Bruce Schneier

Crypto-Gram Newsletter

January 15, 2008

by Bruce Schneier
Founder and CTO
BT Counterpane
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.

For back issues, or to subscribe, visit <http://www.schneier.com/crypto-gram.html>.

You can read this issue on the web at <http://www.schneier.com/crypto-gram-0801.html>. These same essays appear in the "Schneier on Security" blog: <http://www.schneier.com/blog>. An RSS feed is available.

In this issue:

Anonymity and the Netflix Dataset

Last year, Netflix published 10 million movie rankings by 500,000 customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using. The data was anonymized by removing personal details and replacing names with random numbers, to protect the privacy of the recommenders.

Arvind Narayanan and Vitaly Shmatikov, researchers at the University of Texas at Austin, de-anonymized some of the Netflix data by comparing rankings and timestamps with public information in the Internet Movie Database, or IMDb.

Their research illustrates some inherent security problems with anonymous data, but first it's important to explain what they did and did not do.

They did *not* reverse the anonymity of the entire Netflix dataset. What they did was reverse the anonymity of the Netflix dataset for those sampled users who also entered some movie rankings, under their own names, in the IMDb. (While IMDb's records are public, crawling the site to get them is against the IMDb's terms of service, so the researchers used a representative few to prove their algorithm.)

The point of the research was to demonstrate how little information is required to de-anonymize information in the Netflix dataset.

On one hand, isn't that sort of obvious? The risks of anonymous databases have been written about before, such as in this 2001 paper published in an IEEE journal. The researchers working with the anonymous Netflix data didn't painstakingly figure out people's identities -- as others did with the AOL search database last year -- they just compared it with an already identified subset of similar data: a standard data-mining technique.

But as opportunities for this kind of analysis pop up more frequently, lots of anonymous data could end up at

risk.

Someone with access to an anonymous dataset of telephone records, for example, might partially de-anonymize it by correlating it with a catalog merchants' telephone order database. Or Amazon's online book reviews could be the key to partially de-anonymizing a public database of credit card purchases, or a larger database of anonymous book reviews.

Google, with its database of users' internet searches, could easily de-anonymize a public database of internet purchases, or zero in on searches of medical terms to de-anonymize a public health database. Merchants who maintain detailed customer and purchase information could use their data to partially de-anonymize any large search engine's data, if it were released in an anonymized form. A data broker holding databases of several companies might be able to de-anonymize most of the records in those databases.

What the University of Texas researchers demonstrate is that this process isn't hard, and doesn't require a lot of data. It turns out that if you eliminate the top 100 movies everyone watches, our movie-watching habits are all pretty individual. This would certainly hold true for our book reading habits, our internet shopping habits, our telephone habits and our web searching habits.

The obvious countermeasures for this are, sadly, inadequate. Netflix could have randomized its dataset by removing a subset of the data, changing the timestamps or adding deliberate errors into the unique ID numbers it used to replace the names. It turns out, though, that this only makes the problem slightly harder. Narayanan's and Shmatikov's de-anonymization algorithm is surprisingly robust, and works with partial data, data that has been perturbed, even data with errors in it.

With only eight movie ratings (of which two may be completely wrong), and dates that may be up to two weeks in error, they can uniquely identify 99 percent of the records in the dataset. After that, all they need is a little bit of identifiable data: from the IMDb, from your blog, from anywhere. The moral is that it takes only a small named database for someone to pry the anonymity off a much larger anonymous database.

Other research reaches the same conclusion. Using public anonymous data from the 1990 census, Latanya Sweeney found that 87 percent of the population in the United States, 216 million of 248 million, could likely be uniquely identified by their five-digit ZIP code, combined with their gender and date of birth. About half of the U.S. population is likely identifiable by gender, date of birth and the city, town or municipality in which the person resides. Expanding the geographic scope to an entire county reduces that to a still-significant 18 percent. "In general," the researchers wrote, "few characteristics are needed to uniquely identify a person."

Stanford University researchers reported similar results using 2000 census data. It turns out that date of birth, which (unlike birthday month and day alone) sorts people into thousands of different buckets, is incredibly valuable in disambiguating people.

This has profound implications for releasing anonymous data. On one hand, anonymous data is an enormous boon for researchers -- AOL did a good thing when it released its anonymous dataset for research purposes, and it's sad that the CTO resigned and an entire research team was fired after the public outcry. Large anonymous databases of medical data are enormously valuable to society: for large-scale pharmacology studies, long-term follow-up studies and so on. Even anonymous telephone data makes for fascinating research.

On the other hand, in the age of wholesale surveillance, where everyone collects data on us all the time, anonymization is very fragile and riskier than it initially seems.

Like everything else in security, anonymity systems shouldn't be fielded before being subjected to adversarial attacks. We all know that it's folly to implement a cryptographic system before it's rigorously attacked; why should we expect anonymity systems to be any different? And, like everything else in security, anonymity is a trade-off. There are benefits, and there are corresponding risks.

Narayanan and Shmatikov are currently working on developing algorithms and techniques that enable the secure release of anonymous datasets like Netflix's. That's a research result we can all benefit from.

http://www.cs.utexas.edu/~shmat/...
http://www.cs.utexas.edu/~shmat/netflix-faq.html
http://www.securityfocus.com/news/11497
http://arxivblog.com/?p=142

2001 IEEE paper:
http://people.cs.vt.edu/~naren/papers/ppp.pdf

De-anonymizing the AOL data:

http://query.nytimes.com/gst/fullpage.html?...
http://www.securityfocus.com/brief/286

Census data de-anonymization:
http://privacy.cs.cmu.edu/dataprivacy/papers/...
http://crypto.stanford.edu/~pgolle/papers/census.pdf

Anonymous cell phone data:
http://arxivblog.com/?p=88

Wholesale surveillance and data collection:
http://www.schneier.com/blog/archives/2006/03/...
http://www.schneier.com/blog/archives/2007/05/...

This essay originally appeared on Wired.com.
http://www.wired.com/politics/security/commentary/...

News

Microsoft has added the random-number generator Dual_EC-DRBG to Windows Vista, as part of SP1. Yes, this is the same RNG that could have an NSA backdoor. It's not enabled by default, and it's not clear that a user could enable it. It's available as a program call. My advice is to never use it, ever.
http://technet2.microsoft.com/WindowsVista/en/...
http://msdn2.microsoft.com/en-us/library/aa375534.aspx
Backdoor:
http://www.schneier.com/essay-198.html

This program mimics a human in a chat room, and attempts to extract personal information. And I thought ELIZA was so 1960s.
http://www.news.com/8301-13860_3-9831133-56.html

The Top 10 Data Breaches of 2007, according to CSO Magazine:
http://www2.csoonline.com/exclusives/column.html?...

Impressive prison break, involving two people removing the mortar around -- and then smashing -- a cinder block, wiggling through the hole, getting onto the roof, and then jumping off to freedom. They've since been recaptured.
http://www.cnn.com/2007/US/law/12/17/nj.jailbreak/...
http://www.schneier.com/blog/archives/2007/12/...

IEEE Spectrum has a three-part article on Tasers and how they work. Interesting reading, although be aware that two of the authors have connections to Taser manufacturers -- so you should expect biased treatment of the issues.
http://www.spectrum.ieee.org/dec07/5731
http://www.spectrum.ieee.org/dec07/5731/2
http://www.spectrum.ieee.org/dec07/5731/3
Taser video:
http://www.cbc.ca/canada/british-columbia/story/...

I know nothing of the politics of the Downsize DC organization, but their "I am not afraid" campaign is something I can certainly get behind. I think we should all send a letter like this to our elected officials, whatever country we're in: "I am not afraid of terrorism, and I want you to stop being afraid on my behalf. Please start scaling back the official government war on terror. Please replace it with a smaller, more focused anti-terrorist police effort in keeping with the rule of law. Please stop overreacting. I understand that it will not be possible to stop all terrorist acts. I accept that. I am not afraid."
http://action.downsizedc.org/wyc.php?cid=77
Refuse to be terrorized, and you deny the terrorists their most potent weapon -- your fear.
http://www.schneier.com/blog/archives/2006/08/...

There's also this video:
http://www.youtube.com/watch?v=ka5FdP-gNF0

Chicago opens a new front on the war on the unexpected, trying to scare everybody:
http://www.schneier.com/blog/archives/2007/12/...

Last week, Ask.com announced a feature called AskEraser, which erases a user's search history. While it's great to see companies using privacy features for competitive advantage, EPIC examined the feature and wrote to the company about some problems.
http://www.schneier.com/blog/archives/2007/12/...

Identity theft cartoon:
http://www.dilbert.com/creators/speedbump/archive/...
A Vermont federal judge has ruled that a person cannot be compelled by police to divulge his PGP key. This is by no means the end of the legal debate, but it's certainly good news.
http://www.news.com/8301-13578_3-9834495-38.html?...
http://www.news.com/8301-13578_3-9835392-38.html?...
http://yro.slashdot.org/article.pl?sid=07/12/15/1459243
Orin Kerr comments:
http://volokh.com/posts/1197670606.shtml

More voting machine news: from Ohio, Colorado, and elsewhere:
http://www.schneier.com/blog/archives/2007/12/...

Santa and the TSA
http://images.ucomics.com/comics/nq/2007/nq071224.gif

"Tiger Team" reality TV show. Sadly, it will not become a series.
http://en.wikipedia.org/wiki/Tiger_Team_%28TV_series%29
http://www.trutv.com/video/?id=870&link=truTVshlk
http://www.isohunt.com/torrents/%22tiger+team%22?iht=

Picasso stolen from Brazilian museum:
http://www.cnn.com/2007/WORLD/americas/12/20/...
http://www.schneier.com/blog/archives/2007/12/...
The paintings have been recovered:
http://www.foxnews.com/story/0,2933,321176,00.html

An article claims the software that runs the back end of either 35% or 80%-95% (depending on which part of the article you read) of all adult websites has been compromised, and that the adult industry is hushing this up. Like many of these sorts of stories, there's no evidence that the bad guys have the personal information database. The vulnerability only means that they could have it.
http://www.icwt.us/index.php/2007/12/23/...
http://it.slashdot.org/article.pl?sid=07/12/25/0050204

The FBI is building a massive biometrics database. Given its track record, does anyone believe for a minute that his or her biometrics information will be secure in this database?
http://www.washingtonpost.com/wp-dyn/content/...
http://news.bbc.co.uk/go/rss/-/2/hi/americas/...

Starting in 2008, there are new rules for bringing lithium batteries on airplanes. Near as I can tell, this affects no one except audio-video professionals.
http://www.schneier.com/blog/archives/2007/12/...

The Nugache worm/botnet, another new strain of malware.
http://www.schneier.com/blog/archives/2007/12/...

This clip by the Australian TV show The Chasers on terrorism is a couple of years old, but I hadn't seen it before. Funny.
http://www.youtube.com/watch?v=W3grHjibNdA

Amusing photo: wrongly accused.
http://i258.photobucket.com/albums/hh275/pizzler/...
Interesting article on the cybercrime economy.
http://resources.zdnet.co.uk/articles/features/...
The British Government changes their rhetoric, declaring the "war on terror" to be the wrong way to describe things:
http://www.military.com/NewsContent/...

"National Security for the Twenty-First Century," by Charlie Edwards at the British think-tank Demos. It's long -- 121 pages -- but there's some good stuff in it.

http://www.demos.co.uk/publications/...
Join "My SHC Community" on Sears.com, and the company will install some pretty impressive spyware on your computer. If a kid with a scary hacker name did this sort of thing, he'd be arrested. But this is Sears, so who knows what will happen to them. But what should happen is that the anti-spyware companies should treat this as the malware it is, and not ignore it because it's done by a Fortune 500 company.
http://community.ca.com/blogs/securityadvisor/...
Airport profiling, and the arrests it has led to:
http://www.schneier.com/blog/archives/2008/01/...

Good article about the Ft. Dix terrorist plotters: the challenges of going after terrorism more proactively, and the risks of using informants.
http://www.time.com/time/nation/article/...
I wrote about some of these issues here:
http://www.schneier.com/essay-174.html

"Responsible Behavior" cartoon:
http://xkcd.com/364/

Another funny one:
http://xkcd.com/350/

Good article from The New York Times Magazine on electronic voting machines:
http://www.nytimes.com/2008/01/06/magazine/...

The U.S. Army is installing Macintosh computers, because they're harder to hack:
http://www.forbes.com/home/technology/2007/12/20/...
Hacking the Boeing 787. Seems like the passenger Internet access might be connected to the plane's avionics.
http://www.wired.com/politics/security/news/2008/01/...
How well "See Something, Say Something" actually works; real data from New York.
http://www.schneier.com/blog/archives/2008/01/...

Investigative report on passport fraud worldwide:
http://www.msnbc.msn.com/id/22419963/

Interesting article on fear and the brain.
http://www.newsweek.com/id/78178
I've already written about this sort of thing.
http://www.schneier.com/essay-155.html

Swedish army loses classified information on a memory stick:
http://www2.mil.se/en/News/News/...
I wrote about this sort of thing two years ago:
http://www.schneier.com/essay-105.html
http://www.schneier.com/blog/archives/2005/07/...
Although why the Swedish Army doesn't encrypt its portable storage devices is beyond me.
http://www.schneier.com/blog/archives/2007/12/...

The 2007 International Privacy Ranking, from Privacy International:
http://www.privacyinternational.org/article.shtml?...
Five-year old boy detained by the TSA, because his name is similar to a possible terrorist alias. The explanation is simple: to the TSA, following procedure is more important than common sense. But unfortunately, catching the next terrorist will require more common sense than it will following proper procedure.
http://www.boingboing.net/2008/01/09/...
Apparently this was contrary to TSA policy:
http://www.tsa.gov/approach/mythbusters/...

Consumer Reports on Aviation Security and the TSA
http://www.schneier.com/blog/archives/2008/01/...

This story, about NSA backdoors in Crypto AG ciphering machines, made the rounds in European newspapers about ten years ago -- mostly stories in German, if I remember -- but it wasn't covered much here in the U.S.
http://www.inteldaily.com/?c=169&a=4686

Patrick Smith on aviation security; an excellent essay from the New York Times travel blog:
http://jetlagged.blogs.nytimes.com/2007/12/28/...
Business Week has a special report on the Department of Homeland Security that includes three different

articles.
http://www.businessweek.com/technology/...
Paul Torrens, at the Arizona State University School of Geographical Sciences, has a computer simulation that models urban panic.
http://pruned.blogspot.com/2007/06/...

How to cheat on a test by replacing a soft-drink-bottle label with a replica that includes your crib notes. Certainly more clever than hiding a small piece of paper inside your pen.
http://www.youtube.com/watch?v=NpQZDJ2fGnI

"Where Should Airport Security Begin?"

In an essay on the New York Times blog, Clark Ervin argues that airport security should begin at the front door to the airport: "Like many people, I spend a lot of time in airport terminals, and I often think that they must be an awfully appealing target to terrorists. The largest airports have huge terminals teeming with thousands of passengers on any given day. They serve as conspicuous symbols of American consumerism, with McDonald's restaurants, Starbucks coffee shops and Disney toy stores. While airport screeners do only a so-so job of checking for guns, knives and bombs at checkpoints, there's no checking for weapons before checkpoints. So if the intention isn't to carry out an attack once on board a plane, but instead to carry out an attack on the airport itself by killing people inside it, there's nothing to stop a terrorist from doing so."

And: "To prevent smaller attacks -- and larger ones that could be catastrophic -- what if we moved the screening checkpoints from the interior of airports to the entrance? The sooner we screen passengers' and visitors' persons and baggage (both checked and carry-on) for guns, knives and explosives, the sooner we can detect those weapons and prevent them from being used to sow destruction."

This is a silly argument, one that any regular reader of this newsletter should be able to counter. If you're worried about explosions on the ground, any place you put security checkpoints is arbitrary. The point of airport security is to prevent terrorism *on the airplanes*, because airplane terrorism is a more serious problem than conventional bombs blowing up in crowded buildings. (Four reasons. First, airlines are often national symbols. Second, airplanes often fly to dangerous countries. Third, for whatever reason, airplanes are a preferred terrorist target. And fourth, the particular failure mode of airplanes means that even a small bomb can kill everyone on board. That same bomb in an airport means that a few people die and many more get injured.) And most airport security measures aren't effective.

His bias betrays itself primary through this quote: "Like many people, I spend a lot of time in airport terminals, and I often think that they must be an awfully appealing target to terrorists."

If he spent a lot of time in shopping malls, he would probably think they must be awfully appealing targets as well. They also "serve as conspicuous symbols of American consumerism, with McDonald's restaurants, Starbucks coffee shops and Disney toy stores." He sounds like he's just scared.

Face it; there are far too many targets. Stop trying to defend against the tactic, and instead try to defend against terrorism. Airport security is the last line of defense, and not a very good one at that. Real security happens long before anyone gets to an airport, a shopping mall, or wherever.

http://jetlagged.blogs.nytimes.com/2007/12/17/...
http://www.schneier.com/essay-096.html
http://www.schneier.com/essay-124.html
http://www.schneier.com/essay-121.html
http://www.schneier.com/essay-038.html

Airport Security Study

Surprising nobody, a new study concludes that airport security isn't helping: "A team at the Harvard School of Public Health could not find any studies showing whether the time-consuming process of X-raying carry-on luggage prevents hijackings or attacks. They also found no evidence to suggest that making passengers take off their shoes and confiscating small items prevented any incidents."

And: "The researchers said it would be interesting to apply medical standards to airport security. Screening programs for illnesses like cancer are usually not broadly instituted unless they have been shown to work."

Note the defense by the TSA: "'Even without clear evidence of the accuracy of testing, the Transportation Security Administration defended its measures by reporting that more than 13 million prohibited items were

intercepted in one year,' the researchers added. "Most of these illegal items were lighters.'"

This is where the TSA has it completely backwards. The goal isn't to confiscate prohibited items. The goal is to prevent terrorism on airplanes. When the TSA confiscates millions of lighters from innocent people, that's a security failure. The TSA is reacting to non-threats. The TSA is reacting to false alarms. Now you can argue that this level of failures is necessary to make people safer, but it's certainly not evidence that people *are* safer.

For example, does anyone think that the TSA's vigilance regarding pies is anything other than a joke? They're too dangerous to bring on airplanes, yet safe enough to feed to U.S. soldiers.

http://www.abcnews.go.com/Business/Travel/story?...
http://www.sciencedaily.com/releases/2007/12/...
http://www.alertnet.org/thenews/newsdesk/N20228618.htm

Paper:
http://www.bmj.com/cgi/content/full/335/7633/1290

TSA and pies:
http://www.oregonlive.com/oregonian/stories/...
My interview with Kip Hawley, head of the TSA:
http://www.schneier.com/interview-hawley.html

Schneier/BT Counterpane News

Schneier is delivering the opening keynote at the "Technology in Wartime" conference in Palo Alto, CA on January 26:
http://technologyinwartime.org/

Schneier is speaking at Linux Australia in Melbourne on January 30:
http://linux.conf.au/

Schneier was interviewed in "Computerworld Australia":
http://www.computerworld.com.au/index.php/id;1891124482

"Holy Schneier" is now an exclamation:
http://www.schlockmercenary.com/d/20071220.html

My Open Wireless Network

Whenever I talk or write about my own security setup, the one thing that surprises people -- and attracts the most criticism -- is the fact that I run an open wireless network at home. There's no password. There's no encryption. Anyone with wireless capability who can see my network can use it to access the internet.

To me, it's basic politeness. Providing internet access to guests is kind of like providing heat and electricity, or a hot cup of tea. But to some observers, it's both wrong and dangerous.

I'm told that uninvited strangers may sit in their cars in front of my house, and use my network to send spam, eavesdrop on my passwords, and upload and download everything from pirated movies to child pornography. As a result, I risk all sorts of bad things happening to me, from seeing my IP address blacklisted to having the police crash through my door.

While this is technically true, I don't think it's much of a risk. I can count five open wireless networks in coffee shops within a mile of my house, and any potential spammer is far more likely to sit in a warm room with a cup of coffee and a scone than in a cold car outside my house. And yes, if someone did commit a crime using my network the police might visit, but what better defense is there than the fact that I have an open wireless network? If I enabled wireless security on my network and someone hacked it, I would have a far harder time proving my innocence.

This is not to say that the new wireless security protocol, WPA, isn't very good. It is. But there are going to be security flaws in it; there always are.

I spoke to several lawyers about this, and in their lawyerly way they outlined several other risks with leaving your network open.

While none thought you could be successfully prosecuted just because someone else used your network to

commit a crime, any investigation could be time-consuming and expensive. You might have your computer equipment seized, and if you have any contraband of your own on your machine, it could be a delicate situation. Also, prosecutors aren't always the most technically savvy bunch, and you might end up being charged despite your innocence. The lawyers I spoke with say most defense attorneys will advise you to reach a plea agreement rather than risk going to trial on child-pornography charges.

In a less far-fetched scenario, the Recording Industry Association of America is known to sue copyright infringers based on nothing more than an IP address. The accused's chance of winning is higher than in a criminal case, because in civil litigation the burden of proof is lower. And again, lawyers argue that even if you win it's not worth the risk or expense, and that you should settle and pay a few thousand dollars.

I remain unconvinced of this threat, though. The RIAA has conducted about 26,000 lawsuits, and there are more than 15 million music downloaders. Mark Mulligan of Jupiter Research said it best: "If you're a file sharer, you know that the likelihood of you being caught is very similar to that of being hit by an asteroid."

I'm also unmoved by those who say I'm putting my own data at risk, because hackers might park in front of my house, log on to my open network and eavesdrop on my internet traffic or break into my computers. This is true, but my computers are much more at risk when I use them on wireless networks in airports, coffee shops and other public places. If I configure my computer to be secure regardless of the network it's on, then it simply doesn't matter. And if my computer isn't secure on a public network, securing my own network isn't going to reduce my risk very much.

Yes, computer security is hard. But if your computers leave your house, you have to solve it anyway. And any solution will apply to your desktop machines as well.

Finally, critics say someone might steal bandwidth from me. Despite isolated court rulings that this is illegal, my feeling is that they're welcome to it. I really don't mind if neighbors use my wireless network when they need it, and I've heard several stories of people who have been rescued from connectivity emergencies by open wireless networks in the neighborhood.

Similarly, I appreciate an open network when I am otherwise without bandwidth. If someone were using my network to the point that it affected my own traffic or if some neighbor kid was dinking around, I might want to do something about it; but as long as we're all polite, why should this concern me? Pay it forward, I say.

Certainly this does concern ISPs. Running an open wireless network will often violate your terms of service. But despite the occasional cease-and-desist letter and providers getting pissy at people who exceed some secret bandwidth limit, this isn't a big risk either. The worst that will happen to you is that you'll have to find a new ISP.

A company called Fon has an interesting approach to this problem. Fon wireless access points have two wireless networks: a secure one for you, and an open one for everyone else. You can configure your open network in either "Bill" or "Linus" mode: In the former, people pay you to use your network, and you have to pay to use any other Fon wireless network. In Linus mode, anyone can use your network, and you can use any other Fon wireless network for free. It's a really clever idea.

Security is always a trade-off. I know people who rarely lock their front door, who drive in the rain (and, while using a cell phone), and who talk to strangers. In my opinion, securing my wireless network isn't worth it. And I appreciate everyone else who keeps an open wireless network, including all the coffee shops, bars and libraries I have visited in the past, the Dayton International Airport where I started writing this, and the Four Points Sheraton where I finished. You all make the world a better place.

RIAA data:
http://www.sptimes.com/2007/10/02/Business/...
http://www.npd.com/press/releases/press_0703141.html
http://www.guardian.co.uk/technology/2007/mar/22/...

Rulings on "stealing" bandwidth:
http://www.ibls.com/...
http://arstechnica.com/news.ars/post/...
Amusing story of someone playing with a bandwidth stealer:
http://www.ex-parrot.com/~pete/upside-down-ternet.html

ISPs:
http://w2.eff.org/Infrastructure/...
http://www.nytimes.com/2007/04/14/technology/...
Fon:
http://www.iht.com/articles/2006/01/30/business/...

http://www.fon.com/en/

This essay originally appeared on Wired.com.
http://www.wired.com/politics/security/commentary/...
It has since generated a lot of controversy.
http://hardware.slashdot.org/article.pl?sid=08/01/...

Here are opposing essays:
http://wifinetnews.com/archives/008126.html
http://www.dslreports.com/shownews/...
http://www.networkworld.com/community/node/23714

And here are supporting essays:
http://www.boingboing.net/2008/01/10/...
http://techdirt.com/articles/20080110/100007.shtml
http://blogs.computerworld.com/open_wireless_oh_my

Presumably there will be a lot of back and forth in the blog comments section here as well.
http://www.schneier.com/blog/archives/2008/01/...

Comments from Readers

There are hundreds of comments -- many of them interesting -- on these topics on my blog. Search for the story you want to comment on, and join in.

http://www.schneier.com/blog

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 BT Counterpane, and is a member of the Board of Directors of the Electronic Privacy Information Center (EPIC). He is a frequent writer and lecturer on security topics. See <http://www.schneier.com>.

BT Counterpane is the world's leading protector of networked information - the inventor of outsourced security monitoring and the foremost authority on effective mitigation of emerging IT threats. BT Counterpane protects networks for Fortune 1000 companies and governments world-wide. See <http://www.counterpane.com>.