CRYPTO-GRAM, July 15, 2004

Published By: *Bruce Schneier*
Posted By: David Isecke
7/15/2004 13:01

CRYPTO-GRAM

July 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.

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

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

In this issue:

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

Due Process and Security

The U.S. Supreme Court recently decided the three legal challenges to the Bush administration's legal maneuverings against terrorism. These cases have been endlessly debated on legal and civil liberties grounds. They were decided, mostly but not entirely, in favor of presumption-of-innocence and due process.

But I want to talk about how important the decisions are to our nation's security. Security is multifaceted; there are many threats from many different directions. It includes the security of people against terrorism, and also the security of people against tyrannical government.

The three challenges are all similar, with slight variations. In one case, the families of 12 Kuwaiti and two Australian men imprisoned in Guantanamo Bay argue that their detention is an illegal one under U.S. law. In the other two cases, lawyers argue whether U.S. citizens -- one captured in the U.S. and the other in Afghanistan -- can be detained indefinitely without charge, trial, or access to an attorney. In all these cases, the administration argues that these detentions are lawful, based on the current "war on terrorism." The complainants argue that these people have rights under the U.S. Constitution, rights that cannot be stripped away.

There are some very broad security issues at work here. The Constitution (which

There are some very broad security issues at work here. The Constitution (which includes the Bill of Rights) was designed to ensure the security of people: American citizens and visitors. Its limitations on governmental power are a security measure. Its enshrinement of human rights is a security measure. These measures were developed in response to colonial tyranny by Britain, and have been extended in response to abuses of power within our own country. Laws mandating speedy trial by jury, laws prohibiting detention without charge, laws regulating police behavior -- these are all laws that make us more secure. Without them, government and police power remains unchecked.

The case of Jose Padilla is a good illustration. Arrested in Chicago in May 2002, he has never been charged with a crime. John Ashcroft held a press conference accusing him of trying to build a "dirty bomb," but no court has ever seen any evidence to support this accusation. If he's guilty, he deserves punishment; there's no doubt about that. But the way to determine guilt or innocence is by a trial on a specific indictment (charge or accusation of a crime). Without an indictment, there can be no trial, and the prisoner is held in limbo.

Surely none of us wants to live under a government with the right to arrest anyone at any time for any reason, and to hold that person indefinitely without trial.

The Bush administration has countered that it cannot try these people in public because that would compromise its methods and intelligence. Our government has made this claim before, and invariably it turned out to be a red herring. In 1985, retired Naval officer John Walker was caught spying for the Soviet Union; the evidence given by the National Security Agency was enough to convict him without giving away military secrets. More recently, John Walker Lindh -- the "American Taliban" captured in Afghanistan -- was processed by the justice system, and received a 20-year prison sentence. Even during World War II, German spies captured in the U.S. were given attorneys and tried in public court.

We need to carry on these principles of fair and open justice, both because it is the right thing to do and because it makes us all more secure. The United States is admired throughout the world because of our freedoms and our liberties. The very rights inherent in these Supreme Court cases are the rights that keep us all safe and secure. The more our fight against terrorism is conducted within the confines of law, the more it gives consideration to the principles of fair and open trial, due process, and "innocent until proven guilty," the safer we all are.

Unchecked police and military power is a security threat -- just as important a threat as unchecked terrorism. There is no reason to sacrifice the former to obtain the latter, and there are very good reasons not to.

A version of essay was published in the Minneapolis Star Tribune.
<http://www.startribune.com/stories/562/4843840.html>

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

Security Notes from All Over:
X-Ray Machines and Building Security

The other week I visited the corporate headquarters of a large financial institution on Wall Street; let's call them FinCorp. FinCorp had pretty elaborate building security. Everyone -- employees and visitors -- had to have their bags X-rayed.

Seemed silly to me, but I played along. There was a single guard watching the X-ray machine's monitor, and a line of people putting their bags onto the machine. The people themselves weren't searched at all. Even worse, no guard was watching the people. So when I walked with everyone else in line and just didn't put my bag onto the machine, no one noticed.

It was all good fun, and I very much enjoyed describing this to FinCorp's VP of Corporate Security. He explained to me that he got a $5 million rate reduction from his insurance company by installing that X-ray machine and having some dogs sniff around the building a couple of times a week.

I thought the building's security was a waste of money. It was actually a source of corporate profit.

The point of this story is one that I've made in "Beyond Fear" and many other

places: security decisions are often made for non-security reasons. When you encounter a security risk that people worry about inordinately, a security countermeasure that doesn't counter the threat, or any security decision that makes no sense, you need to understand more of the context behind the decision. What is the agenda of the person who made the decision? What are the non-security considerations around the decision? Security decisions make sense, as long as you understand them properly.

Much more about this can be found in "Beyond Fear":
<http://www.schneier.com/bf.html>

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

Cryptographers and U.S. Immigration

Seems like cryptographers are being questioned when they enter the U.S. these days. Recently I received this (anonymous) comment: "It seems that the U.S. State Department has a keen interest in foreign cryptographers: Yesterday I tried to renew my visa to the States, and after standing in line and getting fingerprinted, my interviewer, upon hearing that my company sells [a cryptography product], informed me that "due to new regulations," Washington needs to approve my visa application, and that to do so, they need to know exactly which companies I plan to visit in the States, points of contact, etc. etc. Quite a change from my last visa application, for which I didn't even have to show up."

I'm curious if any of my foreign readers have similar stories. There are international cryptography conferences held in the United States all the time. It would be a shame if they lost much of their value because of visa regulations.

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

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.

How to Fight:
<http://www.schneier.com/crypto-gram-0307.html#1>

Crying Wolf:
<http://www.schneier.com/crypto-gram-0307.html#8>

Embedded Control Systems and Security:
<http://www.schneier.com/crypto-gram-0207.html#1>

Phone Hacking: The Next Generation:
<http://www.schneier.com/crypto-gram-0107.html#1>

Monitoring First:
<http://www.schneier.com/crypto-gram-0107.html#5>

Full Disclosure and the CIA:
<http://www.schneier.com/crypto-gram-0007.html#1>

Security Risks of Unicode:
<http://www.schneier.com/crypto-gram-0007.html#9>

The Future of Crypto-Hacking:
<http://www.schneier.com/crypto-gram-9907.html#hacking>

Bungled SSL:
<http://www.schneier.com/crypto-gram-9907.html#doghouse>

Declassifying Skipjack:
<http://www.schneier.com/crypto-gram-9807.html#skip>

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

Security and Portable Storage Devices

I recently read a research report about the security threat from portable storage devices. Pocket USB drives, MP3 players, portable FireWire drives, and the like are becoming larger, faster, and more common. The research report suggests that companies go so far as to restrict the use of these devices.

I think this is kind of silly. Yes, these devices can store a lot of data. But so can DVDs. And CDs. And before that, floppies held a lot of data. (Data was smaller then.) And don't forget paper.

There are two separate issues here: deliberate copying and stealing of information, and inadvertent copying and leaking.

Regarding the former, banning iPods and USB devices doesn't do any good...because the thief will ignore the ban. USB thumb drives are tiny. What are you going to do, strip search everyone who goes in and out of the building? The ban is a silly countermeasure that annoys all your innocent employees and doesn't faze the potentially guilty ones.

Regarding the latter, it may do some good but not enough to make it worthwhile. Exactly how is my iPod going to accidentally download sensitive files, and then accidentally upload them somewhere insecure? I use my USB thumb drive for file transfer because it's easier than a CD-R. It's not magically more or less dangerous than a CD-R.

The report also talks about the risk of these devices accidentally introducing malicious code into the network. This is a risk, sure, but it's also a risk to allow employees to plug laptops into the network, bring floppy disks from home, and do half a dozen other things. The way to secure a network from these sorts of attacks is through ubiquitous antivirus software, not by trying to control what sorts of devices an employee can use.

I used to work for the U.S. Department of Defense, and every evening when I left work a guard searched the papers in my bag. Back then, computers were still new and the real risk was papers marked "Confidential," "Secret," or worse. Once in a while the guards would catch someone taking classified material out of the building, but it was never someone doing it maliciously. (If it had been, he would have hid the papers better.) It was someone who forgot. Outside of a military environment, this sort of countermeasure just isn't worth it...and probably isn't for most military installations.

It's a big deal to have confidential information leave an organization's building, and it's been a big deal since long before computers. In the end, you have to trust your employees. If they want to steal information, or if they make mistakes, they'll do it regardless of your precautions. You can change the mechanisms of those actions, but don't confuse changing mechanisms with making things safer.

<http://www.eweek.com/article2/0,1759,1621809,00.asp>
<http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C94319%2C00.html> or <http://tinyurl.com/6k7o7>

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

News

Artfully concealed items confiscated by TSA screeners:
<http://www.tsa.gov/public/display?theme=8&content=090005198009a3cf> or <http://tinyurl.com/4elm3>
Interesting, but also confusing. Who were these people who tried to conceal knives and sneak them onto airplanes? Were they hijackers, random loonies, or people trying to evade airport security because they didn't want to check baggage? I think the motivations of the people makes a lot of difference.

An overview of steganography, from the point of view of computer forensics:
<http://www.garykessler.net/library/fsc_stego.html>

The Minneapolis-St. Paul International Airport is testing a new security system: travelers can bypass long security lines by subjecting themselves to advance security checks. I'm curious to see how this system fares, but I am skeptical about its widespread adoption. As a high-level frequent flyer, I can already bypass long lines at most airports by using special lanes. First-class passengers get the same privileges. But who else would use a system like this? I can't figure out who it is targeted towards.
<http://www.boston.com/business/articles/2004/06/28/minn_airport_starts_advance_security_checks> or <http://tinyurl.com/5z48t>

<http://www.cnn.com/2004/US/Midwest/06/28/airport.background.checks.ap/index.html> or <http://tinyurl.com/2v8gu>
<http://www.startribune.com/stories/1631/4847379.html>
<http://www.startribune.com/stories/1576/4864503.html>

Analysis of the Voynich Manuscript:
<http://www.sciam.com/article.cfm?chanID=sa006&colID=1&articleID=0000E3A-70E1-10CF-AD1983414B7F0000> or <http://tinyurl.com/2xung>

Popular back-door program has a back-door in it.
<http://www.securityfocus.com/news/8893>

Avoiding identity theft: a primer.
<http://www.securityfocus.com/news/8908>

Torture has been in the news since 9/11, most recently regarding the U.S. military's practices at the Abu Ghraib prison in Iraq. Politics isn't my area of expertise, and I don't want to debate the politics of the scandal. I don't even want to debate the moral issues: Is it moral to torture a bomber to find a hidden ticking bomb, is it moral to torture an innocent to get someone to defuse a ticking bomb, is it moral to torture N-1 people to save N lives? What interests me more are the security implications of torture: How well does it work as a security countermeasure, and what are the trade-offs? This is an excellent pair of essays about how ineffective torture really is. Given that torture doesn't actually produce useful intelligence, why in the world are we spending so much good will on the world stage to do it?
<http://www.salon.com/opinion/feature/2004/06/18/torture_1/index.html> or <http://tinyurl.com/57668>
<http://www.salon.com/opinion/feature/2004/06/21/torture_algiers/index.html> or <http://tinyurl.com/4v29z>

Great talk by Cory Doctorow on digital rights management:
<http://craphound.com/msftdrm.txt>

It's still easy to fool fingerprint scanners:
<http://www.ep.liu.se/exjobb/isy/2004/3557/>

Good article about sloppy programming and security:
<http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=160>

CERT is advising people not to use Internet Explorer. (Me, I'm a happy Opera user.)
<http://www.theregister.co.uk/2004/06/28/cert_ditch_explorer/>

Great article on the origins of an Internet hoax: the one about Bill Gates paying to track your e-mail.
<http://www.wired.com/wired/archive/12.07/hoax.html>

Seven habits of highly secure companies:
<http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=56003>

Forget about the issues. Who has the more secure website: Bush or Kerry?
<http://www.wired.com/news/infostructure/0,1377,64036,00.html>

Airport security put real explosives in a piece of luggage to test some bomb-sniffing dogs. Problem #1: they lost track of the bag. Problem #2: it was a real piece of luggage belonging to an unwitting passenger.
<http://www.alibi.com/editorial/section_display.php?di=2004-05-20&scn=news#8167> or <http://tinyurl.com/6q4as>

The timeline for fixing a Mozilla security flaw. It's amazing how quickly and competently it was handled:
<http://www.sacarny.com/blog/index.php?p=104>

Hacking for profit:
<http://www.computerworld.com/securitytopics/security/story/0,10801,94407,00.html?nas=SEC-94407> or <http://tinyurl.com/4k46u>

FBI's Guide to Concealable Weapons:
<http://datacenter.ap.org/wdc/fbiweapons.pdf>

Report on the security of Canadian DOD networks:
<http://www.canada.com/national/nationalpost/news/story.html?id=d47120ad-92eb-40d0-a9c3-f47216966493> or <http://tinyurl.com/6uhlm>

Here's a great security attitude. The article discusses a hole in Friendster that allows users to obtain information about who is looking at their online profiles

allows users to obtain information about who is looking at their online profiles. "Notified of the security holes Moore and Chisholm exploit, Friendster rep Lisa Kopp insists, 'We have a policy that we are not being hacked.' When I explain that, policy or no, they are being hacked, she says, 'Security isn't a priority for us. We're mostly focused on making the site go faster.'"
<http://www.wired.com/wired/archive/12.06/dating_pr.html>

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

Counterpane News

Counterpane has a new white paper on how monitoring helps with compliance. As more and more companies fall under the perview of Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, etc., complaince will become more important to security
<http://www.counterpane.com/compliance.html>

And we have another paper about our Enterprise Protection Suite, our comprehensive security service package. Centered around monitoring, EPS is a way for companies to get their networks secure -- fast.
<http://www.counterpane.com/overview.html>

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

Security Notes from All Over: Coca-Cola and the NSA

Coca-Cola has a new contest. Hidden inside 100 cans of Coke there's a SIM card, GPS transmitter, and a microphone. The winners activate the Coke can by pressing a button, which will call a central monitoring facility. Then Coke tracks the winners down using the GPS transmitter and surprises them with their prize.

NSA engineers drink Coke. Lots and lots of Coke. The possibility that an active microphone in a Coke can could be in one of the NSA's highly secure facilities is worth considering. A reasonable threat analysis might look like this: "You know, the chances that one of these 100 cans out of hundreds of millions of cans ends up in our building is extremely small -- somewhere around 1 in 100,000 -- so it's not worth worrying about."

But the NSA's Information Staff Security Office) decreed differently: "It is important that ALL cans of Coca-Cola within our spaces be inspected. This includes cans already in our buildings and those being delivered on a daily basis. If you discover one of these cans, DO NOT activate it. Instead, you should alert your ISSO immediately and report the incident."

This is hysterical. Can you imagine inspecting every can of Coke entering the NSA, opening each of the hundreds of cases of Coke and inspecting every can for a GPS transmitter? What does this cost? What is the NSA not doing because they're doing this instead?

Of course the engineers at NSA are already starting to create Coke cans with antennas, circuit boards, and keypads. They are leaving them around snack messes as practical jokes.

And where's Pepsi in all of this? Shouldn't they be advertising "surveillance-free cola"?

Funny stuff, but there's a serious point here. Again and again, security decisions are clouded by agenda. The NSA's Coca-Cola inspection policy is an example of CYA. Some executive within NSA didn't want to be personally responsible for a GPS receiver slipping through security, so he decided that everything should be inspected. It's a small risk to the greater population, but it's a larger risk to him. His agenda is different from that of society's, but because his agenda matters more to him and it's his decision, his is what gets followed.

We as a society need to figure out how to make security trade-off decisions another way. Having specific individuals or corporations make security trade-offs for us based on their agenda isn't making us more secure, and it's costing us a whole lot of money.

<http://www.wired.com/news/technology/0,1282,64078,00.html>

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

The Doghouse: ICS

ICS of Atlanta has developed the "Tree" cryptographic algorithm.

How is Tree different? Well, for one thing, it "uses no math." I'm not quite sure how that's possible on a computer, but that's what Tree's creator claims. From an e-mail exchange: "...99.99% of the people out there use math to encode and they use math to 'break' the code. Since we don't really use math, it would be quite hard to break."

Not only do they not use math, they don't have a key. "Tree does not use a 'key'.... I just put in text, hit 'encode' and poof, there is the encoded message, to decode, I put in coded messages, hit 'decode' and poof, done. That's it. No key."

Amazing.

How do they demonstrate Tree's security? "Over 100 professionals in mathematics & in computer science at Massachusetts Institute of Technology & at Georgia Tech, had sample encoded messages submitted to them. Not a single person could break this code!" Think about it. These guys sent unsolicited e-mails containing some ciphertext to over 100 professionals, and not one of them decrypted the messages. Anyone have any other explanations for this behavior, other than the possibility that these 100 professionals immediately dropped what they were doing and spent fruitless weeks trying in vain to break Tree?

And if all that isn't enough to make you run screaming from these guys, their website proudly proclaims: "Tree Encoded Files Can Be 'Zipped.'"

That's right; their encryption is so lousy that the ciphertext doesn't even look random.

<http://icsatlanta.netfirms.com/>

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

The CLEAR Act Does Not Help Fight Terror

Danny Sigui lived in Rhode Island. After witnessing a murder, he called 911 and became a key witness in the trial. In the process, he unwittingly alerted officials of his immigration status. He was arrested, jailed, and eventually deported.

In a misguided effort to combat terrorism, some members of Congress want to use the National Crime Information Center (NCIC) database to enforce federal civil immigration laws. The idea is that state and local police officers, who check NCIC in routine situations, will be able to assist the federal government in enforcing our nation's immigration laws. There are a limited number of immigration agents at the Department of Homeland Security, so asking the 650,000 state, local, and tribal police officers to help would be a significant "force multiplier."

The problem is that this idea, currently a pair of legislations in draft called the CLEAR Act and the Homeland Security Enhancement Act (HSEA), aren't going to help fight terrorism. Even worse, this will put an unfunded financial burden on local police forces, and is likely to make us all less safe in the long run.

Security is a trade-off. It's not enough to ask: "Will increased verification of immigration status make it less likely that terrorists remain in our country?" We have to ask: "Given the police resources we have, is this the smartest way to deploy them?"

The CLEAR Act and HSEA will certainly result in more people being arrested for immigration violations, but will probably have zero effect on terrorism. Some of the 9/11 terrorists were in the country legally. Others were easily able to keep their heads down. It's not as if terrorists are waiting to be arrested, if only the police have sufficient information about their immigration status. It's a nice theory, but it's just not true.

And none of this comes cheaply. The cost of adding this information to criminal databases easily runs into the tens of millions of dollars. The cost to the local police forces of enforcing these immigration laws is likely to be at least ten times that. And this cost will have to be borne by the community, either through extra taxes or by siphoning police from other duties. I can't think of a single

extra taxes or by siphoning police from other duties. I can't think of a single community where the local police are sitting around idly, looking for something else to do. Forcing them to become immigration officers means less manpower to investigate other crimes. And this makes us all less safe.

Terrorists represent only a very small minority of any culture. One of the most important things that a good police force does is maintain good ties with the local community. If you knew that every time you contacted the police, your records would be checked for unpaid parking tickets, overdue library fines, and other non-criminal violations, how would feel about policemen? It's far more important that people feel confident, and safe, when calling the police.

When a Muslim immigrant notices something fishy going on next door, we want him to call the police. We don't want him to fear that the police might deport him or his family. We don't want him hiding if the police come to ask questions. We want him, and the community, on our side.

By turning police officers into immigration agents, the CLEAR Act and HSEA will discourage the next Danny Sigui from coming forward to report crimes or suspicious activities. This will harm national security far more than any security benefits received from catching non-criminal immigration violations. Add to that the costs of having policemen chasing immigration violators rather than responding to real crimes, and you've got a really bad security trade-off.

This essay was originally published on CNet:
<http://news.com.com/CLEARly+muddying+the+fight+against+terror/2010-7348_3-5236260.html> or <http://tinyurl.com/2yb9x>

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

Comments from Readers

From: Anonymous
Subject: Witty

You said: "Witty was speedily written. Security company eEye discovered the vulnerability in ISS's BlackICE/RealSecure products on March 8, and ISS released a patched version on March 9. eEye published a high-level description of the vulnerability on March 18. On the evening of March 19, about 36 hours after eEye's public disclosure, the Witty worm was released into the wild."

We updated our BlackIce on March 17th (Wed) and subsequently checked from inside the updated version that no further updates were available (also on Wed). On 20th (Sat) Witty arrived and the computer in question was destroyed.

The most noticeable thing about this to me is the spin ISS put out to suggest it wasn't a big problem. Patch available a week in advance -- no way (and yes, I do have a valid support contract). I'd have preferred it if they put more effort into telling people about the fix than revising history later; unfortunately, the latter is probably more cost-effective for new and unaffected customers, and the others are perhaps "lost" anyway.

It took me half a day to remake the computer and a few things were lost, but nothing of great importance. Where this trend in destructive viruses really alarms me is with home users who keep "prized" possessions on their computers, such as un-backed-up digital photos of important events. Destroying this kind of data is a nasty crime in my book. (Plus in a world where computers are increasingly seen as appliances, the number of opportunities for this sort of damage will only increase.)

I hope Witty will actually improve things, by showing vendors of "protection" products that flaws in them are particularly critical, and if they don't behave in an exemplary manner it will hurt them in the wallet as they lose customers they won't be getting back. I think this is the only process likely to help with Witty-alikes. Unfortunately, as in politics, I suspect many firms will still feel it's cheaper to invest in PR after the event than better behavior before. Here's hoping I'm wrong.

From: Mart van de Wege
Subject: One-time codes for electronic banking

I spotted this little bit in your June Crypto-Gram: "For additional security, she then pulls out a card that has 50 scratch-off codes. Jubran uses the codes, one by one, each time she logs on or performs a transaction. Her bank, Nordea PLC, automatically sends a new card when she's about to run out."

automatically sends a new card when one's about to run out.

I get a feeling that Wired is a bit behind in its coverage. This system has been in use by the Dutch bank Postbank for several years already.

Its Girotel system works by first requiring a user login with a so-called GIN (Gebruikers Identificatie Nummer, translated User Identification Number). After that Girotel requires all transactions to be confirmed with a Transaction Authentication Number (TAN). These TAN codes are supplied as a list on paper to the client, and are replenished as soon as the client has only a limited number left (I believe the threshold is 10, but I'm not sure).

This system has been functioning for at least 10 years to this date, to the great satisfaction of both the bank and the users. Its platform-neutral nature has allowed Postbank to upgrade its software from a standalone client that would dial-in directly to an online version, with no change in the interface, and no compromise to security.

From: "Bryan L. Fordham"
Subject: National ID cards

People in Europe said "I've had the national ID card for X number of years, and I only had to show it once to police. Otherwise I use it to vote, buy drinks, etc."

This seems to strengthen the argument against such IDs, not hurt it. If you only had to show it once it's not terribly useful; how does it help security? And second, my driver license already allows me to show my age and prove I'm me when I go to vote. Why do we need another card?

From: "Steven Shaer"
Subject: Iranian whatever....

Regarding your article on the Iranian code breaking, I think you have ignored another obvious (IMHO) scenario: Perhaps the CIA/NSA purposely leaked to Chalabi that they had the Iranian codes broken and perhaps the reason was that they didn't have the codes broken. One can think of a number of different scenarios where you would want your adversary to THINK he had your codes broken when you didn't, including that the U.S. wanted Iran to change their technology to a technology they had a back door into from the current technology they didn't have a back door into! Another possible reason would be to throw suspicion within the Iranian government on certain individuals which would be beneficial to U.S. interests.

From: Toby Bryans
Subject: Re: Cell Phone Jamming and Terrorist Attacks

This whole thing is particularly annoying as the only functionality of the mobile phones that was used during the attacks was the alarm. They were not called to detonate -- they all had an alarm set for a particular time: they don't even have to be on, as particular brands of phone can turn themselves on if an alarm is due.

Blocking mobile phones will not make any difference to this attack. You may as well ban people from wearing wristwatches...

Of course, there are examples of political opportunism on both sides of the pond:

<http://news.bbc.co.uk/1/hi/uk_politics/3602019.stm>

...would of course also make no difference with this particular attack.

From: Alexey Kirpichnikov
Subject: Photographing Subways and Terrorist Attacks

I live in Ekaterinburg, Russia and I'd like to say that photography is still prohibited in our subway. I don't know the reason and this seems quite funny to me. I think that even security officers here understand that this ban has no sense at all, because my friends tried to take photos in subway and it was ignored by policemen.

Still, "no photo and video" signs are everywhere in subway stations.

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

CRYPTO-GRAM is a free monthly newsletter providing summaries, analyses, insights, and commentaries on security: computer and otherwise. Back issues

insights, and commentaries on security: computer and otherwise. Back issues are available on <http://www.schneier.com/crypto-gram.html>.

To subscribe, visit <http://www.schneier.com/crypto-gram.html> or send a blank message to crypto-gram-subscribe@chaparraltree.com. To unsubscribe, visit <http://www.schneier.com/crypto-gram-faq.html>.

Comments on CRYPTO-GRAM should be sent to schneier@counterpane.com. Permission to print comments is assumed unless otherwise stated. Comments may be edited for length and clarity.

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

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

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