

**From:** Bruce Schneier <schneier@counterpane.com>  
**Subject:** CRYPTO-GRAM, May 15, 2004  
**Date:** May 15, 2004 9:46:39 AM GMT+01:00  
**To:** crypto-gram@chaparraltree.com

---

CRYPTO-GRAM

May 15, 2004

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

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

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

Crypto-Gram also has an RSS feed at <<http://www.schneier.com/crypto-gram-rss.xml>>.

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

In this issue:

- Warrants as a Security Countermeasure
- Counterterrorism in Airports
- Crypto-Gram Reprints
- News
- Counterpane News
- Security Notes from All Over: Bypassing the USPS
- The Doghouse: Markland Technologies
- The Doghouse: IQ Networks
- National Security Consumers
- Comments from Readers

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Warrants as a Security Countermeasure

Years ago, surveillance meant trench-coated detectives following people down streets.

Today's detectives are more likely to be sitting in front of a computer, and the surveillance is electronic. It's cheaper, easier and safer. But it's also much more prone to abuse. In the world of cheap and easy surveillance, a warrant provides citizens with vital security against a more powerful police.

Warrants are guaranteed by the Fourth Amendment and are required before the police can search your home or eavesdrop on your telephone calls. But what other forms of search and surveillance are covered by warrants is still unclear.

An unusual and significant case recently heard in Nassau County's courts dealt with one piece of the question: Is a warrant required before the police can attach an electronic tracking device to someone's car?

It has always been possible for the police to tail a suspect, and wireless tracking is decades old. The only difference is that it's now much easier and cheaper to use the technology.

Surveillance will continue to become cheaper and easier -- and less intrusive. In the Nassau case, the police hid a tracking device on a car used by a burglary suspect, Richard D. Lacey. After Lacey's arrest, his lawyer sought to suppress evidence gathered by the tracking device on the grounds that the police did not obtain a warrant authorizing use of the device and that Lacey's privacy was violated.

It was believed to be the first such challenge in New York State and one of only a handful in the nation. A judge ruled Thursday that the police should have obtained a warrant. But he declined to suppress the evidence -- saying the car belonged to Lacey's wife, not to him, and Lacey therefore had no expectation of privacy.

More and more, we are living in a society where we are all tracked automatically all of the time.

If the car used by Lacey had been outfitted with the OnStar system, he could have been tracked through that. We can all be tracked by our cell phones. E-ZPass tracks cars at tunnels and bridges. Security cameras record us. Our purchases are tracked by banks and credit card companies, our telephone calls by phone companies, our Internet surfing habits by Web site operators.

The Department of Justice claims that it needs these, and other, search powers to combat terrorism. A provision slipped into an appropriations bill allows the FBI to obtain personal financial information from banks, insurance companies, travel agencies, real estate agents, stockbrokers, the U.S. Postal Service, jewelry stores, casinos and car dealerships without a warrant.

Starting this year, the U.S. government is photographing and fingerprinting foreign visitors coming into this country from all but 27 other countries. CAPPS II (Computer Assisted Passenger Prescreening System) will probe the backgrounds of all passengers boarding flights. Over New Year's, the FBI collected the names of 260,000 people staying at Las Vegas hotels. More and more, the "Big Brother is watching you" style of surveillance is becoming a reality.

Unfortunately, the debate often gets mischaracterized as a question about how much privacy we need to give up in order to be secure. People ask: "Should we use this new surveillance technology to catch terrorists and criminals, or should we favor privacy and ban its use?"

This is the wrong question. We know that new technology gives law enforcement new search techniques, and makes existing techniques cheaper and easier. We know that we are all safer when the police can use them. And the Fourth Amendment already allows even the most intrusive searches: The police can search your home and person.

What we need are corresponding mechanisms to prevent abuse. This is the proper question: "Should we allow law enforcement to use new technology without any judicial oversight, or should we demand that they be overseen and accountable?" And the Fourth Amendment already provides for this in its requirement of a warrant.

The search warrant -- a technologically neutral legal requirement -- basically says that before the police open the mail, listen in on the phone call or search the bit stream for key words, a "neutral and detached magistrate" reviews the basis for the search and takes responsibility for the outcome. The key is independent judicial oversight; the warrant process is itself a security measure protecting us from abuse and making us more secure.

Much of the rhetoric on the "security" side of the debate cloaks one of its real aims: increasing law enforcement powers by decreasing its oversight and accountability. It's a very dangerous road to take, and one that will make us all less secure. The more surveillance technologies that require a warrant before use, the safer we all are.

This essay originally appeared in Newsday:  
<<http://www.newsday.com/news/opinion/ny-vpsch103794744may10,0,3318138.st> ory> or <<http://tinyurl.com/yty95>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

### Counterterrorism in Airports

It's just a pilot program, but undercover security officers are roaming Boston's Logan Airport, looking for suspicious people who may be planning a terrorist act. It's got a fancy name, "behavior pattern recognition," but basically it means "be on the lookout for suspicious people."

I think this is the best thing to happen to airplane security since they reinforced the cockpit doors.

I've long argued that traditional airport security is largely useless. Air travelers -- the innocent ones -- are subjected to all sorts of indignities in the name of security. Again and again we read studies about how bad the checkpoints are at keeping weapons out of airports. The system seems to do nothing more than irritate honest people. (Remember, when airport security takes a pair of scissors away from an innocent grandma, that's a security failure. It's a false positive. It's not a success.)

Well-trained officers on the lookout for suspicious people is a great substitute.

The devil is in the details, of course. All too often "he's acting suspicious" really translates to "he's black." Well-trained is the key to avoiding racism, which is both bad for society and bad for security. But security is inherently about people, and smart observant people are going to notice things that metal detectors and X-ray machines will miss.

Of course, machines are better at ducking charges of prejudice. It may be less secure to have a computer decide who to wand, or to have random chance decide whose baggage to open, but it's easier to pretend that prejudice is not an issue. "It's not the officer's fault; the computer selected him" plays well as a defense. And in a world where security theatre

still matters more than security, this is an important consideration.

For about a year now, I've been saying we can improve airport security by doing away with the security checkpoints and replacing them with well-trained officers looking out for suspicious activity. It'll probably never happen, but at least this is a start.

<<http://www.cbsnews.com/stories/2004/04/16/terror/main612369.shtml>>

\*\* \*\*

### Crypto-Gram Reprints

Crypto-Gram is currently in its seventh 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.

Encryption and Wiretapping

<<http://www.schneier.com/crypto-gram-0305.html#1>>

Unique E-Mail Addresses and Spam

<<http://www.schneier.com/crypto-gram-0305.html#6>>

Secrecy, Security, and Obscurity

<<http://www.schneier.com./crypto-gram-0205.html#1>>

Fun with Fingerprint Readers

<<http://www.schneier.com./crypto-gram-0205.html#5>>

What Military History Can Teach Network Security, Part 2

<<http://www.schneier.com/crypto-gram-0105.html#1>>

The Futility of Digital Copy Protection

<<http://www.schneier.com/crypto-gram-0105.html#3>>

Security Standards

<<http://www.schneier.com/crypto-gram-0105.html#7>>

Safe Personal Computing

<<http://www.schneier.com/crypto-gram-0105.html#8>>

Computer Security: Will we Ever Learn?

<<http://www.schneier.com/crypto-gram-0005.html#ComputerSecurityWillWeEverLearn>> or <<http://tinyurl.com/2gj8x>>

Trusted Client Software

<<http://www.schneier.com/crypto-gram-0005.html#TrustedClientSoftware>> or <<http://tinyurl.com/bo6p>>

The IL\*VEYOU Virus (Title bowdlerized to foil automatic e-mail filters.)

<<http://www.schneier.com/crypto-gram-0005.html#ilyvirus>>

The Internationalization of Cryptography  
<<http://www.schneier.com/crypto-gram-9905.html#international>>

The British discovery of public-key cryptography  
<<http://www.schneier.com/crypto-gram-9805.html#nonsecret>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## News

Interesting article on using vulnerability assessments to identify security policy problems:  
<<http://www.onlamp.com/pub/a/security/2004/04/08/networksecurity.html>>

Bill Gates's lengthy e-mail describing the company's security efforts:  
<<http://www.computerworld.com/printthis/2004/0,4814,91801,00.html>>  
<<http://www.microsoft.com/mscorp/execmail/2004/03-31security-print.asp>> or <<http://tinyurl.com/2umnx>>

An interview with Amit Yoran, director of DHS National Cyber Security Division:  
<<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=18600292>> or  
<<http://tinyurl.com/2cetk>>

The TSA is seriously looking into a trusted traveler program. Honestly, I'm not sure of the need. The long lines for security that plagued airports in the months after 9/11 are largely gone, and the top-tier frequent fliers that are likely to register for such a program already have a special fast lane through security.  
<[http://www.computerworld.com/securitytopics/security/story/0,10801,9209\\_9,00.html?nas=SEC-92099](http://www.computerworld.com/securitytopics/security/story/0,10801,9209_9,00.html?nas=SEC-92099)> or <<http://tinyurl.com/3ybyt>>

Good article on security companies fomenting fear to stimulate sales:  
<<http://www.eweek.com/article2/0,1759,1566249,00.asp>>

Long, but good, study on national ID cards:  
<[http://books.nap.edu/html/id\\_questions/](http://books.nap.edu/html/id_questions/)>

Okay, so this is gross. But it's an interesting "security through obscurity" idea:  
<<http://www.shomertec.com/item.cfm?Action=newItems&variable=1164>>

Looks like the TSA may abandon one of the post-9/11 airport rules: only ticketed passengers are allowed through security. The rule made some sense when the security lines were long; only allowing ticketed passengers through meant fewer people in the lines. But now that lines are shorter, the rule no longer makes sense. On the other hand, the TSA is doing its "extra" screening at the security checkpoints. Will everyone without a ticket be subject to this "extra" screening?  
<[http://www.usatoday.com/travel/news/2004-04-19-airport-security\\_x.htm](http://www.usatoday.com/travel/news/2004-04-19-airport-security_x.htm)> or <<http://tinyurl.com/yqax8>>

New NSA patent on a key-escrow system. Note that it was filed in 1996, when this kind of thing was in vogue.  
<<http://cryptome.org/nsa-access.htm>>

Interesting essay on warranties of "cyberworthiness." The author takes the idea of "seaworthiness" of ships and tries to apply it to software. It's a way to manage liabilities. Definitely worth reading.

<<http://csdl.computer.org/comp/mags/sp/2004/02/j2073abs.htm>>

How to turn a disposable camera into a stun gun.

<<http://www.techtv.com/unscrewed/ihateyou/story/0,24682,3653392,00.html>> or <<http://tinyurl.com/2xctm>>

Don't tell anyone who works in airline security about this; they may start banning cameras on airplanes.

More than 70% of people would give their password to a stranger in exchange for a bar of chocolate.

<<http://news.bbc.co.uk/2/hi/technology/3639679.stm>>

This kind of thing doesn't surprise me. Although I expect that at least some of those people gave a fake password, I'm sure many of them gave away their real passwords.

Good rebuttal to Mossberg's Wall Street Journal essay on network and computer security:

<<http://www.securityfocus.com/columnists/236>>

Interesting Q&A with Paul Kocher. I wish it were longer.

<[http://zdnet.com.com/2100-1105\\_2-5201619.html](http://zdnet.com.com/2100-1105_2-5201619.html)>

Massive distributed computing effort breaks a 109-bit elliptic curve crypto problem:

<[http://www.theregister.co.uk/2004/04/29/crypto\\_certicom/](http://www.theregister.co.uk/2004/04/29/crypto_certicom/)>

Good article on spyware (also read the sidebars):

<<http://www.computerworld.com/securitytopics/security/story/0,10801,92784,00.html?SKC=home92784>> or <<http://tinyurl.com/2482t>>

Seems that Microsoft's reward helped capture the author of the Sasser worm.

<[http://news.com.com/2100-7349\\_3-5208762.html](http://news.com.com/2100-7349_3-5208762.html)>

A fascinating piece of side-channel cryptanalysis: breaking RSA keys by listening to computers.

<<http://www.wisdom.weizmann.ac.il/~tromer/acoustic/>>

An island where everyone is constantly under surveillance:

<<http://www.wired.com/news/privacy/0,1848,63316,00.html>>

The latest version of WinZip uses AES encryption. (AES-CTR and HMAC-SHA1, if you want the details.)

<[http://www.winzip.com/aes\\_info.htm](http://www.winzip.com/aes_info.htm)>

Unfortunately, WinZip's encryption is vulnerable to several attacks: <<http://www.cse.ucsd.edu/users/tkohn/papers/WinZip/>>.

Moral (it's not a new one): Cryptography is hard, and simply using AES in a product does not magically make it secure.

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Bruce Schneier is speaking at Princeton University on May 17:  
<<http://webserv03.princeton.edu/cgi-bin/team/webevent.cgi?cmd=showevent&ncmd=listmonth&cal=cal282&id=30564>> or <<http://tinyurl.com/2hxbf>>

Schneier is speaking at EPIC's Freedom 2.0 Conference on May 20:  
<<http://www.epic04.org/>>

Schneier is speaking at the South Sound Technology Conference on May 26:  
<<http://www.sstconference.com/>>

Schneier is speaking at a security conference in Oslo on June 2:  
<<http://mnemonic.no/index.boom?cat=14&art=560>>

Audio interview with Schneier:  
<<http://www.itconversations.com/shows/detail119.html>>

Counterpane's 1st quarter performance:  
<<http://www.counterpane.com/pr-20040827.html>>

Counterpane announces partnership with Getronics:  
<<http://www.counterpane.com/pr-20040512.html>>

Counterpane's webcast with Gartner:  
<[http://www.itworld.com/itwebcast/counterpane\\_msm/](http://www.itworld.com/itwebcast/counterpane_msm/)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

### Security Notes from All Over: Bypassing the USPS

If you're the U.S. government, you're scared about receiving anthrax-laden mail. So you submit all incoming mail to various security screening and decontamination procedures. But that slows mail down. So you're forced to tell people how to get around those procedures:

"The Commission is requesting that any comment or request filed in paper form be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions."

Now maybe we can make a case that services like FedEx are less anonymous than the mail, but that's not true. Anyone with a stolen account number or credit card can toss a FedEx letter into a box.

<<http://www.ftc.gov/os/2004/04/rfidworkshopfrn.pdf>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

### The Doghouse: Markland Technologies

Here's a fascinating website about Markland Technologies' VYN Double Cipher Keyless

Transmission System. The writing is more literate than usual for crackpots, but it has most of the standard snake-oil warning signs: the author displays a profound ignorance of cryptography, the algorithm is "perfect," it relies on impressive sounding mathematics, it's been reviewed and deemed correct by an unnamed expert, and the description is completely devoid of illuminating detail.

Interestingly, the author does admit that the algorithm has a practical drawback: it requires 50 bytes of overhead to transmit one byte of data. No doubt being "keyless" makes up for that limitation.

In addition, naming a product "Crypto.Com" when you don't own the crypto.com domain seems a recipe for confusion.

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

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

### The Doghouse: IQ Networks

In general, the Doghouse is a showcase for stupid security companies or products. Snake-oil cryptography, nonsense computer security, that sort of thing. But this month we have something different: a company committing out-and-out fraud.

IQ Networks claims to have an impressive advisory board: Ross Anderson, Mihir Bellare, Steve Bellovin, Shafi Goldwasser, Peter Gutmann, Doug Stinson, Ron Rivest, and Markus Kuhn. Unfortunately, none of these people had ever heard of the company. Nor did they agree to have content of theirs on the site. They also claim to be involved with the HoneyNet Project -- none of the HoneyNet guys had ever heard of them -- and Password Safe: I've never heard of them, either.

They have an impressive customer list. I'll bet anything that all of them are fabrications, too. Oh; they're under investigation by SANS for pirating SANS training material.

The rest of the site is also amusing, with a lot of generic security gobbledygook and not a whole lot of information. The company claims to do pretty much anything.

Would you buy your security services from a company that lies about, um, everything?

Website:

<<http://www.iq-net-works.com/>>

Customer list (hard to find, and will probably be deleted soon):

<[http://www.iq-net-works.com/clientes\\_english.html](http://www.iq-net-works.com/clientes_english.html)>

Peter Gutmann sent this link to me a few weeks ago, and has challenged the company about their use of his name. In response, the company has pulled their list of technical advisors from its website. It forgot, however, to pull the list from the Spanish website. <<http://www.iq-net-works.com/spanish/equipo.html>>

Look quickly, I expect it will be gone soon.

You can also look them up on archive.org, which has saved the company's list of advisors (also in Spanish) from 2003. (This website is great for finding old versions of webpages, or webpages that are no longer around.)  
<<http://web.archive.org/web/20030705082011/www.iq-net-works.com/equipo.html>> or <<http://tinyurl.com/2dbwj>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## National Security Consumers

National security is a hot political topic right now, as both presidential candidates are asking us to decide which one of them is better fit to secure the country.

Many large and expensive government programs -- the CAPPs II airline profiling system, the US-VISIT program that fingerprints foreigners entering our country, and the various data-mining programs in research and development -- take as a given the need for more security.

At the end of 2005, when many provisions of the controversial Patriot Act expire, we will again be asked to sacrifice certain liberties for security, as many legislators seek to make those provisions permanent.

As a security professional, I see a vital component missing from the debate. It's important to discuss different security measures, and determine which ones will be most effective. But that's only half of the equation; it's just as important to discuss the costs. Security is always a trade-off, and herein lies the real question: "Is this security countermeasure worth it?"

As Americans, and as citizens of the world, we need to think of ourselves as security consumers. Just as a smart consumer looks for the best value for his dollar, we need to do the same. Many of the countermeasures being proposed and implemented cost billions. Others cost in other ways: convenience, privacy, civil liberties, fundamental freedoms, greater danger of other threats. As consumers, we need to get the most security we can for what we spend.

The invasion of Iraq, for example, is presented as an important move for national security. It may be true, but it's only half of the argument. Invading Iraq has cost the United States enormously. The monetary bill is more than \$100 billion, and the cost is still rising. The cost in American lives is more than 600, and the number is still rising. The cost in world opinion is considerable. There's a question that needs to be addressed: "Was this the best way to spend all of that? As security consumers, did we get the most security we could have for that \$100 billion, those lives, and those other things?"

If it was, then we did the right thing. But if it wasn't, then we made a mistake. Even though a free Iraq is a good thing in the abstract, we would have been smarter spending our money, and lives and good will, in the world elsewhere.

That's the proper analysis, and it's the way everyone thinks when making personal security choices. Even people who say that we must do everything possible to prevent another Sept. 11 don't advocate permanently grounding every aircraft in this country. Even though that would be an effective countermeasure, it's ridiculous. It's not worth it. Giving up commercial aviation is far too large a price to pay for the increase in security that it

would buy. Only a foolish security consumer would do something like that.

Oddly, when I first wrote this essay for CNet, I received a comment accusing me of being a pacifist. To me, this completely misses the point. I am not espousing a political philosophy; I am espousing a decision-making methodology. Whether you are a pacifist or a militarist, a Republican or a Democrat, an American or European...you're a security consumer. Different consumers will make different trade-offs, since much of this decision is subjective, but they'll use the same analysis.

We need to bring the same analysis to bear when thinking about other security countermeasures. Is the added security from the CAPPs-II airline profiling system worth the billions of dollars it will cost, both in dollars and in the systematic stigmatization of certain classes of Americans? Would we be smarter to spend our money on hiring Arabic translators within the FBI and the CIA, or on emergency response capabilities in our cities and towns?

As security consumers, we get to make this choice. America doesn't have infinite money or freedoms. If we're going to spend them to get security, we should act like smart consumers and get the most security we can.

The efficacy of a security countermeasure is important, but it's never the only consideration. Almost none of the people reading this essay wear bulletproof vests. It's not because they don't work -- in fact they do -- but because most people don't believe that wearing the vest is worth the cost. It's not worth the money, or the inconvenience, or the lack of style. The risk of being shot is low. As security consumers, we don't believe that a bulletproof vest is a good security trade-off.

Similarly, much of what is being proposed as national security is a bad security trade-off. It's not worth it, and as consumers we're getting ripped off.

Being a smart security consumer is hard, just as being a good citizen is hard. Why? Because both require thoughtful consideration of trade-offs and alternatives. But in this election year, it is vitally important. We need to learn about the issues. We need to turn to experts who are nonpartisan -- who are not trying to get elected or stay elected. We need to become informed. Otherwise it's no different than walking into a car dealership without knowing anything about the different models and prices -- we're going to get ripped off.

This essay originally appeared, in a shorter form, on News.com:  
<<http://news.com.com/2010-7348-5204924.html>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

#### Comments from Readers

From: Alan Morgan <amorgan@CS.Stanford.EDU>  
Subject: Stealing an Election

Stealing an election comes with a huge risk. Ensuring that your favorite obscure political party gets 5% of the popular vote and thus qualifies for federal matching funds is less

risky. Suppose the Green Party or Libertarian Party gets 5% of the popular vote in the next election. Is this a sign that their parties are resonating with the American public or a sign that a mad-as-hell software engineer decided to give them an election year present?

From: Robert <raven@ioa.com>  
Subject: Stealing an Election

In the discussions of voting machine security that I have read, most of the attention seems to have been paid on the vulnerability of the machines to "hacking," to alter the votes cast.

Here's an alternate scenario: To alter the results of the election, isn't destroying the votes of the opposite side just as effective as adding votes for your side? You simply target machines that are in areas that your opponent has a large advantage (the area is known to be radically for one side or the other) and cause the machines to break down and lose their data.

It seems to me that this would be easier to accomplish than hacking the code itself. And since the machines have no paper trail or backup, there is no way to find out what the votes were.

You would want to wait until later in the election day, so as to have the largest effect possible. It would take teams of people to do this though, as one or a few people would (hopefully) not be able to access more than one machine, or be able to enter more than one polling place, although fake IDs could be used to facilitate this.

The machines could be damaged with a small, battery powered "Zapper", like a hand held stun gun. If hit in the right spot, the data would be erased from the machine, or the circuits sufficiently fried as to make it unreadable.

This method might raise red flags after the election, especially if machines in one area were shown to have a higher rate of failure than other areas. But, as our court systems have shown, exactly what could be done about it? They are not going to hold the election again.

This method probably would not be practical on a national or even a state level, but for city and other local types of elections, it could have an impact.

From: Ethan Sommer <sommere@ethanet.com>  
Subject: Stealing an Election

In your analysis, you are comparing apples and oranges. The money spent on a campaign is either the candidate's own money, or donated in limited amounts (\$2000 for presidential candidates) by donors and carefully tracked. If someone wanted to spend the money illegally, they could (and would be better off) using money from people who wanted to donate more than the \$2000 (probably much more) and not pulling from that carefully tracked bank account.

As evidence of this, you know how much money they raised, \$3M-\$8M; don't you think someone would notice if \$1M went missing? There is potentially much more money available for

illegal campaign spending than legal spending because campaign finance reform laws don't apply.

There is even the potential that a wealthy "interested party" (company or individual) might spend the money to fix the election without the candidate even knowing about it.

From: Ethan Benatan <ethan.benatan@reed.edu>  
Subject: Re: Stealing an Election

It seems that the value of an election outcome might be only loosely related to the investment (historically and publicly) made in an attempt to win it. Campaign finance, even in the US, is fairly tightly controlled by law. Actual value might be better measured by the influence gained by the person taking office. This would certainly be a better predictor of the value of a switched vote.

It's also worth noting that potential attackers form a much larger group than the candidates themselves. In many cases they are also less risk-averse and better funded.

From: Pierre Szwarc <pierre.szwarc@laposte.net>  
Subject: National ID Cards

As a French citizen living in France, carrying an ID card is a mandatory thing for me. You're right, it doesn't add to ordinary security. However, it doesn't add to the delays and hindrances as you seem to fear. In all my 59 years, I've been asked for my ID card exactly \*once\* by the authorities in circumstances where I felt I didn't have to prove I'm me, and that was back in 1961, when terrorist attacks by French Algerian Nationalists (the OAS) were an everyday occurrence. I've been asked to prove my identity in many instances, and the ID card is then quite handy, exactly the same way an US citizen would use a driver's license: for getting a drink in a bar just after I was of drinking age, for example, or opening a bank account. Seen from Europe, the average American's concern for privacy in public places, as exemplified in TV serials and movies, looks like an overreaction to a nonexistent threat. Having been submitted to the Nazi domination for almost 6 years, and even though the generation who actually lived these terrible times is on the way to extinction, the average French citizen probably wouldn't stand for the Patriot Act as it was imposed on you, which makes your concern about such a minor thing as an ID card appear ludicrous to us.

From: Pierre Honeyman <phoneyman@telus.net>  
Subject: National ID Cards

\_Shake Hands with the Devil\_, Gen. Romeo D'Allaire's account of the genocide in Rwanda, contains an even more chilling reason to reject national ID cards.

The genocidaires in Rwanda used national ID cards to both find the victims of their genocide, and also to eradicate all records of their existence. The cards were checked to ensure that the right people were being murdered, then the cards were burned at the scene; meanwhile, bureaucrats complicit in the genocide removed records of the victims from that national databases, ensuring that the records confirmed these people had never existed.

The very thought of that potential use of national ID cards is chilling.

While it is an extremely compelling emotional argument to assert that such a thing could never happen here in the West, a good friend of mine from the former Yugoslavia assured me that that attitude was also prevalent there.

From: Arrigo Triulzi <arrigo@northsea.sevensesas.org>  
Subject: National ID Cards

Although I agree with everything you say about the uselessness of ID cards with respect to security, allow me to point out that there is a weak point in your discussion.

As an Italian citizen, I have been required since the age of 14 to carry a valid ID card (or passport) with me at all times when in Italy. Ever since that age, my ID card was checked only once, in 1991 during the first Gulf war. It was a rather unpleasant experience, involving armed policemen with submachine guns pointed at me, and being slammed against a wall approximately 100m from home -- all for the simple reason that I had left home with a large bag and home happened to be above the then-U.S. consulate (it has since moved so pointless, rude and rough security checks can be performed on other unfortunate souls guilty of the terrible sin of their landlord renting office space to the USA). Of course, it should also be mentioned that the same idiots who frisked me had seen me walk past their guard post innumerable times (the teams of four rotated between a small group of policemen), hence an even more pointless gesture "authorised" by the "heightened state of alert."

With the above exception, I have used my ID card for the following activities: to vote, to cross borders within Europe, to prove my identity when purchasing by cheque or credit card above a certain amount, to open a bank account, and to request other documents from the government.

That's pretty much it: no "interruptions" or "delays" due to "incessant ID checks."

From: Joao Luis Pinto <jpinto@inescporto.pt>  
Subject: National ID cards

I have the following comment on your article "National ID cards" in the April issue of your (excellent and interesting) CRYPTO-GRAM Newsletter:

I, for one, support the idea of a national ID card, provided it only aims at authenticating individuals, not in providing generic information on them.

I live in Portugal. The European (minus the UK) trend is to allow and to accept as natural the existence of national IDs, even with biometric information. The problem, particularly in my country, is that several other documents are required for particular functions, like driving licenses, Social Security cards and IRS identification cards, some of them even asserting identity in some scenarios. Some actions even require multiple documents. This absence of information cross-reference creates several problems. For example, notification of an address change has to be sent to several card issuing services.

I believe in a single ID replacing all the aforementioned ones, cross-referenced with context restricted information databases.

The sole function of that identity card would be to state that I am a unique person, with a particular address and a particular identifying number or code. No more, no less. All other information should reside in dedicated context-restricted databases, allowing easier setting of information access privileges (ex: the IRS should only know my fiscal data, not my criminal record). The (for example, smartcard-enabled) ID would have my (State) digitally signed photo and digitally signed fingerprint and/or iris-print, allowing card-present, in-place, identity verification. The ID should also provide a State Certificate Authority signed digital certificate that would assert my identity if required to do so digitally. Naturally this CA would have to be created, and would only be as "strong" as the cryptographic algorithms behind it (to say the most)... But this, I believe, is still stronger than the existing scenarios.

This would, I believe, benefit the assertion of identity, with a several level impact, on for example, web transaction security, credit card fraud and ID forgery. Also, it would be an important step to reduce the "impedance mismatch" that exists between "social" and "digital" and/or "on-line" authentication and identity.

From: Jonathan Bennett <jonathan.bennett@zdnnet.co.uk>  
Subject: Bluetooth Privacy Hack

Regarding the piece in the latest Crypto-Gram on Bluesnarfing. First, the trumpet-blowing bit: The Times didn't break this story. ZDNet UK covered Bluesnarfing extensively during February this year, drawing it to the attention of both vendors and politicians. That the journalist who wrote the article for The Times tried to get the details of one of our contacts from us illustrates this. See:

<<http://news.zdnnet.co.uk/communications/wireless/0,39020348,39145881,00.htm>> or <<http://tinyurl.com/22ptv>>  
<<http://news.zdnnet.co.uk/communications/wireless/0,39020348,39145886,00.htm>> or <<http://tinyurl.com/37816>>  
<<http://news.zdnnet.co.uk/communications/wireless/0,39020348,39146427,00.htm>> or <<http://tinyurl.com/3ezbv>>

Another reporter and I met Adam Laurie and witnessed Bluesnarfing taking place on a phone we took along, and were therefore sure wasn't tampered with. I can offer a bit more insight than the Times article gives -- I'm a specialist technology journalist. The vulnerability that allows Bluesnarfing appears to be an implementation problem in certain phones. There is little evidence to suggest this is a flaw in the Bluetooth security model, and Laurie agrees with this assessment. According to another consultant, the problem lies in how manufacturers implemented the object exchange (OBEX) protocol -- it allows the attacker to connect to the phone, ostensibly to use a service that doesn't require authentication, and then issue a request for a service that does, thus bypassing security.

I believe Bluesnarfing is less of an issue than Laurie or The Times would like you to think. Unlike Internet-based attacks, it needs physical proximity to the target. It's only certain models of phone that are vulnerable, and it's easy for the vendors to test for. There is a very simple work-around: Turn Bluetooth off. You can re-enable it for the short periods when you do need to use it.

It's also not the only way that sensitive details stored in phones are at risk -- it's far more likely that someone will leave a phone or PDA on the train after an evening's

drinking. Paper address books can be lost -- even newspaper reporters have been known to do this. This is before we start thinking about social engineering attacks. There are other things to worry about before we start to panic about Bluesnarfing.

We reported the issue since we believe that people do need to know about these things, and so people who have genuinely sensitive details stored on their phones can take steps against the attack. Reporting the issue also brings pressure on manufacturers to fix such problems and in that respect the Times article, late as it was, will do some good.

From: Paul Leeming <paul@leeming.cjb.net>  
Subject: TSA-Approved Locks

I just read your cryptogram about TSA-approved locks, and how you don't consider it a big problem because they can just break your existing lock anyway.

Being a former airline pilot, I look at the problem from a different perspective -- what if someone unscrupulous wants to put something IN your luggage? A master key would give luggage handlers the perfect tool to place drugs or other contraband into your luggage for collection at the other end. You then run the risk of being "caught" with that contraband, essentially being framed for a crime you didn't commit. It would also allow a potential terrorist to plant a small bomb INSIDE your case and give them plausible deniability since your case was "locked."

The real problem then becomes the fact that you don't KNOW that your luggage has been opened, whereas if your lock is missing because they broke it, you can report that fact to authorities and have them investigate (or at least create a paper trail in your defence).

From: Victor Bogado da Silva Lins <bogado@visgraf.impa.br>  
Subject: License Plate Cover

You mentioned in your last crypto-gram newsletter about a cover that makes a license plate impossible to read from certain angles. Brazilian people have thought in another low-tech solution for the same "problem", they simply tie some ribbons to the plate or the car itself; when the car is running (speeding) the ribbons fly and get in front of the plate making it difficult to read the plate.

From: Matthew Rubenstein <email@mattruby.com>  
Subject: Reader's Comment on "Security Benefits of Centralisation"

Drew Johnson has sent you a flawed analysis of "centralized security," falsely determining that "centralizing is good." His first scenario protects 10 \$100 deposits each with an "individual" safe that costs \$200 to break. But his safes are identical, so \$200 buys entry to not only the first safe, but to every one of the 10. So he has already "centralized" security, by protecting \$1000 with a single \$200 safe, in 10 parts. Bad strategy. His second scenario merely puts all the \$1000 into a single safe, and posits a break-in cost raised to only \$500. Both scenarios are centralized, both cost less than the value of the prize, both are insecure.

If Mr. Johnson were to put \$100 in each of 10 \*different\* \$200 safes, which won't \*all\*

fall once the first \$200 is spent to break in, he'd have decentralized his security and beaten the crooks. We have here a lesson not only in secure decentralization, but the security of polyculture, superior to the insecurity of monoculture.

From: "David Nasset, Sr." <david.nasset.sr@iname.com>  
Subject: Reader's Comment on "Security Benefits of Centralisation"

Drew made three mistakes, all stemming from this statement: "However, as all the virtual vault computers have identical vulnerabilities, the same attack can be replayed at minimal marginal cost (e.g. \$1)." In fact, the flaw Drew found applies, not to the individual ID cards at all, but only to the national ID.

Mistake #1: This statement assumes that the locks are identical. This is unlikely as, in the case of ID, the systems are likely to be very very different. MasterCard does not use the same security system as VISA, and they both use a different security system than the Washington State Department of Licensing, which is still different than Immigration. Thus, my bank card, credit card, driver's licence, and passport will likely not fall to the same attack. Only if the system used is the same is the same attack likely to work every time.

Mistake #2: Even if the \$100 locks are identical, it is still more profitable to go after the larger prize.

Suppose that Drew is right, and all \$200-rated locks are the same, and can fall to a vulnerability that takes only \$200 to find, and \$1 to exploit, getting the culprit \$100. The attacker then uses ten attacks, and gets \$1000, a profit of \$790 and a 478% overall increase in his investment.

Now, suppose he attacks the \$500 lock. He finds an exploit he can use for \$50 per attack (though \$1 is probably almost as likely). He now attacks ten different people's vaults. His cost? \$950. His gain? \$10,000, a profit of \$9,050, or 1052% increase on his investment.

Mistake #3: The vulnerability that Drew described is far worse if we do use the national ID card. If an exploit can be repeated cheaply, and we are all trapped in the same system, then everyone's money is locked up with the same \$500 lock.

Drew assumed that all of the \$1 locks would fall to the same exploit, which we have already established is unlikely. Thus, an attacker cannot get the special benefit of using the same attack cheaply over and over.

However, everyone who uses the \$500 lock (national ID) is required to use the same lock. With the other locks, the locks are forced by circumstance to be different frequently, and, in many cases (Visa vs. MasterCard), the choice of lock is in the hands of the lock's purchaser. At worst, the attacker can attack all Visas, or all Washington State driver's licences, or all US passports. However, with national ID cards, you have no choice. A repeatable exploit that works on one will work on ten, or a hundred, or a thousand different people, and when it works, it gets everything.

So, I'll stick with a system where the worst likely exploit gets many people's small piles, and I lose a small one, rather than go with a system where the same result means everybody loses everything that's being locked up.

