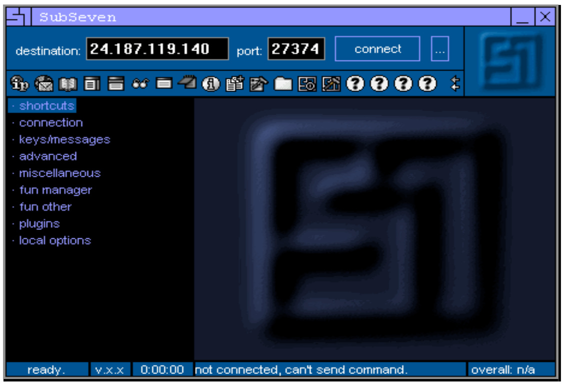
TROJANS & VIRUSES & WORMS

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.

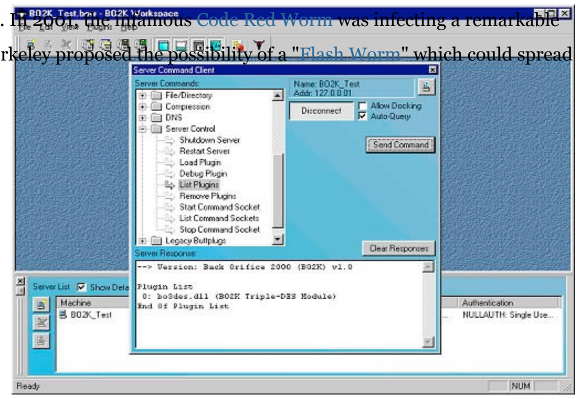


destination: 24.187.119.140 port: 27374

ready. v.x.x 0:00:00 not connected, can't send command. overall: n/a

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.



```
--> Version: Back Orifice 2000 (BO2K) v1.0

Plugin List
 0: bo3des.dll (BO2K Triple-DES Module)
End Of Plugin List
```

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

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 then 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 Wireless 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 256 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 260 calculations in 56 hours, and 269 calculations in three and a quarter years. Or, a machine that cost $25M-$38M could do 269 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.

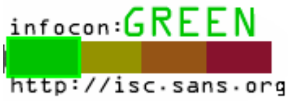
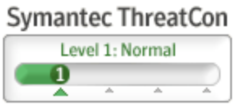
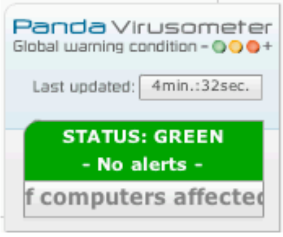
What does this mean for the average person? While these developments are big news for cryptographers, they present little real-world risks to the average user at the moment. However, what these developments make clear is that its time for a new standard.

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 then 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.	 infocon:GREEN http://isc.sans.org	"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."	 Symantec ThreatCon Level 1: Normal 1	"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."	 Panda Virusometer Global warning condition - + Last updated: 4min.:32sec. STATUS: GREEN - No alerts - f computers affecte	"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 then $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 then 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!

Computer users attempting to sign up for an email account or blog are now faced with a mismatch of letters and numbers that they have to try and 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 then 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 keyboards 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 then $100 US. They then proceeded to transfer more that $440 million to various accounts in other countries.

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.