Bruce Schneier

Crypto-Gram Newsletter

September 15, 2003

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

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

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

In this issue:

Accidents and Security Incidents

On August 14 at 4:00 PM, the power went out in New York City and across much of the Northeast. As many as 50 million people were without power, some for days. Although there were some initial rumors of terrorism -- only a few, thankfully -- it was an accident.

At a time when we're worried about attacks -- by terrorists, hackers, and ordinary criminals -- it's worth spending some time talking about accidents.

Some years ago computer-security researcher Ross Anderson described the difference as Murphy vs. Satan. Defending against accidents, he said, means designing and engineering in a world ruled by Murphy's Law. Things go wrong because, well, because things go wrong. When you're designing for safety, you're designing for a world where random faults occur. You're designing a bridge that will not collapse if there's an earthquake, bed sheets that won't burst into flames if there's a fire, computer systems that will still work -- or at least fail gracefully -- in a power blackout. Sometimes you're designing for large-scale events -- tornadoes, earthquakes, and other natural disasters -- and sometimes you're designing for individual events: someone slipping on the bathroom floor, a child sticking a fork into something (accidental from the parent's point of view, even though the child may have done it on purpose), a tree falling on a building's roof.

Security is different. In addition to worrying about accidents, you also have to think about nonrandom events. Defending against attacks means engineering in a world ruled by Satan's Law. Things go wrong because there is a malicious and intelligent adversary trying to force things to go wrong, at the very worst time, with the very worst results. The differences between attacks and accidents are intent, worst time, with the very worst results. The differences between attacks and accidents are intent, intelligence, and control.

Here are some examples:

Safety: You can predict how many fire stations a town needs to handle all the random fires that are likely to break out. Security: A pyromaniac can deliberately set off more fire alarms than the town's fire stations can handle so as to make his attacks more effective.

Safety: Knives are accidentally left in airplane carry-on luggage and can be spotted by airport X-ray machines. Security: An attacker tries to sneak through a knife made of a material hard to detect with an X-ray machine, and then deliberately positions it in her luggage to make it even harder to detect with the X-ray machine.

Safety: Building engineers calculate how many fire doors are required for safe evacuation in an emergency. Security: Those doors are deliberately barricaded before murderers set fire to the building. (This happened in a Rwandan convent in 1994.)

A few years ago, a colleague of mine was showing off his company's network security operations center. He was confident his team could respond to any computer intrusion. "What happens if the hacker calls a bomb threat in to this building before attacking your network?" I asked. He hadn't thought of that. The problem is, attackers do think of these things. The adolescent murderers at the Westside Middle School in Jonesboro, Arkansas, in 1998 set off the fire alarm and killed five and wounded ten others as they all funneled outside.

In an accident, the attacker is fate, luck, or Mother Nature. In an attack, the attacker is both intelligent and deliberate. Attackers can deliberately force faults at precisely the most opportune time and in precisely the most opportune way. Attackers can exploit other people's accidents. And when an attacker finds a vulnerability, he can exploit it again and again. The odds of a natural fire are very low in most industrial countries, but an arsonist can create a fire on demand. Buffer overflows can happen in computers by accident, but they hardly ever do; an attacker can force a buffer overflow that does maximum damage to a computer system. It is the notion of an attacker that separates safety and security engineering. In security, intelligent opposition is trying to make security fail. And a safety failure caused by an attacker becomes a security failure.

The two are also very similar. Regardless of whether you were stabbed by a mugger or the knife slipped in kitchen accident, the emergency room will respond the same way. The response by firemen, policemen, and other rescue personnel after 9/11 would have been no different had the planes lost their bearings in fog and accidentally flown into the Twin Towers (as a plane flew into the Empire State Building in 1945). Backup procedures are the same regardless of whether someone accidentally deleted a file or a worm deleted the file as part of its programming.

Defenses are largely the same: countermeasures to defend the systems, and reactive measures after the events. Better isolation of individual power plants stops blackouts from spreading, regardless of the cause. The rarity of blackouts, which led to inexperience in dealing with them, exacerbated the problem. Disaster recovery works against both floods and bombs. Securing the weakest link, defense in depth, compartmentalization -- all the techniques I talk about to improve security -- also help prevent accidents.

And, in both cases -- security failures and accidents -- it's a series of failures that makes for spectacular results. The power blackout started as a small accident and then cascaded into a large-scale blackout. The 9/11 terrorist attack started out as a relatively small security failure (taking over the airplanes), turned into a large disaster (crashing them into the World Trade Center), and then cascaded into an enormous disaster (lives lost, buildings collapsed, loss of communications, etc.). In neither case could the final results have been predicted based only on the initial failure; the systems were just too complicated.

It's because of the interconnectedness of our systems that these events turned into large-scale disasters. It happens rarely -- neither the blackout nor the terrorist attacks were common events -- but sometimes things are aligned in just the perfect way so that everything comes out wrong. But if an intelligent and malicious attacker is trying to steer events, disaster is more likely.

"Beyond Fear" Reactions

I would like to thank everyone who purchased "Beyond Fear" from Amazon on August 15. The book made #1 on the non-fiction best-seller list (above Al Franken's book), and #3 on the overall best-seller list (behind "The Da Vinci Code" and a diet book).

Technically, the book wasn't published until September 4, and reviews are just starting to appear. "Schneier's latest book, Beyond Fear (Copernicus Books, 2003), is a highly readable compendium of his

"Schneier's latest book, Beyond Fear (Copernicus Books, 2003), is a highly readable compendium of his thoughts on the various aspects of real-world security. Designed for a general audience, it's a great introduction to a complicated and confusing topic." --Business Week
<http://www.businessweek.com/technology/content/...>

"In Beyond Fear, Schneier has utterly demystified the idea of security with a text aimed squarely at nontechnical individuals. He takes his legendary skill at applying common sense and lucidity to information-security problems and applies it to all the bogeymen of the post-9/11 world, and asks the vital question: What are we getting in exchange for the liberties that the Ashcroftian authorities have taken away from us in the name of security?

"This is possibly the most important question of this decade, and that makes Schneier's book one of the most important texts of the decade. This should be required reading for every American, and the world would be a better place if anyone venturing an opinion on electronic voting, airline security, roving wiretaps, or any other modern horror absorbed this book's lessons first." --Cory Doctorow, BoingBoing
<http://boingboing.net/2003_08_01_archive.html#200444060>

"The UN officials should have read security expert Bruce Schneier's new book, Beyond Fear: Thinking Sensibly About Security in an Uncertain World. Schneier points out the dangers of inattention and wishful thinking where security is concerned." --glennreynolds.com <http://www.msnbc.com/news/856672.asp?cp1=1> (linked from Instapundit: <http://www.instapundit.com/archives/011152.php>)

"Bruce Schneier is a security guru who generally preaches common sense (a common theme in RISKS, although common sense is apparently surprisingly uncommon overall). In our time, common sense may seem absolutely heretical to people other than those of us who try to practice it. Fortunately, RISKS readers seem to be much more aware than nonreaders. For those of you who think you believe in common sense, this book will strongly reinforce your beliefs -- and will do so quite entertainingly. On the other hand, those who do not actually practice what we preach here had better read Bruce's book very carefully." --Peter Neumann, comp.risks
<http://groups.google.com/groups?...>

"Something sorely needed about 2 years ago. But, better late than never.... His stuff is _always_ great, and he really has his head screwed on straight and tight." --Hellblazer
<http://www.hellblazer.com/archives/001779.html>

My goal for this book is to appeal to a wider audience, one outside the technology community. In pursuit of that goal, I have been speaking in front of different audiences: product designers, architects, economists, the U.S. Congress, the general public.

Security is too important these days to be mysterious. It's too important to be left to the "experts." Security affects us all, and we all need to make our own security trade-offs consciously and deliberately.

It is my hope that "Beyond Fear" contributes to the debate.

Beyond Fear home page:
<http://www.schneier.com/bf.html>

Amazon's page:
<http://www.amazon.com/exec/obidos/ASIN/0387026207/...>

Crypto-Gram Reprints

Crypto-Gram is currently in its sixth year of publication. Back issues cover a variety of security-related topics, and can all be found on <http://www.schneier.com/crypto-gram.html>. These are a selection of articles that appeared in this calendar month in other years.

Special issue on 9/11, including articles on airport security, biometrics, cryptography, steganography, intelligence failures, and protecting liberty:
<http://www.schneier.com/crypto-gram-0109a.html>

Full Disclosure and the Window of Exposure:
<http://www.schneier.com/crypto-gram-0009.html#1>

Open Source and Security:
<http://www.schneier.com/...>

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

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

Licensing Computer Users

A recent Associated Press story about licensing computer users has some people believing that I am in favor of the idea.

I'm not. Period.

The idea is that users can potentially do damage with their computers, so why not force them to get licenses as we do for automobile drivers. While this is one potential way to deal with the problem of people having default security configurations and not installing their patches, I think that the damage that would do to the Information Age would be disastrous. And that it is a bad security trade-off.

It's interesting that people are taking this idea seriously, though. I think that the computer industry has painted itself into a corner. On the one hand, it has positioned computers as a mass-market consumer item. Everyone should own a computer. On the other hand, they have made computers so complex to administer that you need significant training to do it properly. One of the results of this is bad security, which we're seeing.

But I don't think the solution is to force computer users to be licensed. When I read my quote it's clear to me that I'm not saying that, but I want to correct the impression of anyone who does.

<http://www.cbsnews.com/stories/2003/09/11/tech/...>

News

An interesting, inadvertent, distributed denial-of-service. An accident, not an attacker.
<http://www.cs.wisc.edu/~plonka/netgear-sntp/>

John Poindexter has submitted his letter of resignation from DARPA.
<http://www.washingtonpost.com/ac2/wp-dyn/...>
A copy of his letter:
<http://www.washingtonpost.com/wp-srv/nation/...>

Fascinating news article about a slot-machine hacker:
<http://www.usatoday.com/tech/news/...>

Messing with the Safeway grocery story frequent-buyers card in an effort to retain privacy:
<http://www.wired.com/news/business/0,1367,59589,00.html>

Demonstration of new airport X-ray scanning technology:
<http://www.wired.com/news/images/...>

When Windows XP crashes, it asks you if you want to send a report to Microsoft. Ever wonder what happens to those reports?
<http://www.pcmag.com/article2/0,4149,1210067,00.asp>

Patching doesn't work. (I said this in 2000.)
<http://www.computerworld.com/securitytopics/...>
<http://www.computerworld.com/softwaretopics/os/...>

The U.S. Department of Justice has released "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." At least, the unclassified executive summary.
<http://www.usdoj.gov/oig/special/03-08/index.htm>

NIST report on IDSs:
<http://csrc.nist.gov/publications/nistir/...>

Decryption of a 17th century historical document:
<http://www.telegraph.co.uk/news/main.jhtml?xml=/...>

The sad, sad story of Dell's software license policy. A license that is impossible to read helps no one, neither the buyer nor the seller. It's really bad security.
<http://www.cypherpunks.ca/dell.html>

In an ever-increasing world of technology, it's important not to forget that low-tech works too. Two

people dressed as technicians walked into the "Customs cargo processing and intelligence center" at the Sydney Airport, poked around for a couple of hours, and left with a couple of servers. (Note: "ASIO" stands for Australian Security Intelligence Organization, something like the CIA.)
<http://news.ninemsn.com.au/National/story_51495.asp>
<http://www.smh.com.au/articles/2003/09/04/...>
<http://www.theregister.co.uk/content/55/32677.html>

Serious flaws in GSM cell phone encryption:
<http://www.newscientist.com/news/news.jsp?id=ns99994130>

Interesting report on the security of Diebold's voting machines. Scary stuff, especially if you consider that these are already being purchased for use in U.S. elections.
<http://avirubin.com/vote.pdf>

Computer article saying something I've said for years: the concept of perimeter defense doesn't make sense. The article uses the "submarine warfare" paradigm: attacks can come from anywhere at any time.
<http://infosecuritymag.techtarget.com/ss/...>

Face-scanning in airports -- catching terrorists as they walk by -- fails miserably in tests. The report was written in 2002, but never made public. The ACLU had to file a Freedom of Information Act request to get a copy of it.
<http://www3.gartner.com/DisplayDocument?doc_cd=117139>

Interview with Kevin Mitnick. He has a bunch of interesting things to say about the state of computer security and the circumstances of his arrest and conviction.
<http://www.itsj.com/Articles.aspx?...>

South Korea's Samsung Electronics has banned the use of camera phones in some of its factories for fear they could be used for industrial espionage.
<http://news.bbc.co.uk/1/hi/world/asia-pacific/...>

Counterpane News

Schneier is currently on a national press tour to promote "Beyond Fear." Unfortunately, the East Coast dates were all last week. Here are the upcoming radio and television appearances:

- "KARE 11 News Today," KARE-TV in Minneapolis, September 15 somewhere between 10:00 AM and 11:00 Central Time.
- "The Pete Wilson Show," radio in San Francisco, September 16 at 3:00 PM - 4:00 Pacific Time.
- "Dave Ross Show," KIRO-AM in Seattle, September 18 at 11:00 AM - 12:00 Pacific Time.
- Some show on KLAY-AM in Seattle, September 18 at 12:15 PM - 12:45 Pacific Time.
- "Extension 720," WGN-AM in Chicago, September 19 at 9:00 PM - 11:00 Central Time. I have trouble believing that this will be two full hours, but that's what's on my schedule.
- "Introspect," KPMS-FM/KYCW-AM in Seattle, September 21 at 9:00 AM - 9:15 Pacific Time.
- "9 Good News Day," KMSP-TV in Minneapolis, September 22 at 8:15 AM Central Time.
- "KARE 11 News First Edition, KARE-TV in Minneapolis, September 29 at 6:25 AM Central Time.
- "Midmorning," KNOW-FM in St. Paul, September 29 at 10:00 AM - 11:00 Central Time.

An interview with Schneier:
<http://www.cips.ca/news/national/news.asp?aID=1711>

Business Week interview with Schneier:
<http://www.businessweek.com/technology/content/...>

Interview with Schneier on WNYC's Leonard Lopate Show:
<http://www.wnyc.org/shows/lopate/episodes/09102003>
Link to audio file:
<http://stream.realimpact.net/rihurl.ram?...>

Interview with Schneier on WAMU's Kojo Nnamdi Show:
<http://www.wamu.org/kojo/index.html>
Link to audio file:

<http://www.wamu.org/ram/2003/k1030911.ram>

PRI's "Marketplace" Interview with Schneier:
<http://www.marketplace.org/morning_report/2003/09/...>
Link to audio file:
<http://www.marketplace.org/play/audio.php?media=/...>

Schneier is speaking at the International Conference on Advanced Technologies for Homeland Security, at the University of Connecticut, on September 25th.
<http://www.engr.uconn.edu/icaths/>

Schneier is speaking at ToorCon in San Diego on September 27th.
<http://www.toorcon.org/>

Security Notes from All Over: Hats in Banks

A Birmingham, Alabama, bank is prohibiting its customers from wearing hats inside its branches. The idea is to improve security against bank robberies.

I guess the ideas is that a bank robber without a hat will show up better on security cameras. This makes a little bit of sense, until you start thinking about how it might work in practice.

Someone walks in with a hat. He walks up to a teller and announces a stick-up. Meanwhile, a security guard calls out: "Excuse me, sir. Can you remove your hat." I'll bet the teller will press her little "alarm" button a whole lot quicker than that.

Maybe a hat will tip off bank security quicker, enabling them to react in time. But what about bank robbers in ski masks? Didn't that already arouse suspicion? Why didn't that work? And if it didn't work for ski masks, why will it work for hats?

And the false alarm rate must be horrible. People walk into buildings wearing hats all the time. Almost none of them are bank robbers. How many times a day will security guards say "please remove your hat" before they become conditioned to the fact that no one wearing a hat is a bank robber?

Ski masks, presumably, have a much lower false alarm rate.

But let's assume, for the moment, that there is this breed of hatted criminal that can be foiled by a ban on hats. Why can't they dress up as "a nun, an Orthodox Jew, a Sikh in a turban or a burqa-clad Muslim woman"? Those groups are specifically exempted from the hat restriction.

All this aside, the rule has a little bit of security benefit. Some bank robbers might decide to rob a different bank because the hat rule is a bit too annoying. But bank robbers relying on speed are unlikely to care, and bank robbers relying on stealth are unlikely to care.

Security is always a trade-off: you have to balance the security you receive with what you give up in exchange. This rule is likely to annoy and inconvenience customers, while doing little to improve bank security. Hardly a good trade-off in the end.

And it certainly would never work where the winters are cold. Hats are not just fashion; sometimes they're survival gear. Ski masks, too.

<http://www.kansascity.com/mld/kansascity/business/...>

Benevolent Worms

A week after Blaster infected computers across the Internet, a "benevolent" worm started spreading in its wake. Called Blast.D or Nachi, it infects computers through the same vulnerability that Blaster did. When it infects a computer, it finds and deletes Blaster, and then applies the Microsoft patch to the computer so that the vulnerability is closed and Blaster cannot reinfect. It then scans the network for other infected machines and repairs them, too.

Blast.D represents a cool-sounding idea, and one that surfaces from time to time. Why don't we use worms (or viruses) for good instead of evil? Worms contain two parts: a propagation mechanism and a payload. The propagation mechanism spreads the code from computer to computer. The payload is what it does once it gets to a computer. As long they're infecting everyone's computer, why don't we use them to patch vulnerabilities, update systems, and improve security? Why don't we create worms with beneficial payloads, and then let them propagate unchecked?

This is tempting for several reasons. One, it's poetic: turning a weapon against itself. Two, it lets ethical programmers share in the fun of designing worms. And three, it sounds like a promising technique to solve one of the nastiest online security problems: patching or repairing computers' vulnerabilities.

Everyone knows that patching is in shambles. Users, especially home users, don't do it. The best patching techniques involve a lot of negotiation, pleading, and manual labor...things that nobody enjoys very much. Beneficial worms look like a happy solution. You turn a Byzantine social problem into a fun technical problem. You don't have to convince people to install patches and system updates; you use technology to force them to do what you want.

And that's exactly why it's a terrible idea. Patching other people's machines without annoying them is good; patching other people's machines without their consent is not. A worm is not "bad" or "good" depending on its payload. Viral propagation mechanisms are inherently bad, and giving them beneficial payloads doesn't make things better. A worm is no tool for any rational network administrator, regardless of intent.

A good software distribution mechanism has the following characteristics:
1) People can choose the options they want.
2) Installation is adapted to the host it's running on.
3) It's easy to stop an installation in progress, or uninstall the software.
4) It's easy to know what has been installed where.

A successful worm, on the other hand, runs without the consent of the user. It has a small amount of code, and once it starts to spread, it is self-propagating, and will keep going automatically until it's halted.

These characteristics are simply incompatible. Giving the user more choice, making installation flexible and universal, allowing for uninstallation -- all of these make worms harder to propagate. Designing a better software distribution mechanism, makes it a worse worm, and vice versa. On the other hand, making the worm quieter and less obvious to the user, making it smaller and easier to propagate, and making it impossible to contain, all make for bad software distribution.

All of this makes worms easy to get wrong and hard to recover from. Experimentation, most of it involuntary, proves that worms are very hard to debug successfully: in other words, once worms starts spreading it's hard to predict exactly what they will do. Some viruses were written to propagate harmlessly, but did damage -- ranging from crashed machines to clogged networks -- because of bugs in their code. Many worms were written to do damage and turned out to be harmless (which is even more revealing).

Intentional experimentation by well-meaning system administrators proves that in your average office environment, the code that successfully patches one machine won't work on another. Indeed, sometimes the results are worse than any threat of external attack. Combining a tricky problem with a distribution mechanism that's impossible to debug and difficult to control is fraught with danger. Every system administrator who's ever distributed software automatically on his network has had the "I just automatically, with the press of a button, destroyed the software on hundreds of machines at once!" experience. And that's with systems you can debug and control; self-propagating systems don't even let you shut them down when you find the problem. Patching systems is fundamentally a human problem, and beneficial worms are a technical solution that doesn't work.

On the other hand, automatic update functions are sometimes a good idea. Corporate network administrators often hate them, for all the right reasons, but there's no other way to patch many home-user systems. There are legions of computer users who cannot administer their own computers. For them, I strongly recommend automatic updates. It won't be perfect. It'll occasionally break their system. And sooner or later someone will figure out how to install malware using the automatic update system. But it's a much better solution than the alternative, which is that these systems never get patched.

(An earlier version of this essay was written with Elizabeth Zwicky in 2000, and appeared in "The Industry Standard.")

Blast.D Stories:
<http://www.washingtonpost.com/ac2/wp-dyn/...>
<http://www.computerworld.com/printthis/2003/...>
<http://news.com.com/2102-1002_3-5065117.html?...>

California's Security-Breach Disclosure Law

California's Security Breach Information Act has been in effect since July 1. As reported by the press, the point of the law is to force companies to disclose security breaches to those affected by them. Supposedly, if your credit card number is stolen from some company's database, that company has to inform you of that fact -- at least if you live in California. The idea is twofold. One, consumers will be able to make smarter security decisions because more information is made public. And two, companies wanting to avoid embarrassment will spend more money improving their computer security.

It's a really good idea, but the law is so badly written as to be a sham. There are loopholes large enough to hide any security breach.

1) It applies only to data theft that includes a person's name and one of the following: a SSN, a driver's license number, or financial account number plus requisite PINs or passwords. A database of names and SSNs would be covered. A database of names, debit card numbers, and PINs would be covered. A database of SSNs, debit card numbers, and PINs would not. A database of names and credit card numbers, without PINs, would not. Neither would a credit report or a financial statement, as long as there was no SSN on it.

2) It does not apply to the theft of any other data. No disclosure is required if someone steals a database of sensitive health information. No disclosure is required if someone steals a database of purchasing history. No disclosure is required if someone steals video rental records, book purchasing history, personal e-mails, court proceedings, criminal records, or any other personal information.

3) It only applies if either the name or the other data isn't encrypted. This kind of makes sense, until you realize that the method of encryption isn't specified. Even if the encryption is breakable, even if the encryption key is stolen with the data, even if the database is protected by ROT-13, no disclosure is required.

4) Disclosure can be delayed "if a law enforcement agency determines that the notification will impede a criminal investigation." At least the determination has to be made by the police, and not by the attacked company, but I'm sure it won't be very difficult to find a local law enforcement agency willing to make that determination.

Forcing companies to disclose when their customers' private information has been compromised is a good idea, but unfortunately this law is so badly written that it can be safely ignored. According to a Computerworld article, one attorney said: "What some companies are thinking of doing is assigning a random number to a customer name in one database and linking that random number to the personally identifiable information stored in a completely separate database." That might be following the letter of the law, but it is certainly against the spirit.

Here's just one example. Last month Daniel Baas was arrested for breaking into, and stealing customer data from, the Acxiom Corp. database. Acxiom is a company that analyzes consumer databases for other companies, including Microsoft, IBM, AT&T and General Electric. They have lots of data on lots of California residents. Shouldn't Acxiom have been required to send its California customers an embarrassing confession? Isn't this exactly the kind of security breach that the law should cover? The fact that Acxiom felt no compulsion under the law attests to its ineffectiveness.

Text of the California law:
<http://www.privacyprotection.ca.gov/code/...>

A nice analysis of the law and its implications:
<http://www.eweek.com/article2/0,3959,1191924,00.asp>

Senator Diane Feinstein introduced a Federal bill is modeled after the California law:
<http://www.infoworld.com/article/03/07/18/...>
Text of the bill:
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?...>

Acxiom hack:
<http://www.theregister.co.uk/content/55/32278.html>
<http://www.securityfocus.com/news/6733>

Correction

In the August 15 Crypto-Gram, I erroneously attributed the following letter to Andy Brown <logic@warthog.com>:

"Subject: "I haven't a clue, really"

"I am writing with regard to the message in the Letters-section of your Crypto-Gram of 15 July, 2003, which contains the header, 'From: Somewhere / Subject: I haven't a clue, really'. In a preamble to this message, you assert, 'I reprint it here solely for entertainment purposes.'

"With respect, I must tell you that I did not find this letter entertaining in the slightest degree; on the contrary, I found it disturbing in its content, and annoying inasmuch as you should have chosen to publicize it. Perhaps, as you intimate, the writer of this missive may be delusional. If that were the case, surely s/he would be deserving of compassion -- but hardly of public display; and in any event, it is anything but yours (or mine) to arrogate to ourselves the role of armchair-analyst omniscience. ('... delusional paranoia...'? That is an extremely powerful term, which even the 'experts' appear to have trouble with.)"

The author of this letter was, in fact, Dr. Robert Taylor <RobertTaylor@SpamCop.net>.

Apologies to both people.

Comments from Readers

From: Bruce McNair <bmcnair@novidesic.com>
Subject: How to Fight

I think it's horrible that someone would intentionally provide incorrect information to government agencies or corporate data gatherers as Richard suggests. I know that when the State of New Jersey asks me for my SSN on my driver's license renewal or vehicle registrations, I wouldn't think of giving them bad information. Of course, I am generally in a hurry, so my handwriting may not be the most legible...

And although I do occasionally do get my merds wixed up, I hardly ever accidentally swap digits. I am especially careful to enter the proper numbers -- I wouldn't want to compound the problem deciphering my writing. But my numerals do tend to look like the Greek lower case letters my professors loved to use. You know: eta and zeta, and the others that looked like snakes in abdominal spasm.

Just like the checkout clerks that insist on capturing your credit card signature electronically, the DMV clerks are not concerned with what gets written down, just as long as they can show their boss that they didn't let someone by without filling in the box.

By the way, what are the Roman numerals to signify numbers on the order of 10**8? I have verified that the DMV forms state no requirement for legibility, but I don't see that they require SSNs be provided in Arabic numerals, either.

From: Pekka Pihlajasaari <pekka@data.co.za>
Subject: How to Fight

But incitement to a felony almost certainly is an offence and should not be too difficult to prove. I agree that the path of least resistance is often the submission of inaccurate data, but I do not think that deliberately or otherwise altering the data corrects the underlying expectation on the part of the service provider and certainly adds an incentive to demand a copy of the underlying identity to confirm the correctness of the information.

I was leaving a mall car park yesterday and noticed that I had lost the parking voucher after it had been validated by the pay terminal. I happened to have the optional payment receipt and showed this as proof of payment in an effort to be allowed out. I declined to provide more than the minimum identification to the security personnel that I felt was appropriate and was prevented from leaving.

The security manager said that payment receipts could be drawn after the fact, and they could be used to avoid payment of the fee after a long-term period of parking. The ostensible reason for requesting the documentation was to counter the widely understood risk of car theft (there are often signs at mall entrances requesting that owners not leave the voucher in their cars). He stated that this was a measure that demonstrated that they were not negligent and would thus maintain their declaration of liability disclaimer.

In the end the police came out to the parking lot and confirmed my identity against the registered owner of the vehicle (which happened to be mine). I wasted about 90 minutes and possibly the security manager will think longer before making a customer irate and having a car blocking an exit lane.

From: "Balog Pal" <pasa@lib.hu>
Subject: Photo-ID Verification

> Security Notes from All Over: Photo-ID Verification

> Employee: This is my face -- I am wearing it on my head.
>
> Security Guard: I need another piece of ID with a picture on it to
> compare against this one.
>
> This is a great story, because it illustrates how completely
> clueless security guards can be about how security really works.

This story made me a really good laugh. However I can't agree with all your comments. The actual guard may have been clueless, and his arguments make that more likely. But if I were that guard, I'd definitely ask an ID too.

Otherwise it would allow a pretty cheap attack. If I have a face enough resembling an employee, all I need to know his ID number. Not something secret at all. Then I come with the same story about the lost token and get in. If a driver's license is requested, the guard can be (more) sure I really am that employee by matching the name on the presented ID card. To make the attack work I have at least to gather enough personal data on the targeted employee, and make a fake ID. Or steal it.

From: "Anderson, Kevin" <kevina@datapower.com>
Subject: Photo-ID Verification

No pun intended, but on the surface the guard seems foolish, but I can imagine that the "employee" may really be someone who had hacked into the company site the night before and simply switched his photo for the one that should be there. Another form of authentication that matched name and photo and address would be a good security check. In this case the guard should ALWAYS check for an ID to verify against the company's records based on policies set by others who are hopefully smarter than he is about security. It is better that the guard mindlessly goes through the "security checklist" than to start determining which steps can be dismissed on occasion. If the security guard was a firewall and skipped some filter processing sometimes we'd call it a bug and fix it.

From: "Heber Watts" <hewatts@comcast.net>
Subject: National Crime Information Center (NCIC) Database Accuracy

I recently read your article; National Crime Information Center (NCIC)
Database Accuracy in your April 15, 2003 edition of Crypto-Gram. The only error that I found in your article is as follows:

You state that;

1. "The Privacy Act of 1974 requires the FBI to make reasonable efforts to ensure the accuracy and completeness of the records in this database. Last month, the Justice Department exempted the system from the law's accuracy requirements."

2. "This isn't just bad social practice, it's bad security. A database with more errors is much less useful than a database with fewer errors, and an error-filled security database is much more likely to target innocents than it is to let the guilty go free."

These statements appear to assume that there is no oversight to the accuracy of information entered into the database. The problem with the Privacy Act of 1974 requirements was that nobody could foresee the volume of information that would be entered into the NCIC database. You are absolutely correct that the database is enormous and it was the enormity of the database that proved to be the issue. It was impossible for the FBI to insure that accuracy of information entered by the more than 80,000 participating agencies. The burden of insuring the accuracy now falls to the individual States. With that responsibility comes the liability burden as well.

There is no way that a single centralized agency can insure the accuracy of the information contained in such a large data base. Additionally, police officers do not arrest based on the database proclaiming one's "guilt." Warrants provide "probable cause to arrest." For example, a Maryland police officer stops a motorist, makes an NCIC inquiry and receives a "hit," the database says the individual is wanted by California. The police officer will detain the motorist and the Maryland police terminal operator will immediately contact the California agency holding the warrant. The California agency has a specific amount of time to confirm that the warrant is valid and that they will travel to Maryland to transport the wanted person back to California (extradite). If California is unwilling to transport the wanted person back to California or cannot "validate" the warrant within the time specified, the wanted person is released, no arrest is made.

The individual participating agencies are required to have systems in place to confirm the accuracy of the information they enter into the system. In addition, NCIC information has very limited evidentiary value. Its greatest evidentiary value comes in cases such as in the initial example. If the California warrant for the motorist could not be validated or California was unwilling to extradite, and the motorist decided to sue the Maryland police officer claiming false arrest, the Maryland officer's defense would be that he/she only detained the person long enough to validate the warrant that California placed in the NCIC system. The Maryland police officer would be protected because his/her actions were reasonable and prudent. In this case, California has the responsibility to insure that every warrant is valid and to inform the system far they are willing to travel to retrieve the wanted person. They are technically liable for maintaining an invalid warrant or not clearly stating how far they will travel to retrieve the wanted person.

This is not exactly efficient in the eyes of information technologists, but it is an excellent safeguard. People are not detained for outrageous periods of time nor are they arrested erroneously on a large scale because of the safeguards. There are still various errors such as typographical errors, but those issues can be confirmed through subsequent investigation. The system is not perfect, but it is not wide open, either.

From: Saul Backal <saul@meganet.com>, Ralph Lotkin <lotkinlaw@aol.com>
Subject: Meganet

Meganet Corporation is the inventor and owner of encryption technology referred to as VME--Virtual Matrix Encryption, a 1 million-bit symmetric encryption algorithm that was granted U.S. Patent No. 6,219,421 on April 17, 2001. Despite this patent grant, and the fact that major customers exist for the technology worldwide, certain individuals in the "crypto-community" still express disdain for Meganet Corporation and belittle VME without ever having taken a serious look at the technology.

In our view, both Meganet Corporation and VME have been misjudged. All we ask is that you give our technology a serious look. The only outcome we desire is that the crypto-community judges Meganet and VME objectively.

Why has there been criticism? The first answer is because we made some unintended business mistakes. And, for its part, the community rushed to judgment relying upon those errors rather than upon an objective and thorough analysis on the merits.

Meganet Corporation started as a two-man operation. The technology was great, but there was no professional marketing force so, not having an experienced, businessman on board, we naively selected the wrong marketing company--a company that presented itself to be a leader in marketing but was not what it claimed. The VME technical documentation was broken into pieces to create marketing documents in an industry they did not know or understand and, of course, the results were tragic. People who read the material disparaged VME without ever seeing it or evaluating it thoroughly. The sad fact is that, to our knowledge, not one of those experts ever looked at our algorithm, the source code, the U.S. Patent, or even called us.

So, what did Meganet do wrong? We employed the wrong marketing team with no knowledge of the industry or technology, a mistake many new startup companies make. With the benefit of hindsight, that hopefully has been corrected.

Second, Meganet was faulted for its decision not to publicly disclose the source code for VME. However, we did this to preserve our ability to make a profit selling our technology and to prevent others from making illegal copies or incorporating our intellectual property into their own. In Applied Cryptography, Bruce Schneier claims that such non-disclosure is "security through obscurity" and is unacceptable. Nevertheless, when discussing Professor

Shamir's RC4 and RC5 algorithms, Schneier did not hold Shamir to the same disclosure requirement; apparently because Shamir is a respected professor and therefore was deemed exempt. RC4 and RC5 became mainstream algorithms. Why were the algorithm kept private? We believe it was because Professor Shamir sought to earn a profit on the sale of his technology, unlike RSA, that in the first eight years of its existence saw the whole world use their technology royalty free, even though they had a patent in place. To our knowledge, it took RSA approximately two decades before it began earning a decent profit from their technology, while RC4 and RC5 earned a profit quickly.

Thus, we do not agree that our refusal to disclose source code was, or continues to be, a mistake. Importantly, the VME application has been available for free (in EVAL versions) for 7 years. So again we ask, "Did any of the experts ever look at the patent and algorithm materials thoroughly"? Did anyone ever contact us? To the best of our knowledge, the answer is, "No".

Perhaps it is easier to claim that VME is "snake oil" than it is to analyze a new approach to encryption. Furthermore, disassembly of the VME executable code, which is a scant 160KB, should be a simple task for encryption experts. If "security through obscurity" is, per se, bad, how is it that an industry filled with experts cannot simply decompile a 160KB executable code to prove that VME is "snake oil" or solve repeated challenges to do so?

Indeed, many have complained about the challenges we issued periodically to hackers and encryption enthusiasts. Those challenges were attacked as "unfair", "lies", and "unfounded". We disagree. We gave the application that encrypted the file. We also gave the cyphertext file and, at the end of the challenge, each and every participant was able to enter the solution published on our website and decrypt the file themselves on their own computer to prove that there was indeed a solution for the challenge. Nothing was missing. Isn't this how credible government and corporate security are supposed to work?

Finally, criticism has been focused on the basic claim of our technology - one million bits. What an attractive opportunity to poke fun, indeed the so-called first sign of "snake oil". If it is so bad, then how is it that the algorithm ridiculed by the technology community has now been acquired and is available for use in thousands of U.S. Government computers and even by more corporate users worldwide? Why did they buy the technology? Because they apparently concluded that VME is one of the most competitively priced and strongest commercially off the shelf symmetric encryption technologies available.

Where do we go from here? We offer the following suggestions:

First, check out VME for yourself--don't simply accept or parrot others' opinions. Not understanding a phrase does not mean that it is incorrect or meaningless. Better yet, if you wish more information, just call us.

Second, participate in the "Crypto-Community Challenge" that will be posted on our website and will start on September 15 and will last 6 months. We will provide an encrypted file and the application that encrypted it and will decrypt the solution on your own computer, free of charge. If successful, the winner will be given a large monetary prize. We invite--better yet--we urge Bruce Schneier and Counterpane to organize the entire crypto-community into an effective challenge-breaking attempt, just like the one that was undertaken to respond to the RSA challenges. Be thorough and see for yourself if VME is truly what it claims to be.

As a constantly evolving technology community, we owe it to ourselves to be professional and to examine new and emerging approaches on their merits. Meganet seeks only this minimal fairness. We hope this brief communication will help start that reexamination.

Thank you for your attention.

CRYPTO-GRAM is a free monthly newsletter providing summaries, analyses, insights, and commentaries on security: computer and otherwise. Back issues are available on <http://www.schneier.com/crypto-gram.html>.

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>.

CRYPTO-GRAM is written by Bruce Schneier. Schneier is the author of the best sellers "Beyond Fear," "Secrets and Lies," and "Applied Cryptography," and an inventor of the Blowfish and Twofish algorithms. He is founder and CTO of Counterpane Internet Security Inc., and is a member of the Advisory Board of the Electronic Privacy Information Center (EPIC). He is a frequent writer and lecturer on security topics. See <http://www.schneier.com>.

Counterpane Internet Security, Inc. is the world leader in Managed Security Monitoring. Counterpane's expert security analysts protect networks for Fortune 1000 companies world-wide. See <http://www.counterpane.com>.

later issue
earlier issue
back to Crypto-Gram index