CRYPTO-GRAM

February 15, 2013

by Bruce Schneier
Chief Security Technology Officer, BT
schneier@schneier.com
http://www.schneier.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-1302.html>. These same essays and news items appear in the "Schneier on Security" blog at <http://www.schneier.com/blog>, along with a lively comment section. An RSS feed is available.

** *** ***** ******* *********** *************

In this issue:

** *** ***** ******* *********** *************

Power and the Internet

All disruptive technologies upset traditional power balances, and the Internet is no exception. The standard story is that it empowers the powerless, but that's only half the story. The Internet empowers everyone. Powerful institutions might be slow to make use of that new power, but since they are powerful, they can use it more effectively.

Governments and corporations have woken up to the fact that not only can they use the Internet, they can control it for their interests. Unless we start deliberately debating the future we want to live in, and the role of information technology in enabling that world, we will end up with an Internet that benefits existing power structures and not society in general.

We've all lived through the Internet's disruptive history. Entire industries, like travel agencies and video rental stores, disappeared. Traditional publishing -- books, newspapers, encyclopedias, music -- lost power, while Amazon and others gained. Advertising-based companies like Google and Facebook gained a lot of power. Microsoft lost power (as hard as that is to believe).

The Internet changed political power as well. Some governments lost power as citizens organized online. Political movements became easier, helping to topple governments. The Obama campaign made revolutionary use of the Internet, both in 2008 and 2012.

And the Internet changed social power, as we collected hundreds of "friends" on Facebook, tweeted our way to fame, and found communities for the most obscure hobbies and interests. And some crimes became easier: impersonation fraud became identity theft, copyright violation became file sharing, and accessing censored materials -- political, sexual, cultural -- became trivially easy.

Now powerful interests are looking to deliberately steer this influence to their advantage. Some corporations are creating Internet environments that maximize their profitability: Facebook and Google, among many others. Some industries are lobbying for laws that make their particular business models more profitable: telecom carriers want to be able to discriminate between different types of Internet traffic, entertainment companies want to crack down on file sharing, advertisers want unfettered access to data about our habits and preferences.

On the government side, more countries censor the Internet -- and do so more effectively -- than ever before. Police forces around the world are using Internet data for surveillance, with less judicial oversight and sometimes in advance of any crime. Militaries are fomenting a cyberwar arms race. Internet surveillance -- both governmental and commercial -- is on the rise, not just in totalitarian states but in Western democracies as well. Both companies and governments rely more on propaganda to create false impressions of public opinion.

In 1996, cyber-libertarian John Perry Barlow issued his "Declaration of the Independence of Cyberspace." He told governments: "You have no moral right to rule us, nor do you possess any methods of enforcement that we have true reason to fear." It was a utopian ideal, and many of us believed him. We believed that the Internet generation, those quick to embrace the social changes this new technology brought, would swiftly outmaneuver the more ponderous institutions of the previous era.

Reality turned out to be much more complicated. What we forgot is that technology magnifies power in both directions. When the powerless found the Internet, suddenly they had power. But while the unorganized and nimble were the first to make use of the new technologies, eventually the powerful behemoths woke up to the potential -- and they have more power to magnify. And not only does the Internet change power balances, but the powerful can also change the Internet. Does anyone else remember how incompetent the FBI was at investigating Internet crimes in the early 1990s? Or how Internet users ran rings around China's censors and Middle Eastern secret police? Or how digital cash was going to make government currencies obsolete, and Internet organizing was going to make political parties obsolete? Now all that feels like ancient history.

It's not all one-sided. The masses can occasionally organize around a specific issue -- SOPA/PIPA, the Arab Spring, and so on -- and can block some actions by the powerful. But it doesn't last. The unorganized go back to being unorganized, and powerful interests take back the reins.

Debates over the future of the Internet are morally and politically complex. How do we balance personal privacy against what law enforcement needs to prevent copyright violations? Or child pornography? Is it acceptable to be judged by invisible computer algorithms when being served search results? When being served news articles? When being selected for additional scrutiny by airport security? Do we have a right to correct data about us? To delete it? Do we want computer systems that forget things after some number of years? These are complicated issues that require meaningful debate, international cooperation, and iterative solutions. Does anyone believe we're up to the task?

We're not, and that's the worry. Because if we're not trying to understand how to shape the Internet so that its good effects outweigh the bad, powerful interests will do all the shaping. The Internet's design isn't fixed by natural laws. Its history is a fortuitous accident: an initial lack of commercial interests, governmental benign neglect, military requirements for survivability and resilience, and the natural inclination of computer engineers to build open systems that work simply and easily. This mix of forces that created yesterday's Internet will not be trusted to create tomorrow's. Battles over the future of the Internet are going on right now: in legislatures around the world, in international organizations like the International Telecommunications Union and the World Trade Organization, and in Internet standards bodies. The Internet is what we make it, and is constantly being recreated by organizations, companies, and countries with specific interests and agendas. Either we fight for a seat at the table, or the future of the Internet becomes something that is done to us.

This essay appeared as a response to Edge's annual question, "What *Should* We Be Worried About?"
http://edge.org/response-detail/23818
http://www.edge.org/annual-question/q2013

** *** ***** ******* *********** *************

Who Does Skype Let Spy?

Lately I've been thinking a lot about power and the Internet, and what I call the feudal model of IT security that is becoming more and more pervasive. Basically, between cloud services and locked-down end-user devices, we have less control and visibility over our security -- and have no point but to trust those in power to keep us safe.

The effects of this model were in the news last week, when privacy activists pleaded with Skype to tell them who is spying on Skype calls.

> "Many of its users rely on Skype for secure communications -- whether they are activists operating in countries governed by authoritarian regimes, journalists communicating with sensitive sources, or users who wish to talk privately in confidence with business associates, family, or friends," the letter explains.
>
> Among the group's concerns is that although Skype was founded in Europe, its acquisition by a US-based company -- Microsoft -- may mean it is now subject to different eavesdropping and data-disclosure requirements than it was before.
>
> The group claims that both Microsoft and Skype have refused to answer questions about what kinds of user data the service retains, whether it discloses such data to governments, and whether Skype conversations can be intercepted.
>
> The letter calls upon Microsoft to publish a regular Transparency Report outlining what kind of data Skype collects, what third parties might be able to intercept or retain, and how Skype interprets its responsibilities under the laws that pertain to it.
> In addition it asks for quantitative data about when, why, and how Skype shares data with third parties, including governments.

That's security in today's world. We have no choice but to trust Microsoft. Microsoft has reasons to be trustworthy, but they also have reasons to betray our trust in favor of other interests. And all we can do is ask them nicely to tell us first.

http://www.theregister.co.uk/2013/01/25/activists_demand_skype_transparency/ or
http://tinyurl.com/a7db9cd
http://www.skypeopenletter.com/

Feudal security:
http://www.schneier.com/essay-406.html

** *** ***** ******* *********** *************

Our New Regimes of Trust

Society runs on trust. Over the millennia, we've developed a variety of mechanisms to induce trustworthy behavior in society. These range from a sense of guilt when we cheat, to societal disapproval when we lie, to laws that arrest fraudsters, to door locks and burglar alarms that keep thieves out of our homes. They're complicated and interrelated, but they tend to keep society humming along.

The information age is transforming our society. We're shifting from evolved social systems to deliberately created socio-technical systems. Instead of having conversations in offices, we use Facebook. Instead of meeting friends, we IM. We shop online. We let various companies and governments collect comprehensive dossiers on our movements, our friendships, and our interests. We let others censor what we see and read. I could go on for pages.

None of this is news to anyone. But what's important, and much harder to predict, are the social changes resulting from these technological changes. With the rapid proliferation of computers -- both fixed and mobile -- computing devices and in-the-cloud processing, new ways of socialization have emerged. Facebook friends are fundamentally different than in-person friends. IM conversations are fundamentally different than voice conversations. Twitter has no pre-Internet analog. More social changes are coming. These social changes affect trust, and trust affects everything.

This isn't just academic. There has always been a balance in society between the honest and the dishonest, and technology continually upsets that balance. Online banking results in new types of cyberfraud. Facebook posts become evidence in employment and legal disputes. Cell phone location tracking can be used to round up political dissidents. Random blogs and websites become trusted sources, abetting propaganda. Crime has changed: easier impersonation, action at a greater distance, automation, and so on. The more our nation's infrastructure relies on cyberspace, the more vulnerable we are to cyberattack.

Think of this as a "security gap": the time lag between when the bad guys figure out how to exploit a new technology and when the good guys figure out how to restore society's balance.

Critically, the security gap is larger when there's more technology, and especially in times of rapid technological change. More importantly, it's larger in times of rapid social change due to the increased use of technology. This is our world today. We don't know *how* the proliferation of networked, mobile devices will affect the systems we have in place to enable trust, but we do know it *will* affect them.

Trust is as old as our species. It's something we do naturally, and informally. We don't trust doctors because we've vetted their credentials, but because they sound learned. We don't trust politicians because we've analyzed their positions, but because we generally agree with their political philosophy -- or the buzzwords they use. We trust many things because our friends trust them. It's the same with corporations, government organizations, strangers on the street: this thing that's critical to society's smooth functioning occurs largely through intuition and relationship. Unfortunately, these traditional and low-tech mechanisms are increasingly failing us. Understanding how trust is being, and will be, affected -- probably not by predicting, but rather by recognizing effects as quickly as possible -- and then deliberately creating mechanisms to induce trustworthiness and enable trust, is the only thing that will enable society to adapt.

If there's anything I've learned in all my years working at the intersection of security and technology, it's that technology is rarely more than a small piece of the solution. People are always the issue and we need to think as broadly as possible about solutions. So while laws are important, they don't work in isolation. Much of our security comes from the informal mechanisms we've evolved over the millennia: systems of morals and reputation.

There will exist new regimes of trust in the information age. They simply must evolve, or society will suffer unpredictably. We have already begun fleshing out such regimes, albeit in an ad hoc manner. It's time for us to deliberately think about how trust works in the information age, and use legal, social, and technological tools to enable this trust. We might get it right by accident, but it'll be a long and ugly iterative process getting there if we do.

This essay was originally published in "The SciTech Lawyer," Winter/Spring 2013.

** *** ***** ******* *********** *************

News

There's a fascinating story about a probable tournament chess cheat. No one knows how he does it; there's only the facts that 1) historically he's not nearly as good as his recent record, and 2) his moves correlate almost perfectly with one of best computer chess programs. The general question is how valid statistical evidence is when there is no other corroborating evidence.
http://rjlipton.wordpress.com/2013/01/13/the-crown-game-affair/
It reminds me of this story of a marathon runner who arguably has figured out how to cheat undetectably.
http://www.schneier.com/blog/archives/2012/09/hacking_maratho.html

Good essay on FBI-mandated back doors by Matt Blaze and Susan Landau.
http://www.wired.com/opinion/2013/01/wiretap-backdoors/

This essay about obscurity is worth reading:
http://www.theatlantic.com/technology/archive/2013/01/how-to-think-about-your-online-data/267283/ or http://tinyurl.com/ay9z43u

Google is working on non-password authentication techniques.
http://www.wired.com/wiredenterprise/2013/01/google-password/all/
http://www.networkworld.com/news/2013/011913-google-looks-to-kill-passwords-265977.html or http://tinyurl.com/a8cz9a8

Ever since the launch of Kim Dotcom's file-sharing service, I have been asked about the unorthodox encryption and security system. I have not reviewed it, and don't have an opinion. All I know is what I read.
http://www.wired.com/threatlevel/2013/01/mega-is-no-megaupload/
http://arstechnica.com/business/2013/01/megabad-a-quick-look-at-the-state-of-megas-encryption/ or http://tinyurl.com/agsw48h
http://fail0verflow.com/blog/2013/megafail.html
http://nakedsecurity.sophos.com/2013/01/23/crypto-critics-take-on-kim-dotcom-and-mega6/ or http://tinyurl.com/afszymd
http://www.infosecurity-magazine.com/view/30392/megas-security-put-under-the-microscope-and-mega-responds/ or http://tinyurl.com/bh5a3n6
http://www.informationweek.com/security/encryption/mega-insecure-kim-dotcom-defends-reboote/240146801 or http://tinyurl.com/axx3ztf
https://spideroak.com/blog/20130123130638-spideroaks-analysis-and-recommendations-for-the-crypto-in-kim-dotcoms-mega-part-one or http://tinyurl.com/a6lhtae

Identifying people from their DNA.
http://www.nytimes.com/2013/01/18/health/search-of-dna-sequences-reveals-full-identities.html or http://tinyurl.com/b8bt62g

Identifying people from their writing style is called stylometry, and it's based on the analysis of things like word choice, sentence structure, syntax, and punctuation. In one experiment, researchers were able to identify 80% of users with a 5,000-word writing sample.
http://www.smh.com.au/it-pro/security-it/why-hackers-should-be-afraid-of-how-they-write-20130116-2csdo.html or http://tinyurl.com/bx4bhua
https://psal.cs.drexel.edu/index.php/JStylo-Anonymouth#You-can-download-it-here or http://tinyurl.com/anjt3ov

Janesville, Wisconsin, has published information about repeated drunk driving offenders since 2010. The idea is that the public shame will reduce future incidents.
http://host.madison.com/wsj/news/local/on-wisconsin-janesville-police-hope-online-map-will-shame-repeat/article_544c6e90-6107-11e2-b680-0019bb2963f4.html or http://tinyurl.com/bh47glv

Violence as a contagious disease.
http://www.wired.com/wiredscience/2013/01/violence-is-contagious/
I am reminded of this paper on the effects of bystanders on escalating and de-escalating potentially violent situations.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1298601

I have written about complexity and security for over a decade now. (For example, http://www.schneier.com/essay-018.html from 1999.) Here's the results of a survey that confirms this.
http://www.wired.com/insights/2013/01/uncovering-the-dangers-of-network-security-complexity/ or http://tinyurl.com/aeeyf9c
Usual caveats for this sort of thing apply. The survey is only among 127 people -- I can't find data on what percentage replied. The numbers are skewed because only those that chose to reply were counted. And the results are based on self-reported replies: no way to verify them. But still.

Backdoors built in to Barracuda Networks equipment:
http://arstechnica.com/security/2013/01/secret-backdoors-found-in-firewall-vpn-gear-from-barracuda-networks/ or http://tinyurl.com/b6xdmf8
http://krebsonsecurity.com/2013/01/backdoors-found-in-barracuda-networks-gear/ or http://tinyurl.com/a3tl6nf
http://www.theregister.co.uk/2013/01/24/barracuda_backdoor/
Don't we know enough not to do this anymore?

Dan Farmer has an interesting paper discussing the Baseboard Management Controller on server motherboards. Basically, it's a perfect spying platform. You can't control it. You can't patch it. It can completely control your computer's hardware and software. And its *purpose* is remote monitoring. At the very least, we need to be able to look into these devices and see what's running on them. I'm amazed we haven't seen any talk about this before now.
http://fish2.com/ipmi/
http://fish2.com/ipmi/itrain.html

Pentagon staffs Up U.S. Cyber Command from 900 to 4900. This is a big deal: more stoking of cyber fears, another step toward the militarization of cyberspace, and another ratchet in the cyberwar arms race.
http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html or http://tinyurl.com/bgbh6b3
Stoking cyber fears:
http://www.schneier.com/essay-404.html
Cyberwar arms race:
http://www.schneier.com/essay-399.html
Glenn Greenwald has a good essay on this.

http://www.guardian.co.uk/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet or http://tinyurl.com/aney62j

Using imagery to avoid censorship.
http://allthingsd.com/20130122/toward-a-more-visual-language-how-social-networks-skirt-censorship-in-china/ or http://tinyurl.com/ahudybp

I don't see a lot written about security seals, despite how common they are. This article is a very basic overview of the technologies.
http://jps.anl.gov/Volume6_iss1/Johnston.pdf

I just printed this out: "Proactive Defense for Evolving Cyber Threats," a Sandia Report by Richard Colbaugh and Kristin Glass. It's a collection of academic papers, and it looks interesting.
http://www.fas.org/irp/eprint/proactive.pdf

Clothing designed to thwart drones.
http://andrewsullivan.thedailybeast.com/2013/01/dressing-for-big-brother.html or http://tinyurl.com/bz6s3gp

Why is quantum computing so hard? Blog post (and two papers) by Ross Anderson and Robert Brady. Note that I do not have the physics to evaluate these claims.
http://www.lightbluetouchpaper.org/2013/02/01/hard-questions-about-quantum-crypto-and-quantum-computing/ or http://tinyurl.com/a3o82za
http://arxiv.org/abs/1301.7351
http://arxiv.org/abs/1301.7540
http://www.theregister.co.uk/2013/02/01/cambridge_boffins_doubt_quantum_experiments/ or http://tinyurl.com/a4ceeyk

Google's contest at the CanSecWest conference offers over $3M in prizes for Chrome hacks:
http://blog.chromium.org/2013/01/show-off-your-security-skills-pwn2own.html or http://tinyurl.com/ahmp4r2
http://www.theregister.co.uk/2013/01/29/google_third_pwnium_prizes/

Basically, Tide detergent is a popular product with a very small profit margin. So small non-chain grocery and convenience stores are happy to buy it cheaply, no questions asked. This makes it easy to sell if you steal it. And drug dealers have started taking it as currency, large bottles being worth about $5.
http://nymag.com/news/features/tide-detergent-drugs-2013-1/
Snopes rates this as undetermined:
http://www.snopes.com/media/notnews/tide.asp

A first-person account of the security surrounding the second inauguration of President Obama. Read it more for the details than for the author's reaction to them.
http://www.mvjantzen.com/blog/?p=3037

This long report looks at risky online behavior among the Millennial generation, and finds that they respond positively to automatic reminders and prodding. No surprise, really.
http://sites.duke.edu/ihss/files/2011/12/IHSS_FinalReport_MillenialCybersecurity_Greis.pdf or http://tinyurl.com/b74rls9

Interesting article about the difficulty Google has pushing security updates onto Android phones. The problem is that the phone manufacturer is in charge, and there are a lot of different phone manufacturers of varying ability and interest.
http://www.washingtonpost.com/business/technology/android-phones-vulnerable-to-hackers/2013/02/01/f3248922-6723-11e2-9e1b-07db1d2ccd5b_story.html or
http://tinyurl.com/aff24o5

This is an extremely clever man-in-the-middle timing attack against TLS that exploits the interaction between how the protocol implements AES in CBC mode for encryption, and HMAC-SHA1 for authentication. (And this is a really good plain-language description of it.)
http://www.isg.rhul.ac.uk/tls/TLStiming.pdf
http://nakedsecurity.sophos.com/2013/02/07/boffins-crack-https-encryptionin-lucky-thirteen-attack/ or http://tinyurl.com/cnhgstu

There's not a lot of information -- and quite a lot of hyperbole -- in this article about a new al Qaeda encryption tool.
http://www.hstoday.us/industry-news/general/single-article/new-encryption-is-it-the-key-to-al-qaeda-s-resurgence/cd30a1be7e88931a3513d4c3c6257316.html or
http://tinyurl.com/am6lxlb

There's a real Prisoner's Dilemma going on in France right now. A pair of identical twins who are suspected in a crime. There is there is CCTV and DNA evidence that could implicate either suspect. Detailed DNA testing that could resolve the guilty twin is prohibitively expensive. So both have been arrested in the hope that one may confess or implicate the other.
http://www.bbc.co.uk/news/world-europe-21401200

Long article on anti-cheating security in casinos:
http://www.theverge.com/2013/1/14/3857842/las-vegas-casino-security-versus-cheating-technology

Usability engineer Bruce Tognazzini talks about how an iWatch -- which seems to be either a mythical Apple product or one actually in development -- can make authentication easier.
http://asktog.com/atc/apple-iwatch/

Guessing smart-phone PINs by monitoring the accelerometer.
http://www.cs.swarthmore.edu/~aviv/papers/aviv-acsac12-accel.pdf

http://www.bbc.co.uk/news/technology-21203035

This keynote speech by Jacob Appelbaum from last December's 29C3 (29th Chaos Communication Congress) is worth listening to. He talks about what we can do in the face of oppressive power on the Internet. I'm not sure his answers are right, but am glad to hear someone talking about the real problems.
http://www.youtube.com/watch?v=QNsePZj_Yks>QNsePZj_Yks

There has been an enormous amount written about the suicide of Aaron Swartz. This is primarily a collection of links, starting with those that use his death to talk about the broader issues at play.
http://www.volokh.com/2013/01/14/aaron-swartz-charges/
http://www.volokh.com/2013/01/16/the-criminal-charges-against-aaron-swartz-part-2-prosecutorial-discretion/ or http://tinyurl.com/ak358y4
http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully
http://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz or http://tinyurl.com/bcut9bd
http://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2 or http://tinyurl.com/aojmv27
http://www.guardian.co.uk/commentisfree/2013/jan/12/aaron-swartz-heroism-suicide1 or http://tinyurl.com/c36m7yx
http://crookedtimber.org/2013/01/12/remembering-aaron-swartz/
http://www.zephoria.org/thoughts/archives/2013/01/13/aaron-swartz.html
http://boingboing.net/2013/01/12/rip-aaron-swartz.html
http://www.theatlantic.com/technology/archive/2013/01/aaron-swartz/267110/ or http://tinyurl.com/bqxcvob
http://blog.archive.org/2013/01/12/aaron-swartz-hero-of-the-open-world-rip/ or http://tinyurl.com/bf6qqn8
https://public.resource.org/aaron/
http://www.markbernstein.org/Jan13/AaronSwartz.html
Here are obituaries.
http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html or http://tinyurl.com/by2pkss
http://www.economist.com/news/obituary/21569674-aaron-swartz-computer-programmer-and-activist-committed-suicide-january-11th-aged-26-aaron or http://tinyurl.com/bb8ogfu
Here are articles and essays, mostly about the prosecutor's statement after the death and the problems with plea bargaining in general.
http://www.cnn.com/2013/01/17/tech/aaron-swartz-death/
http://www.huffingtonpost.com/2013/01/17/aaron-swartz-prosecutor_n_2492652.html or http://tinyurl.com/blx93x7
http://lessig.tumblr.com/post/40845525507/a-time-for-silence
http://www.techdirt.com/articles/20130117/02090421710/carmen-ortiz-releases-totally-bogus-statement-concerning-aaron-swartz-prosecution.shtml or http://tinyurl.com/ajbcrpb
http://news.cnet.com/8301-1023_3-57564807-93/larry-lessig-blasts-prosecutors-defense-in-swartz-case/ or http://tinyurl.com/b8e6ze4

http://www.forbes.com/sites/timothylee/2013/01/17/aaron-swartz-and-the-corrupt-practice-of-plea-bargaining/ or http://tinyurl.com/avq9vhn
Representative Zoe Lofgren is introducing a bill to prevent this from happening again.
http://www.reddit.com/r/technology/comments/16njr9/im_rep_zoe_lofgren_im_introducing_aarons_law_to/ or http://tinyurl.com/bmsfqwd
http://www.forbes.com/sites/andygreenberg/2013/01/16/aarons-law-suggests-reforms-to-hacking-acts-but-not-enough-to-have-protected-aaron-swartz/ or
http://tinyurl.com/afga2sq
More links:
http://www.groklaw.net/article.php?story=20130116022816840
http://www.emptywheel.net/2013/01/13/two-days-before-cambridge-cops-arrested-aaron-swartz-secret-service-took-over-the-investigation/ or http://tinyurl.com/a88bt89
http://blackagendareport.com/content/freedom-rider-state-killing-aaron-swartz or
http://tinyurl.com/byq57xp

** *** ***** ******* ********** ************

TSA Removing Rapiscan Full-Body Scanners from U.S. Airports

This is big news:

> The U.S. Transportation Security Administration will remove airport body scanners that privacy advocates likened to strip searches after OSI Systems Inc. (OSIS) couldn't write software to make passenger images less revealing.

This doesn't mean the end of full-body scanning. There are two categories of these devices: backscatter X-ray and millimeter wave.

> The government said Friday it is abandoning its deployment of so-called backscatter technology machines produced by Rapiscan because the company could not meet deadlines to switch to generic imaging with so-called Automated Target Recognition software, the TSA said. Instead, the TSA will continue to use and deploy more millimeter wave technology scanners produced by L-3 Communications,which has adopted the generic-outline standard.
>
> [...]
>
> Rapiscan had a contract to produce 500 machines for the TSA at a cost of about $180,000 each. The company could be fined and barred from participating in government contracts, or employees could face prison terms if it is found to have defrauded the government. In all, the 250 Rapiscan machines already deployed are to be

> phased out of airports nationwide and will be replaced with machines produced by L-3 Communications.

And there are still backscatter X-ray machines being deployed, but I don't think there are very many of them.

> TSA has contracted with L-3, Smiths Group Plc (SMIN) and American Science & Engineering Inc. (ASEI) for new body-image scanners, all of which must have privacy software. L-3 and Smiths used millimeter-wave technology. American Science uses backscatter.

This is a big win for privacy. But, more importantly, it's a big win because the TSA is actually taking privacy seriously. Yes, Congress ordered them to do so.   But they didn't defy Congress; they did it. The machines will be gone by June.

http://www.bloomberg.com/news/2013-01-18/naked-image-scanners-to-be-removed-from-u-s-airports.html or http://tinyurl.com/atzvvfd
http://www.wired.com/threatlevel/2013/01/tsa-abandons-nude-scanners/
http://www.bloomberg.com/news/2013-01-18/naked-image-scanners-to-be-removed-from-u-s-airports.html or http://tinyurl.com/atzvvfd
http://hosted.ap.org/dynamic/stories/U/US_AIRPORT_SCANNERS

** *** ***** ******* *********** *************

Dangerous Security Theater: Scrambling Fighter Jets

This story exemplifies everything that's wrong with our see-something-say-something war on terror: a perfectly innocent person on an airplane, a random person identifying him as a terrorist threat, and a complete overreaction on the part of the authorities.

Typical overreaction, but in this case -- as in several others over the past decade -- F-15 fighter jets were scrambled to escort the airplane to the ground. *Very* expensive, and potentially catastrophically fatal.

This blog post makes the point well:

> What bothers me about this is not so much that they interrogated the wrong person -- that happens all the time, not that it's okay -- but rather the fighter jets. I think most people probably understand this, but just to make it totally clear, if they send up fighters that is not because they are bringing the first-class passengers some more of those little hot towels. It is so they can be ready to SHOOT YOU DOWN if necessary. Now, I realize the odds that would ever happen, even accidentally, are very tiny. I still

> question whether it's wise to put fighters next to a passenger plane at the drop of a hat, or in this case because of an anonymous tip about a sleeping passenger.
>
> [...]
>
> According to the Seattle Times report, though, interceptions like this are apparently much more common than I thought. Citing a NORAD spokesman, it says this has happened "thousands of times" since 9/11. In this press release NORAD says there have been "over fifteen hundred" since 9/11, most apparently involving planes that violated "temporary flight restriction" areas. Either way, while this is a small percentage of all flights, of course, it still seems like one hell of a lot of interceptions -- especially since in every single case, it has been unnecessary, and is (as NORAD admits) "at great expense to the taxpayer."

http://blogs.seattletimes.com/today/2013/01/military-jets-escort-alaska-flight-to-sea-tac-fbi-detains-passenger/ or http://tinyurl.com/am4koap

Blog post:
http://www.loweringthebar.net/2013/01/fighters-intercept-sleepy-terrorist.html or
http://tinyurl.com/am87g57

** *** ***** ******* *********** *************

Massive Police Shootout in Cleveland Despite Lack of Criminals

This is an amazing story. I urge you to read the whole thing, but here's the basics:

> A November car chase ended in a "full blown-out" firefight, with glass and bullets flying, according to Cleveland police officers who described for investigators the chaotic scene at the end of the deadly 25-minute pursuit.
>
> But when the smoky haze -- caused by rapid fire of nearly 140 bullets in less than 30 seconds -- dissipated, it soon became clear that more than a dozen officers had been firing at one another across a middle school parking lot in East Cleveland.

At the end of the scene, both unarmed -- and presumably innocent -- people in the car were dead.

There's a lot that can be said here, but I don't feel qualified to say it. There's a whole body of research on decision making under stress -- police, firefighters, soldiers -- and how easy it is to get caught up in the heat of the moment. I have read one book on that subject, "Sources of Power," but that was years ago.

What interests me right now is how this whole situation was colored by what "society" is talking about and afraid of, which became the preconceptions the officers brought to the event. School shootings are in the news, so as soon as the car drove into a school parking lot, the police assumed the worst. Firefights with dangerous criminals are what we see on TV, so that's not unexpected, either. When you read the story, it's clear how many of the elements that the officers believed -- police cars being rammed, for example -- are right out of television violence. This would have turned out very differently if the officers had assumed that, as is almost always true, the two people in the car were just two people in a car.

I'm also curious as to how much technology contributed to this. Reports on the radio brought more and more officers to the scene, and misinformation was broadcast over the radio.

Again, I'm not really qualified to write about any of this. But it's what I've been thinking about.

http://www.cleveland.com/metro/index.ssf/2013/02/cleveland_police_chase_and_shooting_scene.html or http://tinyurl.com/auhsepf

"Sources of Power":
http://www.amazon.com/dp/0262611465/counterpane/

** *** ***** ******* *********** *************

"New York Times" Hacked by China

The "New York Times" hack was big news last week, and I spent a lot of time doing press interviews about it. But while it is an important story -- hacking a newspaper for confidential sources is fundamentally different from hacking a random network for financial gain -- it's not much different than GhostNet in 2009, Google's Chinese hacking stories from 2010 and 2011, or others.

Why all the press, then? Turns out that if you hack a major newspaper, one of the side effects is a 2,400-word newspaper story about the event.

It's a good story, and I recommend that people read it. The newspaper learned of the attack early on, and had a reporter embedded in the team as they spent months watching the hackers and clearing them out. So there's a lot more detail than you usually get. But otherwise, this seems like just another of the many cyberattacks from China. (It seems that the "Wall Street Journal" was also hacked, but they didn't write about it. This tells me that, with high probability, other high-profile news organizations around the world were hacked as well.)

My favorite bit of the "New York Times" story is when they ding Symantec for not catching the attacks:

> Over the course of three months, attackers installed 45 pieces of custom malware. The Times -- which uses antivirus products made by Symantec -- found only one instance in which Symantec identified an attacker's software as malicious and quarantined it, according to Mandiant.

Symantec, of course, had to respond:

> Turning on only the signature-based anti-virus components of endpoint solutions alone are not enough in a world that is changing daily from attacks and threats. We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough.

It's nice to have them on record as saying that.

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html or http://tinyurl.com/aw2ccrc

Other Chinese hacks
http://www.nytimes.com/2009/03/29/technology/29spy.html
http://www.wired.com/threatlevel/2010/01/operation-aurora/
http://www.guardian.co.uk/technology/2011/jun/01/google-hacking-chinese-attack-gmail
or http://tinyurl.com/3qpr7ca
http://arstechnica.com/security/2010/04/son-of-ghostnet-china-based-hacking-targets-india-government/ or http://tinyurl.com/arw8eoo
http://www.schneier.com/essay-227.html

Wall Street Journal hacked:
http://www.bbc.co.uk/go/em/fr/-/news/world-asia-china-21287757

Symanetec's responses:
http://www.theregister.co.uk/2013/02/01/symantec_responds_nyt_apt/
http://blogs.csoonline.com/data-protection/2549/shame-symantec-throwing-nyt-under-bus or http://tinyurl.com/awtv7ka

** *** ***** ******* *********** *************

Schneier News

I'm speaking at the RSA Conference in San Francisco, Feb 26-28. I have a solo talk Tuesday at 1:00, and I'm on a panel Wednesday at 12:00. Akamai is giving away 1,500 copies of "Liars and Outliers," and I'll be doing three signings at their booth. Zscalar is giving away 300 copies of "Schneier on Security," and I'll be doing one signing at their booth. I'm also doing two book signings at the RSA bookstore -- for everyone else. Check at the conference for schedule.
http://www.rsaconference.com/events/2013/usa/

I'm also speaking at SEGURINFO Argentina 2013 in Buenos Aires on March 12th:
http://www.segurinfo.org/home.php

This interview was conducted last month, at an artificial intelligence conference at Oxford.
http://www.schneier.com/blog/archives/2013/01/video_interview_5.html
https://www.youtube.com/watch?v=AUyIMWnb1JQ

I seem to be a physical security expert now.
http://www.ifsecglobal.com/author.asp?section_id=414&doc_id=558743&page_number=2&goback=.gde_2162880_member_209595197 or http://tinyurl.com/aspv3se
This seems so obviously written by someone who Googled me on the Internet, without any other knowledge of who I am or what I do.

** *** ***** ******* *********** *************

Jared Diamond on Common Risks

Jared Diamond has an op-ed in the "New York Times" where he talks about how we overestimate rare risks and underestimate common ones. Nothing new here -- I and others have written about this sort of thing extensively -- but he says that this is a bias found more in developed countries than in primitive cultures.

> I first became aware of the New Guineans' attitude toward risk on a trip into a forest when I proposed pitching our tents under a tall and beautiful tree. To my surprise, my New Guinea friends absolutely refused. They explained that the tree was dead and might fall on us.
>
> Yes, I had to agree, it was indeed dead. But I objected that it was so solid that it would be standing for many years. The New Guineans were unswayed, opting instead to sleep in the open

> without a tent.
>
> I thought that their fears were greatly exaggerated, verging on paranoia. In the following years, though, I came to realize that every night that I camped in a New Guinea forest, I heard a tree falling. And when I did a frequency/risk calculation, I understood their point of view.
>
> Consider: If you're a New Guinean living in the forest, and if you adopt the bad habit of sleeping under dead trees whose odds of falling on you that particular night are only 1 in 1,000, you'll be dead within a few years. In fact, my wife was nearly killed by a falling tree last year, and I've survived numerous nearly fatal situations in New Guinea.

Diamond has a point. While it's universally true that humans exaggerate rare and spectacular risks and downplay mundane and common risks, we in developed countries do it more. The reason, I think, is how fears propagate. If someone in New Guinea gets eaten by a tiger -- do they even have tigers in New Guinea? -- then those who know the victim or hear about it learn to fear tiger attacks. If it happens in the U.S., it's the lead story on every news program, and the entire country fears tigers. Technology magnifies rare risks. Think of plane crashes versus car crashes. Think of school shooters versus home accidents. Think of 9/11 versus everything else.

On the other side of the coin, we in the developed world have largely made the pedestrian risks invisible. Diamond makes the point that, for an older man, falling is a huge risk, and showering is especially dangerous. How many people do you know who have fallen in the shower and seriously hurt themselves? I can't think of anyone. We tend to compartmentalize our old, our poor, our different -- and their accidents don't make the news. Unless it's someone we know personally, we don't hear about it.

http://www.nytimes.com/2013/01/29/science/jared-diamonds-guide-to-reducing-lifes-risks.html or http://tinyurl.com/bkdknum

More writing on the topic:
http://www.schneier.com/blog/archives/2009/11/fear_and_overre.html
http://www.schneier.com/essay-401.html
http://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html
http://www.schneier.com/blog/archives/2009/11/fear_and_overre.html
http://www.schneier.com/blog/archives/2009/04/book_review_the.html
http://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html
http://www.schneier.com/blog/archives/2011/08/steven_pinker_o.html

** *** ***** ******* *********** *************

Man-in-the-Middle Attacks Against Browser Encryption

Last week, a story broke about how Nokia mounts man-in-the-middle attacks against secure browser sessions. "The Finnish phone giant has since admitted that it decrypts secure data that passes through HTTPS connections -- including social networking accounts, online banking, email and other secure sessions -- in order to compress the data and speed up the loading of Web pages."

The basic problem is that https sessions are opaque as they travel through the network. That's the point -- it's more secure -- but it also means that the network can't do anything about them. They can't be compressed, cached, or otherwise optimized. They can't be rendered remotely. They can't be inspected for security vulnerabilities. All the network can do is transmit the data back and forth.

But in our cloud-centric world, it makes more and more sense to process web data in the cloud. Nokia isn't alone here. Opera's mobile browser performs all sorts of optimizations on web pages before they are sent over the air to your smart phone. Amazon does the same thing with browsing on the Kindle. MobileScope, a really good smart-phone security application, performs the same sort of man-in-the-middle attack against https sessions to detect and prevent data leakage. I think Umbrella does as well. Nokia's mistake was that they did it without telling anyone. With appropriate consent, it's perfectly reasonable for most people and organizations to give both performance and security companies that ability to decrypt and re-encrypt https sessions -- at least most of the time.

This is an area where security concerns are butting up against other issues. Nokia's answer, which is basically "trust us, we're not looking at your data," is going to increasingly be the norm.

http://yro.slashdot.org/story/13/01/10/1356228/nokia-admits-decrypting-user-data-claiming-it-isnt-looking or http://tinyurl.com/ary6bl7
http://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/ or http://tinyurl.com/auznbtq
http://www.zdnet.com/nokia-hijacks-mobile-browser-traffic-decrypts-https-data-7000009655/ or http://tinyurl.com/adbclks

MobileScope:
https://mobilescope.net/

Umbrella:
http://www.umbrella.com/

** *** ***** ******* *********** *************

"People, Process, and Technology"

Back in 1999 when I formed Counterpane Internet Security, Inc., I popularized the notion that security was a combination of people, process, and technology. Back then, it was an important notion; security back then was largely technology-only, and I was trying to push the idea that people and process needed to be incorporated into an overall security system.

This blog post argues that the IT security world has become so complicated that we need less in the way of people and process, and more technology:

> Such a landscape can no longer be policed by humans and procedures. Technology is needed to leverage security controls. The Golden Triangle of people, process and technology needs to be rebalanced in favour of automation. And I'm speaking as a pioneer and highly experienced expert in process and human factors.
>
> [...]
>
> Today I'd ditch the Triangle. It's become an argument against excessive focus on technology. Yet that's what we now need. There's nowhere near enough exploitation of technology in our security controls. We rely far too much on policy and people, neither of which are reliable, especially when dealing with fast-changing, large scale infrastructures.

He's right. People and process work on human timescales, not computer timescales. They're important at the strategic level, and sometimes at the tactical level -- but the more we can capture and automate that, the better we're going to do.

The problem is, though, that sometimes human intelligence is required to make sense of an attack, and to formulate an appropriate response. And as long as that's the case, there are going to be instances where an automated attack is going to have the advantage.

Blog post:
http://www.computerweekly.com/blogs/david_lacey/2013/01/we_need_more_use_of_security_t.html or http://tinyurl.com/aovaja3

Counterpane Internet Security, Inc.:
http://en.wikipedia.org/wiki/BT_Managed_Security_Solutions

** *** ***** ******* *********** *************

Since 1998, CRYPTO-GRAM has been a free monthly newsletter providing summaries, analyses, insights, and commentaries on security: computer and otherwise. You can subscribe, unsubscribe, or change your address on the Web at <http://www.schneier.com/crypto-gram.html>. Back issues are also available at that URL.

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

CRYPTO-GRAM is written by Bruce Schneier. Schneier is the author of the best sellers "Liars and Outliers," "Beyond Fear," "Secrets and Lies," and "Applied Cryptography," and an inventor of the Blowfish, Twofish, Threefish, Helix, Phelix, and Skein algorithms. He is the Chief Security Technology Officer of BT, and is on 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>.

Crypto-Gram is a personal newsletter. Opinions expressed are not necessarily those of BT.

** *** ***** ******* *********** *************