Bruce Schneier

Crypto-Gram Newsletter

September 15, 2000

by Bruce Schneier
Founder and CTO
Counterpane Internet Security, Inc.
schneier@schneier.com
<http://www.counterpane.com>

A free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography.

Back issues are available at <http://www.counterpane.com>. To subscribe or unsubscribe, see below.

In this issue:

Full Disclosure and the Window of Exposure

Every season yields a bumper crop of computer security stories: break-ins, new vulnerabilities, new products. But this season has also given us a crop of stories about computer security philosophy. There has been a resurgence in opposition to the full disclosure movement: the theory that states that publishing vulnerabilities is the best way to fix them. In response, defenders of the movement have published their rebuttals. And even more experts have weighed in with opinions on the DeCSS case, where a New York judge ruled that distributing an attack tool is illegal.

What's interesting is that everybody wants the same thing; they're just disagreeing about the best way to get there.

When a security vulnerability exists in a product, it creates what I call a window of exposure. This window exists until the vulnerability is patched, and that patch is installed. The shape of this window depends on how many people can exploit this vulnerability, and how fast it is patched. What everyone wants is to make this window as small as possible.

A window of exposure has five distinct phases. Phase 1 is before the vulnerability is discovered. The vulnerability exists, but no one can exploit it. Phase 2 is after the vulnerability is discovered, but before it is announced. At that point only a few people know about the vulnerability, but no one knows to defend against it. Depending on who knows what, this could either be an enormous risk or no risk at all. During this phase, news about the vulnerability spreads -- either slowly, quickly, or not at all -- depending on who discovered the vulnerability. Of course, multiple people can make the same discovery at different times, so this can get very complicated.

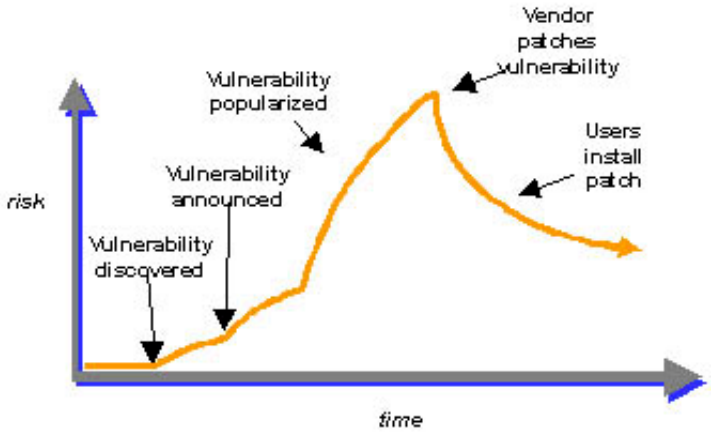

Figure 1

Phase 3 is after the vulnerability is announced. Maybe the announcement is made by the person who discovered the vulnerability in Phase 2, or maybe it is made by someone else who independently discovered the vulnerability later. At that point more people learn about the vulnerability, and the risk increases. In Phase 4, an automatic attack tool to exploit the vulnerability is published. Now the number of people who can exploit the vulnerability grows exponentially. Finally, the vendor issues a patch that closes the vulnerability, starting Phase 5. As people install the patch and re-secure their systems, the risk of exploit shrinks. Some people never install the patch, so there is always some risk. But it decays over time as systems are naturally upgraded.

In some instances the phases are long, and sometimes they're short. Sometimes Phase 5 happens so fast that Phases 3 and 4 never occur. Sometimes Phase 5 never occurs, either because the vendor doesn't care or no fix is possible. But this is basically the way things work.

The goal of any responsible security professional is to reduce the window of exposure -- the area under the curve -- as much as possible. There are two basic approaches to this.

The first is to reduce the window in the space dimension by limiting the amount of vulnerability information available to the public. The idea is that the less attackers know about attack methodologies, and the harder it is for them to get their hands on attack tools, the safer networks become. The extreme position in this camp holds that attack tools should be made illegal.

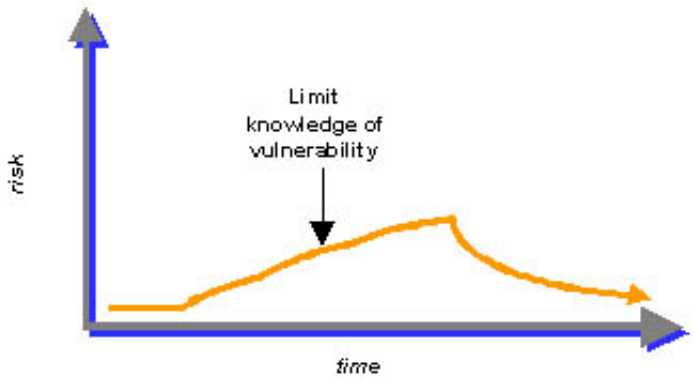

Figure 2

This might work in theory, but unfortunately it is impossible to enforce in practice. There is a continuous stream of research in security vulnerabilities, and most of this research results in public announcements. Hackers write new attack exploits all the time, and the exploits quickly end up in the hands of malicious attackers. Any one country could make some of these actions illegal, but it would make little difference on the international Internet. There have been some isolated incidences of a researcher deliberately not publishing a vulnerability he discovered, but public dissemination of vulnerability information is the norm...because it is the best way to improve security.

The second approach is to reduce the window of exposure in time. Since a window remains open until the vendor patches the vulnerability and the network administrator installs the patches, the faster the vendor can issue the patch the faster the window starts closing. To spur the vendors to patch faster, full-disclosure proponents publish vulnerabilities far and wide. Ideally, the vendor will distribute the patch before any automatic attack tools are written. But writing such tools can only hasten the patches.

This also works a lot better in theory than in practice. There are many instances of security-conscious vendors publishing patches in a timely fashion. But there are just as many examples of security vendors ignoring problems, and of network administrators not bothering to install existing patches. A series of credit card thefts in early 2000 was facilitated by a vulnerability in Microsoft IIS that was discovered, and a patch released for, a year and a half earlier.

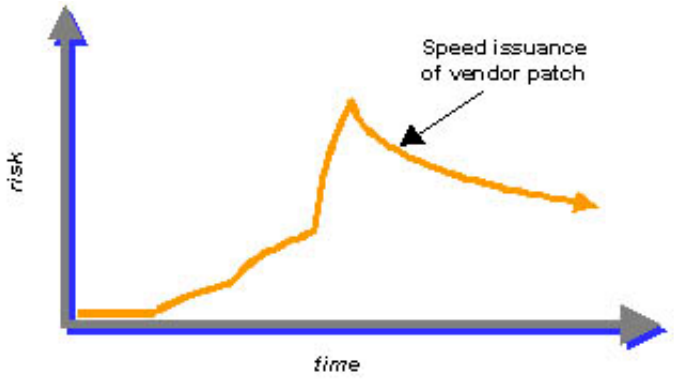

Figure 3

The problem is that for the most part, the size and shape of the window of exposure is not under the control of any central authority. Not publishing a vulnerability is no guarantee that someone else won't publish it. Publishing a vulnerability is no guarantee that someone else won't write an exploit tool, and no guarantee that the vendor will fix it. Releasing a patch is no guarantee that a network administrator will actually install it. Trying to impose rules on such a chaotic system just doesn't work.

And to make matters worse, it's never one single vulnerability. There are dozens and hundreds of vulnerabilities, all with overlapping windows. One vulnerability might be shrinking while another ten are growing. We're like the little Dutch boy, plugging leaks in the dike with our fingers while others spring up nearby. It doesn't matter if we believe that full disclosure is the best way to reduce the window's size or if quietly alerting the vendor does better...we're going to lose the war fighting it either way.

Vulnerabilities are inevitable. As our networks get more complex and more pervasive, the vulnerabilities will become more frequent, not less. We're already seeing this; every year brings more security holes than the previous one. The only way to close the window of exposure is to make it not matter. And the only way to do that is to build security systems that are resilient to vulnerabilities.

In *Secrets and Lies*, I talk about security processes that make systems resilient to vulnerabilities. The most relevant one to this debate is detection and response. Most computer-security products are sold as prophylactics: firewalls prevent network intrusions, PKI prevents impersonation, encryption prevents eavesdropping, etc. The problem with this model is that the product can either succeed or fail: either the window of exposure is closed or it is open. Good security includes not only protection, but also detection and response. An Internet alarm system that detects attacks in progress, regardless of the vulnerability that was exploited, has the ability to close the window of exposure completely.

The key to Internet detection and response is vigilance. Attacks can happen at all times of the day and night, and any day of the year. New attack tools appear all the time; new vulnerabilities become public all the time. I built Counterpane Internet Security, Inc. as a managed security monitoring company because I saw this as the only way to bring security to computer networks. Without outsourced detection and monitoring, we're at the mercy of all the hackers and product vendors and security professionals.

Those advocating secrecy are right that full disclosure causes damage, in some cases more damage than good. They are also right that those who build attack tools should be held liable for their actions; the defense of "I just built the bomb; I didn't place it or set the fuse" rings hollow. But they are wrong to think they can enforce secrecy. Information naturally disseminates, and strategies that go against that are doomed. Those advocating full disclosure are right that rapid dissemination of the information benefits everyone, even though some people make ill use of that information. We would be in a much worse position today if vulnerability information were only in the hands of a privileged few.

Neither full disclosure nor secrecy "solve" computer security; the debate has no solution because there is no one solution. Both sides are missing the point. The real issue, how to close the window of exposure, is more subtle. We have to stop thinking of software security as an end state, that fixing the bugs will somehow make the software perfect. Security vulnerabilities are inevitable and there will always be a window of exposure; smart security solutions will work regardless.

Marcus Ranum started this debate at BlackHat. A transcript of his talk isn't available on-line, but these two essays are:
<http://pubweb.nfr.net/~mjr/usenix/ranum_5.pdf> <http://pubweb.nfr.net/~mjr/usenix/...>

Weld Pond's rebuttal:
<http://www.zdnet.com/zdnn/stories/comment/...>

Stuart McClure and Joel Scambray's rebuttal:
<http://www.infoworld.com/articles/op/xml/00/08/14/...>

Another view:
<http://news.cnet.com/news/0-1005-200-2634067.html>

News article:
<http://www.zdnet.com/zdnn/stories/news/...>

My older writings on this topic:
<http://www.schneier.com/...> <http://www.schneier.com/...>

Secrets and Lies News

Secrets and Lies is officially published. This means that you can walk into a bookstore and buy it. Last month, when I announced the book, it was printed and in the Wiley warehouse but not in bookstores.

Initial feedback has been great. There are already reviews on the Amazon.com Web site. The Economist published a review of the book, as did Business Week, Industry Standard, New Scientist, and Salon. Other reviews are coming in the next few weeks.

Here's the publishing information:
Secrets and Lies: Digital Security in a Networked World Bruce Schneier
John Wiley & Sons, 2000 ISBN: 0-471-25311-1
$29.99

Book Web site:
<http://www.schneier.com/book-sandl.html>

See the Table of Contents:
<http://www.schneier.com/book-sandl-cont.html>
Read the Preface:
<http://www.schneier.com/book-sandl-pref.html>
Amazon.com has posted Chapter 3:
<http://www.amazon.com/exec/obidos/ts/book-excerpt/...>

Buy the book here:
<http://www.amazon.com/exec/obidos/ASIN/0471253111/...>

Reviews:
<http://www.salon.com/tech/review/2000/08/31/...>
<http://www.businessweek.com/2000/00_38/b3699176.htm>
<http://www.thestandard.com/subject/book/display/...> All reviews:
<http://www.schneier.com/book-sandl-rev.html>

Bruce Schneier is planning a book tour for October. Planned locations include San Francisco, San Jose, Seattle, Portland, New York, Boston, and Washington, DC. Tour dates and locations can be found here:
<http://www.schneier.com/book-sandl-tour.html>

Crypto-Gram Reprints

Open-source and security:
<http://www.schneier.com/...>

Factoring a 512-bit number:
<http://www.schneier.com/...>

News

Another massive net attack coming?
http://www.zdnet.com/zdnn/stories/news/...

Analytic Thinking and Presentation for Intelligence Producers, Analysis Training Handbook. By the CIA's Office of Training and Education.
<http://216.167.120.50/cia-ath-pt1.htm>

How one bank survived a security audit: In an effort to identify potential security risks, a bank shares its experiences of having its systems scrutinized.
<http://www.eweek.com/a/pcwt0008141/2613074/>

Software Risk Management Conference:
<http://www.isacc.com/>

Why Microsoft doesn't have to improve security.
<http://news.cnet.com/news/0-1005-200-2528362.html>

Cheaper technologies than PKI:
<http://www.zdnet.com/eweek/stories/general/...> There's a lot of snake-oil in this article, but some of the ideas are good.

A good article on the difficulty of normal people actually using security technology.
<http://www.zdnet.com/eweek/stories/general/...>

Hacking insurance (a good article).
<http://www.computerworld.com/cwi/story/...>

An excellent analysis of the DeCSS decision by Emmanuel Goldstein. Worth reading.
<http://www.2600.com/news/2000/0821.html>

Now that CSS is broken, the DVD manufacturers have another dumb idea: watermarking.
<http://www.wired.com/news/technology/...>

Internet bank robbery:
<http://www.independent.co.uk/news/Digital/Update/...>
The bank is claiming that no money was stolen, and the truth seems very mundane.
<http://www.theregister.co.uk/content/1/12822.html>
And the culprits have been apprehended.
<http://www.zdnet.com/zdnn/stories/news/...>

Two good articles on encryption algorithms, the first on DES and the second on AES.
<http://www.ams.org/notices/200003/fea-landau.pdf> <http://www.ams.org/notices/200004/fea-landau.pdf>

It's over six months since last February's massive distributed denial-of-service attacks. One survey found over 100,000 computers still vulnerable. What does it take to get through to some people?
<http://www.internetnews.com/bus-news/article/...>

New trend: breaking into networks and extorting money out of the owners:
<http://www.businessweek.com/bwdaily/dnflash/aug2000/...>

New computer virus (similar to the Love Bug, but with a much nastier payload) targets children:
<http://www.wired.com/news/technology/...> <http://vnunet.com/News/1109520>

The safety of open source operating systems:
<http://securityportal.com/topnews/...>

TRUSTe violating its own security policy? Weren't they the ones who told us that self-regulation would work?
<http://www.computerworld.com/cwi/story/...> <http://www.cnn.com/2000/TECH/computing/08/24/...>

JAVA emulators of WWII crypto devices: Purple, Sigaba, Enigma, Russian Espionage Cipher, and a public domain Bombe. Good descriptions, too.
<http://dev.thinkquest.org/C004911/>

First malware for the Palm Pilot (a Trojan horse):
<http://www.zdnet.com/zdhelp/stories/main/...> And a response from anti-virus companies:
<http://news.cnet.com/news/0-1006-200-2720432.html?...>

Password crackers: This site lists all sorts of password crackers that run dictionary attacks against a variety of encryption products. My own Password Safe is on the list; there's a password cracker for that, too. The moral is not to choose a guessable password, and that more and more passwords become guessable every year.
<http://members.aol.com/jpeschel/crack.htm#ktools>

Schneier and security:
<http://www.zdnet.com/enterprise/stories/main/...>

In a bizarre twist, @Stake (a company filled with hackers) refuses to hire someone because he's a reformed (but once convicted) hacker. I understand the reluctance to hire criminals, but it seems hypocritical to make a hiring decision based on whether someone was caught hacking ten years ago or whether he got away with it.
<http://www.securityfocus.com/news/79>

A good essay on the risks of Carnivore:
<http://www.crypto.com/papers/carnivore-risks.html>

A Thai company has developed a security robot that can shoot criminals. According to the company: "It is armed with a pistol that can be programmed to shoot automatically or wait for a fire order delivered with a password from anywhere through the Internet."
<http://catless.ncl.ac.uk/Risks/21.02.html#subj8> <http://news.bbc.co.uk/hi/english/sci/tech/...>
Words fail me on this one.

More web bugs. Someone can add a web bug to a Microsoft Word document and track who opens it. Nasty side effect of being online all the time.
<http://www.privacyfoundation.org/advisories/...> A demonstration bugged document:
<http://www.privacycenter.du.edu/demos/bugged.doc>
News articles:
<http://news.cnet.com/news/0-1005-200-2652562.html> <http://www.computerworld.com/cwi/story/...>
<http://www.wired.com/news/technology/...>

Microsoft's response to the web bugs is pretty weird. They make a big deal about cookies, not web bugs. It's sort of like they missed the point completely.
<http://www.microsoft.com/technet/security/cookie.asp>

RSA Inc. executes a clever publicity move. Many events and parties are planned to commemorate the expiration of the RSA algorithm patent on 20 September 2000. So what does RSA Inc. do? They put the algorithm in the public domain two weeks early and pre-empt the publicity. Meaningless, but pretty clever.
<http://www.rsasecurity.com/news/pr/000906-1.html> <http://www.zdnet.com/zdnn/stories/news/...>

DDOS tools get even easier to use:
<http://www.nwfusion.com/news/2000/0906ddos.html>

Another Microsoft bug (this one in NetBIOS). This one affects Windows 95, 98, NT, and 2000. The really odd piece of this story is that Microsoft doesn't plan on releasing a patch for this one.)
<http://www.pgp.com/research/covert/advisories/045.asp>

Global tracking and MSN GUID. Nasty privacy violation.
<http://www.pc-help.org/privacy/ms_guid.htm>

Internet Explorer persistence. Yet another Microsoft security problem:
<http://news.cnet.com/news/0-1005-200-2751843.html>

Amazon.com leaks customer e-mail addresses:
<http://computerworld.com/cwi/story/...>

The Secure Digital Music Initiative is having a hacking contest to see which of their content protection schemes are better. I've already written about why hacking contests make no sense, and don't do anything to show which scheme is better. I've also already written about why the whole concept of content protection is flawed, and that it doesn't matter how good the scheme is.

<http://www.hacksdmi.org/>

Self-propagating security patch...in rabbits!
<http://www.newscientist.com/news/news.jsp?id=ns225354>

The story of the stolen Bletchley Park Enigma machine gets wierder:
<http://www.guardianunlimited.co.uk/Archive/Article/...>
<http://www.thetimes.co.uk/news/pages/tim/2000/09/13/...>

The European Telecommunication Standards Institute (ETSI) has made a bunch of encryption algorithms public:
<http://www.etsi.org/dvbandca/>

A just-released GAO report gives the government bad marks when it comes to security. Collectively, the agencies averaged D-, with more than a quarter of them flunking, and only two out of twenty-four agencies getting better than a C rating.
<http://washingtonpost.com/wp-dyn/articles/...>
<http://www.foxnews.com/national/091100/govsecurity.sml>
<http://www.cnn.com/2000/TECH/computing/09/11/...>

Counterpane Internet Security News

Bruce Schneier is speaking at the eCFO Conference in Atlanta, on 19 September.
<http://www.e-cfoexpo.com/>

Bruce Schneier is speaking at the E-Business Security Summit in Chicago, on 4 October.
<http://www.aliconferences.com/conferences/...>

Carnivore Disinformation

This bit, from Newsweek's Periscope, sounds very much like government propaganda:

Tracking bin Laden's E-Mail

American counter-terrorism experts are aghast that the FBI has gone public with Carnivore, its new Internet-wiretap system. The reason for their dismay: Osama bin Laden uses e-mail to communicate with his terrorist network. The intelligence community's ability to track his messages has been, according to one intelligence source, "the biggest single factor in shutting down several planned operations," including some in the United States. "Bin Laden thought his communications were secure," says the source. "They weren't. Now we've told him."

FBI officials acknowledge that Carnivore has been used about 25 times, primarily in terrorism investigations. But they decline to comment on its use against bin Laden. "Everyone knows we can wiretap phones," says a bureau spokesman. "There's no reason why an ability to intercept e-mails must necessarily be covert."

FBI Requires Constitutional Changes

It's hard to know what to think of this:

"One of the FBI requirements for the Internet kiosks at the 2002 Olympics is that the FBI be able to record all passwords, copy all sent email, and divert sent email for administrative decisions on whether it should be delivered."

If it is true, it is the most intrusive power grab we've seen so far. Would there even be warning notices on the kiosks? Would they demand eavesdropping rights on all direct computer hookups as well? The mind boggles.

<http://www.pbs.org/cringely/pulpit/pulpit20000803.html>

The Doghouse: FaceMail

FaceMail uses your "personal biometric facial template" to encrypt and decrypt emails. They don't say what

happens if someone else steals your key or if you have surgery.

Zero technical details can be found at:
<http://www.identalink.de/>

PGP Vulnerability

A very serious PGP vulnerability was just discovered. Using this vulnerability, an attacker can create a modified version of someone's public key that will force a sender to encrypt messages to that person AND to the attacker.

Let me explain.

Starting with PGP version 5.5, the software supported something called an Additional Decryption Key (ADK). Normally, when a PGP user creates a PGP certificate, it contains a single public key (as well as identifying information as to who the key belongs to). PGP version 5.5 and 6.x allow the user to add additional ADKs to the certificate. When a sender encrypts a message to that user, PGP will automatically encrypt the message in both the user's public key and the ADK. The idea is that the ADK belongs to the secret police, or the user's employer, or some organization, and that organization can intercept the encrypted message and read it.

(On Slashdot I said that Network Associates did this when they joined the Key Recovery Alliance, but PGP Inc. added the feature before then. They needed it to get certain corporate contracts.)

The flaw is that some version of PGP don't require the ADKs to be in the signed portion of the PGP certificate. What this means is that an organization can take a PGP certificate, append his ADK, and spread it out to the world. This tampered version of the certificate will remain unnoticed by anyone who doesn't manually examine the bytes, and anyone using that tampered version will automatically and invisibly encrypt all messages to the organization as well as the certificate owner.

Colleague Greg Guerin likened the lesson of this vulnerability to something he learned in kindergarten: "Don't put something in your mouth unless you know where it's been."

The reaction from Network Associates has been pretty good: they fixed the problem. Unfortunately, the president of the PGP Security unit demonstrated a high degree of cluelessness when he said: "This a fairly esoteric attack. It's not likely that anybody without specialized knowledge could use it." Certainly it is an esoteric attack but, as we all know, that person with specialized knowledge could easily encapsulate the attack in a point-and-click program that any script kiddie could use.

On the plus side, it doesn't seem like anyone took advantage of this vulnerability. Network Associates inspected all 1.2 million PGP keys on its keyserver, and found none of them were tampered with in this way.

Way back in 1997 a bunch of us cryptographers predicted that adding key escrow would make system design harder, and would result in even more security problems. This is an example of that prediction coming true.

Research paper on the vulnerability:
<http://senderek.de/security/key-experiments.html>

CERT Advisory:
<http://www.cert.org/advisories/CA-2000-18.html>

Slashdot article:
<http://slashdot.org/articles/00/08/24/155214.shtml>

News reports:
<http://www.thestandard.com/article/display/...>

Nice summary article:
<http://www.digitalmass.com/columns/software/0828.html>

Network Associates reaction:
<http://www.pgp.com/other/advisories/adk.asp> [link dead; see http://www.pgp.com/support/product-advisories/adk.asp]

1997 Risks of Key Escrow Paper:
<http://www.schneier.com/paper-key-escrow.html>

Comments from Readers

From: Brian Taylor
Subject: PGP Vulnerability and the DMCA

I have copyrighted works protected with PGP. I did not consent to the TPM I use being circumvented. Bruce's description of this vulnerability is clearly a circumvention technology that will be used to pirate my work and is thereby illegal under the DMCA.

I'm going to file a lawsuit against Bruce and Slashdot and anyone who links to Slashdot and anyone who reads the article and anyone who points at or otherwise refers to a person who reads the article. In fact, Bruce himself is circumvention technology, so I'm suing his parents, too, along with the major airlines, both of which have distributed Bruce.

From: Aleph One <aleph1@underground.org>
Subject: Firewalls and tunnelling protocols

Firewalls were never meant to stop covert channels.

While it's all too true that current firewalls performs a rather lacking job at verifying that a protocol they are forwarding meets its specification, and you could certainly be creative and attempt to find ways to detect and stop covert channels, as long as the firewalls allows some traffic through, any traffic, a covert channel will be possible.

So the real problems are in your expectation of a firewalls capabilities, something all too common, and in vendors exploiting overly generic and complex protocols to bypass what they see as nothing more that an annoyance to the ease of use and deployment of their application.

From: "Scott Tousley" <stousley@genuity.net>
Subject: SANS

I think you let SANS wriggle off the hook in your article from two weeks ago, and I think their fingerprints from the MSNBC article runs the same direction. While I'm not convinced that Genuity, UUNet, AT&T, C&W, Sprint, PSINet and others are doing all that our business motivation demand, I also do not think that the answer is found in a loose confederation of SANS, CERT CC, OMB/FEDCIRC, and WH/NSC/CIAO staff designing private-sector requirements. SANS now and CERT CC in the past have contributed to some good work for network security, but I do not think this means they should take an operational role and drive the private sector on behalf of the government. The SANS stumbling over the Microsoft problem is a reflection of this inappropriate role.

From: "Gary Hinson" <gary.hinson@cccl.net>
Subject: SANS

I completely agree with your editorial about the SANS news flash thing. It has done their credibility no good at all, which is such a shame because (until then) I had been very impressed with the SANS services and their (usually) tempered tone. It seems quite out of character, in fact I wondered if someone had hacked the SANS emailer and sent out a spoof! The 'virus to catch a virus' was really over the top!

From: "Mikolaj J. Habryn" <dichro-mail-2d77bd17@rcpt.to>
Subject: Bluetooth

If you visit www.bluetooth.com, you will find that the full specifications (1400 pages long and amusingly captioned 'Wireless Connections Made Easy') are available and include information on link encryption and key generation and exchange mechanisms.

The specifications do explicitly leave some security issues up to the applications to deal with. If the security of something is terribly important to you, you will need to provide heftier application level security mechanisms than Bluetooth provides, *and* ensure that the hardware platform

that you are running on has the computational resources required to service the application. Remember that Bluetooth is, to some degree, a lowest common denominator.

From: Lasse Leskelä <lasse.leskela@iki.fi>
Subject: a paper on Bluetooth security

There is a paper about Bluetooth security at:
<http://www.hut.fi/~mhermeli/julkaisut/icisc99s.ps.gz>

From: "Reynolds,Martin" <martin.reynolds@gartner.com>
Subj: Bluetooth Security

The Bluetooth security system is well documented in the Bluetooth specs.

Hold tight for this one: it exchanges secret keys using SAFER+. No, this is not my error. They are serious. You are supposed to use sideband information -- a PIN or a serial number -- to enhance the key that you must exchange to use SAFER+ in the first place. The only "good" news is that the keys are persistent and the devices only need to do this on first introduction.

In a cellphone (the cellphone guys wrote the spec) there is a smart card to help this process along.

Worse, there is no security requirement.

Bottom line: it could be worse but, in most hands, Bluetooth security is going to be a mess.

From: John Savard <jsavard@ecn.ab.ca>
Subject: M-134-A

Take my word for it: the Friedman patent issued last month is definitely the M-134-A, and not the M-229. This is indicated unambiguously in the abstract of the patent, and in the wording of claim 6, but I'll admit it is hard even to read the claims.

The diagram on page 1 (shown enlarged on page 2) also makes it clear that the keyboard is connected through the rotors to a lamp-board in conventional Hebern (or Enigma) fashion, but the 5-level signal goes to the 5 rotors individually.

Starting near the bottom of page 4, the first text page of the patent, we read:

"Now, in all cryptographs based upon the use of rotatable cipher wheels of the type referred to above, and arranged as indicated, means are embodied within the cryptograph for automatically changing the rotatory portions of
the cipher wheels during the course of enciphering or deciphering a message; these means are always of such a nature as to make these changes of a definite and predetermined character...."

"The basic feature of my invention of this predictable factor and the provision of a mechanism for displacing the cipher wheels in an entirely irregular, aperiodic manner. This is accomplished by means of the wheel-stepping mechanisms shown as at 4, and operated in the present embodiment by individual magnets which are controlled by the single tape transmitter 5..."

(Incidentally, all information in the following is based on openly published sources, including, admittedly, material released in the National Archives, and hence may be freely used and disseminated. I have not at any time had exposure to any information covered by security restrictions of a military or intelligence nature by the government of the United States or any other country.)

The distinguishing feature of the M-134-A is that it took the bits of a paper tape as input, and used that input to control the movement of rotors, and these rotors then encrypted a character in the basic fashion of a Hebern machine. This is mentioned explicitly in the patent.

The M-229 and M-228, for different purposes, did exactly the reverse of this. Rotors moved (still with the use of an electrical circuit) conventionally, in the way usually produced by gears, but the rotors were wired to a fixed set of live inputs to produce what were essentially binary bits as output.

In the M-228, these bits were XORed with a teleprinter character, and in the M-229 they were used to control rotor movement in an M-134 (the M-134, M-134-A, and M-134-T2 were essentially the same machine; the M-134-T1 was the subject of a patent granted on January 28, 1936 (U.S. patent 2,028,772, as referenced in a Cryptologia article on Friedman's patents). And, of course, the M-134-C is one U.S. Army designation for the famous ECM Mark II, or SIGABA.

It should be clear, from the quotes given from the patent, why I am definite about this being the M-134, since the patent clearly refers to the distinguishing feature of that machine: paper tape as input, a permutation of the alphabet as output.

From: Lance Urbas <lurbas@authentica.com>
Subject: Re: Authentica in the Dog House

Authentica recognizes that a Frequently Asked Question (FAQ) on its Web site, which correlated the strength of encryption with the security of our products, was misleading. This FAQ has been removed and we thank Mr. Schneier for pointing this out as well as apologize for using his name without his permission. We recognize that no security products are unbreakable and protecting information after it's been delivered to another user's computer is not foolproof. However, our goal is not to ensure "absolute" security, but to provide organizations with tools that better manage the risk in sharing digital information.

CRYPTO-GRAM is a free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography.

To subscribe, visit <http://www.schneier.com/crypto-gram.html> or send a blank message to crypto-gram-subscribe@chaparraltree.com. To unsubscribe, visit <http://www.schneier.com/crypto-gram-faq.html>. Back issues are available on <http://www.counterpane.com>.

Please feel free to forward CRYPTO-GRAM to colleagues and friends who will find it valuable. Permission is granted to reprint CRYPTO-GRAM, as long as it is reprinted in its entirety.

CRYPTO-GRAM is written by Bruce Schneier. Schneier is founder and CTO of Counterpane Internet Security Inc., the author of "Applied Cryptography," and an inventor of the Blowfish, Twofish, and Yarrow algorithms. He served on the board of the International Association for Cryptologic Research, EPIC, and VTW. He is a frequent writer and lecturer on computer security and cryptography.

Counterpane Internet Security, Inc. is a venture-funded company bringing innovative managed security solutions to the enterprise.

<http://www.counterpane.com/>

next issue
previous issue
back to Crypto-Gram index
