

February 15, 2003

Crypto-Gram Newsletter

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.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.

Copyright (c) 2003 by Counterpane Internet Security, Inc.

In this issue:

- Locks and Full Disclosure
- Crypto-Gram Reprints
- Random Notes on the SQL Slammer
- The Doghouse: Meganet
- News
- Counterpane News
- Security Notes from All Over: Anti-Fraud Security at Banks
- The Importance of Authentication
- Comments from Readers

Locks and Full Disclosure

The full disclosure vs. bug secrecy debate is a lot larger than computer security. In January, security researcher Matt Blaze published a paper describing a new attack against door locks. The specific locks are "master key systems," the sorts that allow each person to have a key to his own office and the janitor to have a single key that opens every office. The specific attack is one where a person with an individual office key can make himself a master key. The specifics are interesting, and I invite you to read the paper. It turns out that the ways we've learned to conceptualize security and attacks in the computer world are directly applicable to other areas of security -- like door locks. But the most interesting part of this entire story is that the locksmith community went ballistic after learning about what Blaze did.

The technique was known in the locksmithing community and in the criminal community for over a century, but was never discussed in public and remained folklore. Customers who bought these master key systems for over a century were completely oblivious to the security risks. Locksmiths liked it that way, believing that the security of a system was increased by keeping these sorts of vulnerabilities from the general population.

The bug secrecy position is a lot easier to explain to a layman. If there's a vulnerability in a system, it's better not to make that vulnerability public. The bad guys will learn about it and use it, the argument goes. Last month's SQL Slammer is a case in point. If the hacker who wrote the worm hadn't had access to the public information about the SQL vulnerability, maybe he wouldn't have written the worm. The problem, according to this position, is more the information about the vulnerability and less the vulnerability itself.

This position ignores the fact that public scrutiny is the only reliable way

to improve security. There are several master key designs that are immune to the 100-year-old attack that Blaze rediscovered. They're not common in the marketplace primarily because customers don't understand the risks, and because locksmiths continue to knowingly sell a flawed security system rather than admit and then fix the problem. This is no different from the computer world. Before software vulnerabilities were routinely published, vendors would not bother spending the time and money to fix vulnerabilities, believing in the security of secrecy. And since customers didn't know any better, they bought these systems believing them to be secure. If we return to a world of bug secrecy in computers, we'll have the equivalent of 100-year-old vulnerabilities known by a few in the security community and by the hacker underground.

That's the other fallacy with the locksmiths' argument. Techniques like this are passed down as folklore in the criminal community as well as in the locksmithing community. In 1994, a thief made his own master key to a series of safe-deposit boxes and stole \$1.5 million in jewels. The same thing happens in the computer world. By the time a software vulnerability is announced in the press and patched, it's already folklore in the hacker underground. Attackers don't abide by secrecy agreements.

What we're seeing is a culture clash; it's happening in many areas of security. Attorney General Ashcroft is working to keep details of many antiterrorism countermeasures secret so as not to educate the terrorists. But at the same time, the people -- to whom he is ultimately accountable -- would not be allowed to evaluate the countermeasures, or comment on their efficacy. Security couldn't improve because there'd be no public debate or public education. Whatever attacks and defenses people learn would become folklore, never spoken about in the open but whispered from security engineer to security engineer and from terrorist to terrorist. And maybe in 100 years someone will publish an attack that some security engineers knew about, that terrorists and criminals had been exploiting for much of that time, but that the general public had been

blissfully unaware of.

Secrecy prevents people from assessing their own risk. For example, in the master key case, even if there weren't more secure designs available, many customers might have decided not to use master keying if they knew how easy it was for an attacker to make his own master key.

I'd rather have as much information as I can to make an informed decision about security. I'd rather have the information I need to pressure vendors to improve security. I don't want to live in a world where locksmiths can sell me a master key system that they know doesn't work or where the government can implement security measures without accountability.

Blaze's home page for his research:

<<http://www.crypto.com/masterkey.html>>

The paper itself:

<<http://www.crypto.com/papers/mk.pdf>>

The reaction to the paper:

<<http://www.crypto.com/papers/kiss.html>>

News articles on the research:

<<http://www.nytimes.com/2003/01/23/business/23LOCK.html>>

<<http://www.mail-archive.com/...>>

Previous web references to Blaze's technique:

<<http://sethf.com/infothought/blog/archives/000164.html>>

Jewel theft using the master key vulnerability:

<<http://www.nbc4columbus.com/news/1921563/detail.html>>

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.

Microsoft and "Trustworthy Computing":

<http://www.schneier.com/crypto-gram-0202.html#1>

Judging Microsoft:

<http://www.schneier.com/crypto-gram-0202.html#2>

Hard-drive-embedded copy protection:

<http://www.schneier.com/crypto-gram-0102.html#1>

A semantic attack on URLs:

<http://www.schneier.com/crypto-gram-0102.html#7>

E-mail filter idiocy:

<http://www.schneier.com/crypto-gram-0102.html#8>

Air gaps:

<http://www.schneier.com/crypto-gram-0102.html#9>

Internet voting vs. large-value e-commerce:

<http://www.schneier.com/crypto-gram-0102.html#10>

Distributed denial-of-service attacks:

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

Recognizing crypto snake-oil:

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

Random Notes on the SQL Slammer

The Internet had its first big worm epidemic since Nimda: the Sapphire

Worm, aka SQL Slammer. Normally, I wouldn't bother mentioning this worm. It's news, but there are no real lessons to learn from the event. But there's an interesting Microsoft twist. During the days of the attack, Microsoft tried to deflect any blame by claiming that they issued a patch for the vulnerability six months previously, and that the only affected companies were the ones who didn't keep their patches up to date. A couple of days later, news leaked that Microsoft's own network was hit pretty badly by the worm because they didn't patch their own network.

For a couple of years now I've been saying that the idea that we can achieve network security by finding and patching vulnerabilities in the field is fatally flawed. I don't blame Microsoft sysadmins for not having their patches up to date -- no one does -- but I don't like the hypocrisy out of the company.

The SQL Slammer worm also reopened the full disclosure debate. Microsoft announced the vulnerability in July 2002, at the same time they released the patch. A few days later, David Litchfield published exploit code that demonstrated how the vulnerability could be used to break into systems. January's SQL Slammer worm used that exact code. Some point to that and say that Litchfield should not have released the code, while others correctly say that the code wasn't hard to write, and that the worm author could have easily written it himself.

An amusing, but irrelevant, incident: A week after the worm, I was invited to speak about it live on CNN. The program was eventually preempted by the Columbia tragedy, but not before the CNN producers invited Microsoft to appear on the segment with me. Microsoft's spokesman -- I don't know who -- said that the company was unwilling to appear on CNN with me. They were willing to appear before me, they were willing to appear after me, but they were not willing to appear with me. Seems that it is official Microsoft corporate policy not to be seen in public with Bruce Schneier.

The best technical write-up of the worm and how it propagated (very

interesting reading):

<<http://www.silicondefense.com/research/sapphire/>>

Microsoft's internal network problems from the worm:

<<http://www.theregister.co.uk/content/56/29073.html>>

<<http://news.com.com/2100-1001-982305.html>>

<<http://www.cnn.com/2003/TECH/biztech/01/28/...>>

<<http://www.nytimes.com/2003/01/28/technology/...>>

Here's my essay on the patch treadmill from two years ago:

<<http://www.schneier.com/crypto-gram-0103.html#1>>

Microsoft's original security alert:

<<http://www.microsoft.com/technet/treeview/...>>

Litchfield's comments on the similarity between his code and the worm:

<<http://groups.google.com/groups?...>>

Korean civic group considers suing Microsoft:

<<http://times.hankooki.com/lpage/nation/200302/...>>




The Doghouse: Meganet

Back in 1999 I wrote an essay about cryptographic snake oil and the common warning signs. Meganet's Virtual Matrix Encryption (VME) was a shining example. It's four years later and they're still around, peddling the same pseudo-mathematical nonsense, albeit with a more professional-looking website. I get at least one query a month about these guys, and recently they convinced a reporter to write an article that echoes their nonsensical claims. It's time to doghouse these bozos, once and for all.

First, an aside. If you're a new reader, or someone who doesn't know about cryptography, this is going to seem harsh. You might think: "How does he KNOW that this is nonsense? If it's so bad, why can't he break

it?" That's actually backwards. In the world of cryptography, we assume something is broken until we have evidence to the contrary. (And I mean evidence, not proof.) Everything Meganet writes clearly indicates that they haven't the faintest idea about how modern cryptography works. It's as if you went to a doctor who talked about bloodletting and humors and magical healing properties of pyramids. Sure, it's possible that he's right, but you're going to switch doctors. Two essays of mine at the bottom of this section, one on snake oil and the other on amateur cipher designers, will help put this into context.

Back to Meganet. They build an alternate reality where every cryptographic algorithm has been broken, and the only thing left is their own system. "The weakening of public crypto systems commenced in 1997. First it was the 40-bit key, a few months later the 48-bit key, followed by the 56-bit key, and later the 512 bit has been broken..." What are they talking about? Would you trust a cryptographer who didn't know the difference between symmetric and public-key cryptography? "Our technology... is the only unbreakable encryption commercially available." The company's founder quoted in a news article: "All other encryption methods have been compromised in the last five to six years." Maybe in their alternate reality, but not in the one we live in.

Their solution is to not encrypt data at all. "We believe there is one very simple rule in encryption  - if someone can encrypt data, someone else will be able to decrypt it. The idea behind VME is that the data is not being encrypted nor transferred. And if it's not encrypted and not transferred  there is nothing to break. And if there's nothing to break  - it's unbreakable." Ha ha; that's a joke. They really do encrypt data, but they call it something else.

Reading their Web site is like reading a litany of snake-oil warning signs and stupid cryptographic ideas. They've got "proprietary technology." They've got one-million-bit keys. They've got appeals to new concepts:

"It's a completely new approach to data encryption." They've got a "mathematical proof" that their VME is equal to a one-time pad. A mathematical proof, by the way, with no mathematics: they simply show that the encrypted data is statistically random in both cases. (The "proof" is simply hysterical to read; summarizing it here just won't do it justice.)

They've got pseudo-scientific gobbledygook galore, including paragraphs like this: "Stated simply, the content of the message is not sent with the encrypted data. Rather, the encrypted data consists of pointers to locations within a virtual matrix, a large (infinitely large in concept), continuously changing array of values." I just love stuff like this. It almost just barely makes sense. It's as if someone took a cryptography book, had it machine-translated from language to language to language, and then tried to write similar-sounding text. Some of the words and phrases are scientific, but the paragraph makes no sense. (Although, sadly, their stuff looks very much like the virtual one-time pad that TriStrata came up with some years ago.)

They have unfair cracking contests and challenges, unsubstantiated claims, outright lies, and a weird "evaluation" from one professor and even weirder "experimental results" from another. It's every snake-oil warning sign in the book in one convenient-to-make-fun-of place.

Unfortunately, this stuff seems to have continued to hoodwink buyers. According to a press release on their Web site, the U.S. Department of Labor recently gave them \$4M. Various smaller companies are supposedly using this stuff. SC Magazine gave them a five-star rating, for goodness' sake! I am amazed at the sheer stubbornness that can be exhibited by a company that simply refuses to accept reality.

Another quote from the news article: "Most of the encryption community called our product snake oil. Everyone competed to throw stones at us and didn't bother trying to understand the product." What does Meganet expect? Most snake oil is subtly bad; their marketing is so over-the-top

it's entertaining, their "science" is so eccentric it's ridiculous, and their claims are so laughable it's dangerous.

Meganet's technology Web site:

<<http://www.meganet.com/Technology/default.htm>>

Funny news article on Meganet:

<[http://www.israel21c.org/bin/en.jsp?...>](http://www.israel21c.org/bin/en.jsp?...)

My original snake-oil essay:

<[http://www.schneier.com/...>](http://www.schneier.com/...)

My "Memo to the Amateur Cipher Designer" essay:

<[http://www.schneier.com/...>](http://www.schneier.com/...)

News

The U.S. shut down Somalia's Internet, but it was a low-tech attack:

<<http://news.bbc.co.uk/1/hi/world/africa/1672220.stm>>

People don't erase personal information from their hard drives before selling them:

<<http://rss.com.com/2100-1040-980824.html>>

<[http://sfgate.com/cgi-bin/article.cgi?f=/news/...>](http://sfgate.com/cgi-bin/article.cgi?f=/news/...)

Essay by Whitfield Diffie on the relationship between openness and security:

<<http://news.com.com/2010-1071-980462.html>>

The ACLU has just published a new report, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society."

<<http://www.aclu.org/Privacy/Privacylist.cfm?c=39>>

Many Sprint DSL modems are configured with the password "1234":

<<http://www.wired.com/news/infostructure/...>>

Anyone can get their own .mil domain.

<<http://212.100.234.54/content/55/29026.html>>

A company that makes automatic garage-door openers is using the DMCA to halt the distribution of a competing product:

<<http://www.extremetech.com/article2/...>>

This Internet Security Threat Report is filled with interesting statistics and information. I recommend reading it. (Symantec requires you to give them some personal information before they'll let you download the report, presumably so they can market to you, but you can make up information on the form.)

<<http://enterprisesecurity.symantec.com/Content.cfm?...>>

Tips on implementing cryptography in systems:

<<http://www.cs.auckland.ac.nz/~pgut001/pubs/...>>

Richard Clarke is leaving the position of White House Security Czar, and Howard Schmidt is replacing him. The following article repeats the rumor that Clarke's stand on protecting personal privacy put him at odds with the Bush administration.

<<http://www.washingtonpost.com/wp-dyn/articles/...>>

Good essay on software liabilities:

<<http://www.bos.frb.org/economic/nerr/rr2002/q3/...>>

The Senate Committee on National Security and Defense in Canada recently released a report on the new airport security measures. It's well written and sensible, unlike a lot of security reports I read.

<<http://www.parl.gc.ca/37/2/parlbus/commbus/senate/...>>

Buyer doesn't trust seller, so he uses an escrow site to protect himself

from fraud. But what happens if the escrow site is untrustworthy?

<<http://www.msnbc.com/news/854552.asp?0cl=cR>>

Lawyers as a threat to computer security:

<<http://www.osopinion.com/perl/story/20581.html>>

Interesting interview with Kevin Mitnick:

<<http://interviews.slashdot.org/article.pl?sid=03/02/...>>

The U.S. military is developing rules for cyber-warfare:

<<http://www.vnunet.com/News/1138573>>

<<http://www.washingtonpost.com/wp-dyn/articles/...>>

<http://www.gcn.com/vol1_no1/daily-updates/21122-1.html>

Send your suggestions for the World's Most Stupid Security Measure.

Awards will be given.

<<http://www.privacyinternational.org/activities/...>>

<<http://www.theregister.co.uk/content/55/29279.html>>

Good essay on the dangers of identity theft, and ideas on how to fix the problem:

<<http://www.businessweek.com/technology/content/...>>

Forensics on Windows:

<<http://online.securityfocus.com/infocus/1661>>

<<http://online.securityfocus.com/infocus/1665>>

Interesting cyber-extortion scam. Innocent user visits Web site. Web server downloads files into innocent's computer. Server owner then sends innocent e-mail, telling him that he has child porn on his computer and that he will inform various authorities if the innocent doesn't pay.

<<http://www.csoonline.com/read/020103/undercover.html>>

Counterpane News

Hot on the heels of our \$20M funding, Counterpane has announced two additions to our executive team: Paul Stich as President and COO, and Rahoul Seth as CFO. Tom Rowley remains at the helm as CEO.

<<http://www.counterpane.com/pr-stich.html>>

<<http://www.counterpane.com/pr-seth.html>>

Security Notes from All Over: Anti-Fraud Security at Banks

Banks generally don't verify signatures on checks and credit card charges. Instead, they rely on the customer to notify them about fraudulent transactions and to then investigate. The bank assumes debits are correct unless the customer complains. The costs may be higher, in the aggregate, for all the customers to do the checking than for the bank to, but the bank reduces its costs by relying on the customer to do its work. Even though the bank is supposed to be acting in the interests of the customer, the bank has chosen a security solution that is more expensive in time and inconvenience for the customer.

The Importance of Authentication

Authentication is more important than encryption. Most people's security intuition says exactly the opposite, but it's true. Imagine a situation where Alice and Bob are using a secure communications channel to exchange data. Consider how much damage an eavesdropper could do if she could read all the traffic. Then think about how much damage Eve could do if she could modify the data being exchanged. In most situations, modifying data is a devastating attack, and does far more damage than merely reading it.

Here's another example: a Storage Area Network over IP within a

corporate LAN. Eavesdropping on traffic is passive, and doesn't necessarily expose private data (particularly on a switched network). But a lack of authentication allows sector-level data tampering that was never possible with direct-attached storage. Adding authentication avoids that problem entirely.

Or consider your own personal computer. Because data isn't authenticated, you are much more likely to be the victim of viruses, Trojans, and malware. Encryption is important; authentication is more important. If your computer is controlled by someone on the other end of a Trojan, it doesn't really matter what kind of encryption you've implemented.

Of course any secure system should have both encryption and authentication, but to the novice, per-packet authentication seems like a painful and superfluous overhead. Again and again I see protocols designed by otherwise-intelligent committees that mandate encryption but not authentication: WEP, Bluetooth, etc. An early version of the IPsec standard had a mode that encrypted but did not authenticate.

Last year I had a conversation with an engineer involved with security for the Bluetooth wireless protocol. I told him that Bluetooth has only privacy and not per-packet authentication. He responded with the prototypical lame responses: 1) pseudorandom frequency hopping makes it "nearly impossible" for an attacker to get in, and 2) the range is only 8 feet, so the attacks are naturally limited.

I tried to argue the point, but eventually gave up. Then I said something like: "I can hardly wait for Bluetooth to become universal, because I really want a wireless keyboard and mouse with the "base station" built into my computer." He said: "Yes, but you really probably don't want to use Bluetooth for that, because then somebody could stuff keystrokes or mouse clicks into your system." I didn't know whether to laugh or cry. Talk about not getting it.

Comments from Readers

From: Ira Winkler <ira_winkler@hp.com> Subject: Counterattack

I am concerned with Jennifer Granick's comments in response to Counterattack. First, Counterattack as a habit and policy are bad; however, there should be some conditions where taken action is permissible, such as the DoD handling of a planned protest and bombardments arising from known attacks like Code Red.

However, she went on to comment about the legality of spam. Her pro-spam analogies are a major concern and misrepresentation of the issue. Specifically, she claims that spam should be treated like noise. She claims that noise travels over air or "ether", and that noise that travels over boundaries is best classified as a nuisance. Let's assume that this is somehow correct. The spam analogy to noise is not someone playing their stereo loud enough that a neighbor can hear it on their own property. Spam is equivalent to a neighbor blasting their stereo specifically so anyone, anywhere in the world, can hear it. On top of that, the person blasting the stereo has a personal interest to blast the stereo, usually money. That is not an unintentional nuisance, but an intentional infliction of distress for purely selfish reasons. Forgive me for not being a lawyer and knowing the legal definitions of things. It is inconceivable that any court would classify this behavior as a "nuisance." On top of that, governments do have noise ordinances that blanketly classify types of noise as unacceptable. Spam is much more comparable to telemarketing calls, which are being regulated now to the point of universal opt outs.

Spam, however, is not like noise. While overhearing a neighbor's music does not cost people money, the proliferation of spam costs

companies, and inevitably the general public, billions of dollars. The latest reliable studies indicate that spam is now 40% of e-mail. E-mail storage costs money. E-mail transactions cost bandwidth, which has to be upgraded for traffic, including spam traffic. E-mail transactions cost processor utilization, which would have to be upgraded for increased traffic volume. Spam filters, and the maintenance of those filters, cost money. Sifting through spam costs lost productivity for businesses and home users. Home users cancel Internet accounts because spam takes up too much of their valuable time, despite the major inconvenience of letting people know about the change of address.

Then there are the pornography issues. Well-supported studies indicate that more than 25% of spam is for pornographic sites. Since spammers don't keep track of who is an adult or child, children receive the pornographic spams as well. Worse is that spammers go out of their way to get around spam- and porn-blocking filters. Even using noise analogies, public profanity and lewdness is illegal.

Then there is the business issue of pornographic spam. It is not inconceivable that a disgruntled employee could sue their employer when they receive pornographic spam, claiming that the employer created a hostile work environment by poorly filtering that spam.

However the most troubling of Jennifer's comments involved her contention that the Internet is a "Public Commons" and there should be no implication of ownership of computers on the Internet, such as mail servers. God help us if any court upholds that argument. That means that if a computer is connected to the Internet in any way, anyone can do with it what they want. In her argument, the computer becomes public property. Anybody has a right to use the computer and its data as they see fit. If you follow and extend her argument, if you have a computer connected to the Internet in any way, it would be

illegal to limit access to that computer. She bemoans the argument that hooking up to the Internet does not force someone to give up their ownership rights to those computers in the same way that driving your car on a public street does not mean that you give up ownership right to your car.

Jennifer claims that protecting ownership rights of computers connected to the Internet is "detrimental to socially beneficial uses." Extending that argument to the real world doesn't work, and it doesn't make sense for the Internet either.

From: "Jennifer S. Granick" <jennifer@granick.com> Subject: Counterattack

Ira and I agree that counterattack as habit and policy is undesirable. We also agree that there should be some conditions under which counterattack is legally permissible, just as we discourage punching people, but sometimes allow it in self-defense. What's a punch and what's self-defense is a more delicate question, which lawyers have spent hundreds of years answering and refining. More to the point, I disagree with Ira's implication that self-defense is a privilege that only the government may exercise.

As for the Intel v. Hamidi discussion, calling messages spam obfuscates the real issues. Ira is obviously very concerned about spam, pornography, and lewd language, perhaps more concerned, even, than the law, which says that all these are protected to varying degrees by the First Amendment. Rather, the question is whether and when the owner of an Internet-connected computer can control what messages I send, Web pages I serve, files I transmit.

I believe Intel has the right to agree with its employees about how they can use their workplace computers and to enforce that agreement, against the employees. Intel should have no right to tell me, a member

of the public, what e-mail addresses I can type into my Eudora program. Intel also has the right to protect its computer systems from damage, to seek redress if I damage their systems intentionally or through negligence. Intel can try to filter out messages, [a practice I feel a lot better about if the users are notified, particularly when we're talking about ISPs and not private companies]. I also believe that I as an individual user should be able to opt out of receiving unsolicited commercial messages that I don't want to receive.

However, the rule Intel seeks in the Hamidi case is that the server owner can get injunctions stopping members of the public from sending any packets through their servers at the owner's discretion, regardless of what the end user might want. This rule would apply to more than just private employers, and to more than just spam. And since we're really talking about packets, this same rule could be used to force Hamidi to put a filter on his Web page so that no Intel employees could view it. I don't think that my ISP should be able to make that decision on my behalf.

Ira assumes that a certain type of ownership right applies to computers connected to the Internet, the absolute right to exclude. Why presume that? That right applies in the real world only to real property (land). Private property traditionally does not come with an absolute right to exclude. (This is the debate over the definition of trespass to chattels that occupies the main briefs in the case.) So long as the user does not deprive the owner of use of the private property, as in stealing his car, and does not harm the property, the owner's right to the property is not sufficiently infringed for the law to get involved. I can pet your dog, even if you don't want me to.

A nuisance rule allows the courts to balance the interests of the server owner with the interests of the speaker and the interests of the public in receiving information before issuing a ban. Commercial speech may

be less valuable than political speech. A flood of irrelevant e-mails may be less protected than a bunch of e-mails targeted to the relevant audience. The users' desire to read what the sender has to say is a factor. Server owners are protected, but so are speakers and users. The Intel rule, and the one advocated by Winkler, certainly is better for companies. The public can send only approved messages, and the users receive only approved messages, and the companies, whether it's Intel or Earthlink, decide what's approved. AOL refuses to carry MSN Messenger packets. Earthlink sues to stop competitors from sending e-mails or Web pages advertising cheaper service to its customers. Great for them, but that's not a world I want to live in. Nor does the law require things to be this way.

For a law review article that does far more justice to this argument, please see: Dan Burk, "The Trouble with Trespass" (2000) 4 J. Small & Emerging Bus. L. 27, 49, available at the following link: <http://www.law.umn.edu/FacultyProfiles/BurkD.htm>.

From: Ira Winkler <ira_winkler@hp.com> Subject: Counterattack

I did not imply government can only perform self-defense. I used two examples of acceptable self-defense, in my opinion, which were the most publicly known. While the DoD example is government, the Code Red self-defense was employed by commercial and government entities.

To first summarize the Intel vs. Hamidi case, Hamidi was an Intel employee who was fired and sued Intel. The courts sided with Intel, and instead of going on with his life, Hamidi basically decided to make himself a thorn in Intel's side. For several years thereafter, Hamidi did various things, including sending unsolicited e-mails to 29,000 Intel employees. As a result of this, Intel sought an injunction against Hamidi sending unsolicited mass mailings to its employees again.

Hamidi's behavior appears obsessive. As I previously noted, spam costs individuals and businesses billions of dollars. Intel is not an ISP providing guaranteed delivery of e-mail to its employees. I do admit I think it is too kind to call people who send unsolicited e-mail "the scum of the Earth."

Concerning unsolicited e-mail as protected First Amendment speech, Jennifer's position means that any party of the choosing of the sender is required to utilize their resources at the discretion of anyone who chooses to spam the accounts they maintain. I disagree. E-mail is not just the forwarding of data packets as she states, but requires the receiver to use their computer resources.

The issue that stopping people from spamming implies that they must limit their own Web sites is not a valid argument and borders on ridiculous. Intel may choose to block the Web site at their own router, but cannot tell anyone else what they can do.

Jennifer's argument that there really are no rights of ownership in the real and Internet worlds is also questionable. In her argument, to convict someone of theft of anything, you have to prove that they did not intend to return it and that you also intended to use it. Imagine that if you notice your car missing. However even with this argument, spam costs storage, processing, bandwidth, and electric utilization, which costs money. As I said before, God help us if people no longer have discretion over the use of computers they own and maintain because they decide to attach it to the Internet.

There is nothing in Intel's case or their argument that says that they want to limit e-mail or other Internet services to only preauthorized people. They only want to stop someone who has previously sent their employees unsolicited e-mails, and states they will again and again, from doing so. Hamidi can use his own resources and take Opt-In requests from Intel employees to their home accounts; however, he

and you know that they are probably tired of his rantings or they would have done so already. Again, nothing is stopping him from using his own resources for exercising his First Amendment rights, except of course for the fact that few people seem to care about his personal opinion.

From: "Jennifer S. Granick" <jennifer@granick.com>Subject: Counterattack

>Jennifer's argument that there really are no rights of ownership
>in the real and Internet worlds is also questionable. In her
>argument, to convict someone of theft of anything you have to
>prove that they did not intend to return it and that you also
>intended to use it.

Actually, under the English common law, for hundreds of years, this was exactly the case. Theft was the taking of property of another with the intent to deprive permanently. If I intended to return it, it wasn't theft. In many states, that has been changed by statute, particularly for crimes like joyriding. What you're thinking of as "ownership" isn't a single natural, logical and indivisible right, but a set or subset of all possible rights that human beings have intentionally decided over time to associate with different types of property for the overall benefit of society.

From: Mike Robinson <miker@sundialservices.com>Subject: Re: Counterattack

Particularly with Internet issues, one must take a careful look at both sides of the coin, and consider how (not whether) a well-intentioned law or principle can be turned against its makers in cyberspace.

For example, if the principle of "counterattack" is permitted under law, then "I in the black hat" can savage your system and claim, as my

defense, that you were attacking me and that I defended myself. To support my claim I can fabricate whatever information-files I might require. Since your machine has been destroyed in my attack, you have nothing to refute me with, and "the law is on my side." And while all of this legal gerrymandering is going on (perhaps I have persuaded the authorities to seize your equipment), you are well on your way to going out of business.

This is why laws are written the way they are, and why I think that at least for the moment we can do no better. Well-intentioned laws that "legalize lynching" will dress a lot of telephone-poles with the remains of victims...killed, as it were, by the law itself.

From: Dorothy Denning <dedennin@nps.navy.mil> Subject: Disabling the Internet

Another reason a government might not want to take out an adversary's Internet connections is to launch a psyops campaign. Look at <<http://www.fcw.com/fcw/articles/2003/0113/...>>. The U.S. Department of Defense sent e-mail messages to Iraqi officials.

From: ketil@ii.uib.no (Ketil Z. Malde) Subject: Disabling the Internet

There's another reason why a country might want to disable the Internet connections of an enemy. Wars are less and less about weapons, and more and more about information, and you certainly want to avoid the enemy freely distributing information (think vivid and colourful images of killed and maimed children -- an inevitable result of any war) to your public. Look how that worked in the Vietnam war!

This is particularly important for USA and its allies, who are much better equipped and trained than the adversary, and can fight without suffering severe losses. The people are kept far from the battleground, which keeps them happy. But the Internet lets any geek with a Web

camera bring the battleground a lot closer, without any military censorship (or regards to viewer ratings, which is probably even more effective)

From: Arturo Bejar <arturo@yahoo-inc.com> Subject: Yahoo in the Doghouse

Got doghoused! Alas, the information on that is inaccurate. If a user needs to recover account access, their birthday is only one of several pieces of information we request. First, we ask for the birthday, zip code, and either user ID or alternate e-mail address. If that's entered correctly, we then authenticate the account by asking a secret question designated by the user when they registered.

If the user can't remember the answer to their secret question, we also support recovery by use of a verified alternative e-mail address (you can only verify by proving knowledge of the password), once the initial identifying information (birthday, zip, user ID/alternate e-mail) has been provided.

We only greet you with your birthday once you've logged in (assumes ownership of the account), and on that day of the year (server side controlled date).

If you ever hear anything about Yahoo! that raises a concern, you can let me, or security@yahoo-inc.com, know. We take user privacy and security very seriously and try to be very responsive to any issues raised.

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

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 "Secrets and Lies" and "Applied Cryptography," and an inventor of the Blowfish, Twofish, and Yarrow algorithms. He is a member of the Advisory Board of the Electronic Privacy Information Center (EPIC). He is a frequent writer and lecturer on computer security and cryptography.

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.

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

[next issue](#)

[previous issue](#)

[back to Crypto-Gram index](#)

Schneier.com is a personal website. Opinions expressed are not necessarily those of [BT](#).