

THE CPIRC NEWS



Happy Holidays To All Our Readers & A Special Thanks To Our Members

Inside this issue:

A Holiday Message	1
Did NSA Put a Secret Backdoor in New Encryption Standard?	2-3
Google Street View May Be Illegal In Canada	4-5
Interrogation Procedures: Promises of Leniency	7-9
Resource Centre Roundup	6, 10
Contact Information	11

We have come to the end of another year and everyone at The Canadian Private Investigators' Resource Centre wanted to take this moment to say THANKS to everyone who contributed in making CPIRC a success in 2007.

To our partners– By supporting us in giving our members discounts on everything from purchases of surveillance equipment, training (tactical, practical & theoretical) and rentals to aid our members on any particular contract.

Finally a SPECIAL THANKS to all our Canadian and International members, new and veteran alike who supported us in 2007 and in previous years since 1999 by financially contributing to the site. Literally paying for our website, its maintenance, constant Resource Centre updates, newsletters and site marketing that all our members benefit from. Their contributions are worth far more than the membership dues they pay - without them, we wouldn't have a site.

From everyone at The Canadian Private Investigators' Resource Centre to all of you

**Have A Great Holiday
And A Safe And
Successful 2008!**

Did NSA Put a Secret Backdoor in New Encryption Standard?

Random numbers are critical for cryptography: for encryption keys, random authentication challenges, initialization vectors, nonces, key-agreement schemes, generating prime numbers and so on. Break the random-number generator, and most of the time you break the entire security system. Which is why you should worry about a new random-number standard that includes an algorithm that is slow, badly designed and just might contain a backdoor for the National Security Agency.

Generating random numbers isn't easy, and researchers have discovered lots of problems and attacks over the years. A recent paper found a flaw in the Windows 2000 random-number generator. Another paper found flaws in the Linux random-number generator. Back in 1996, an early version of SSL was broken because of flaws in its random-number generator. With John Kelsey and Niels Ferguson in 1999, I co-authored Yarrow, a random-number generator based on our own cryptanalysis work. I improved this design four years later – and renamed it Fortuna – in the book *Practical Cryptography*, which I co-authored with Ferguson.

The U.S. government released a new official standard for random-number generators this year, and it will likely be followed by software and hardware developers around the world. Called NIST Special Publication 800-90 (.pdf), the 130-page document contains four different approved techniques, called DRBGs, or "Deterministic Random Bit Generators." All four are based on existing cryptographic primitives. One is based on hash functions, one on HMAC, one on block ciphers and one on elliptic curves. It's smart cryptographic design to use only a few well-trusted cryptographic primitives, so building a random-number generator out of existing parts is a good thing.

But one of those generators – the one based on elliptic curves – is not like the others. Called Dual_EC_DRBG, not only is it a mouthful to say, it's also three orders of magnitude slower than its peers. It's in the standard only because it's been championed by the NSA, which first proposed it years ago in a related standardization project at the American National Standards Institute.

The NSA has always been intimately involved in U.S. cryptography standards – it is, after all, expert in making and breaking secret codes. So the agency's participation in the NIST (the U.S. Commerce Department's National Institute of Standards and Technology) standard is not sinister in itself. It's only when you look under the hood at the NSA's contribution that questions arise.

Problems with Dual_EC_DRBG were first described in early 2006. The math is complicated, but the general point is that the random numbers it produces have a small bias. The problem isn't large enough to make the algorithm unusable – and Appendix E of the NIST standard describes an optional work-around to avoid the issue – but it's cause for concern. Cryptographers are a conservative bunch: We don't like to use algorithms that have even a whiff of a problem.

But today there's an even bigger stink brewing around Dual_EC_DRBG. In an informal presentation (.pdf) at the CRYPTO 2007 conference in August, Dan Shumow and Niels Ferguson showed that the algorithm contains a weakness that can only be described a backdoor.

This is how it works: There are a bunch of constants – fixed numbers – in the standard used to define the algorithm's elliptic curve. These constants are listed in Appendix A of the NIST publication, but nowhere is it explained where they came from.

What Shumow and Ferguson showed is that these numbers have a relationship with a second, secret set of numbers that can act as a kind of skeleton key. If you know the secret numbers, you can predict the output of the random-number generator after collecting just 32 bytes of its output. To put that in real terms, you only need to monitor one TLS internet encryption connection in order to crack the security of that protocol. If you know the secret numbers, you can completely break any instantiation of Dual_EC_DRBG.

The researchers don't know what the secret numbers are. But because of the way the algorithm works, the person who produced the constants might know; he had the mathematical opportunity to produce the constants and the secret numbers in tandem.

Of course, we have no way of knowing whether the NSA knows the secret numbers that break Dual_EC_DRBG. We have no way of knowing whether an NSA employee working on his own came up with the constants – and has the secret numbers. We don't know if someone from NIST, or someone in the ANSI working group, has them. Maybe nobody does.

We don't know where the constants came from in the first place. We only know that whoever came up with them could have the key to this backdoor. And we know there's no way for NIST – or anyone else – to prove otherwise.

This is scary stuff indeed.

Even if no one knows the secret numbers, the fact that the backdoor is present makes Dual_EC_DRBG very fragile. If someone were to solve just one instance of the algorithm's elliptic-curve problem, he would effectively have the keys to the kingdom. He could then use it for whatever nefarious purpose he wanted. Or he could publish his result, and render every implementation of the random-number generator completely insecure.

It's possible to implement Dual_EC_DRBG in such a way as to protect it against this backdoor, by generating new constants with another secure random-number generator and then publishing the seed. This method is even in the NIST document, in Appendix A. But the procedure is optional, and my guess is that most implementations of the Dual_EC_DRBG won't bother.

If this story leaves you confused, join the club. I don't understand why the NSA was so insistent about including Dual_EC_DRBG in the standard. It makes no sense as a trap door: It's public, and rather obvious. It makes no sense from an engineering perspective: It's too slow for anyone to willingly use it. And it makes no sense from a backwards-compatibility perspective: Swapping one random-number generator for another is easy.

My recommendation, if you're in need of a random-number generator, is not to use Dual_EC_DRBG under any circumstances. If you have to use something in SP 800-90, use CTR_DRBG or Hash_DRBG.

In the meantime, both NIST and the NSA have some explaining to do.

*Bruce Schneier is CTO of BT Counterpane and author of *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*.*

Google Street View May Be Illegal In Canada

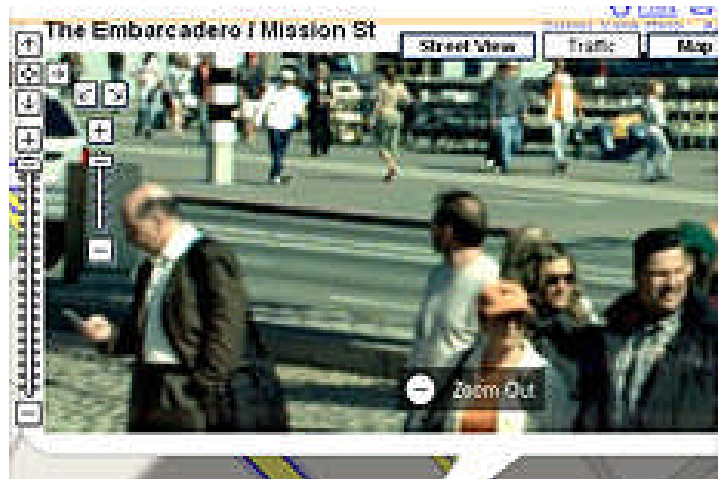
Privacy commissioner concerned about new application

Canada's privacy commissioner has been googling Google, and she's raising concerns over the search engine's new Street View web photo application.

Jennifer Stoddart says many of the street-level images Google is making available on the internet could break Canada's privacy laws.

Street View isn't yet available in Canada but has been expanding in the United States since being launched in May.

Stoddart has written to Google, and Calgary-based Immersive Media – which helped develop the imagery technology for Street View – asking both companies to respond to her concerns.



"I am concerned that, if the Street View application were deployed in Canada, it might not comply with our federal privacy legislation," Stoddart says in a letter to David Drummond, Google's senior vice-president of corporate development and chief legal officer.

"In particular, it does not appear to meet the basic requirements of knowledge, consent, and limited collection and use as set out in the legislation."

Removing images at request not enough

A number of websites carry satellite images or low-resolution photographs and video.

Stoddart doesn't have a problem with those. However, she warned that high-resolution pictures such as those available on Street View could contravene the Personal Information Protection and Electronic Documents Act, which came into effect on Jan. 1, 2004.

"Our Office considers images of individuals that are sufficiently clear to allow an individual to be identified to be personal information within the meaning of PIPEDA," Stoddart writes.

Of particular concern to Stoddart is that the images on Street View appear to have been collected largely without the consent of the people in them. Street View does allow viewers to request their images be removed. However, by then, Stoddart says, it's too late.

"This is only a partial solution ... given that individuals may not be aware that images relating to them are on Street View," she said.

"By the time individuals become aware that images relating to them are contained in Street View, their privacy rights may already have been affected."

In a letter to Immersive Media's CEO Myles McGovern, the commissioner said she is aware the company already has images of Canada in its database.

The firm's website specifically refers to pictures from Vancouver, Calgary, Toronto, Ottawa, Montreal and Quebec City being among the more than 60,000 kilometres of imagery captured in North America.

Stoddart's office has not given Google or Immersive Media a specific deadline for responding to her concerns.

© The Canadian Press, 2007



Resource Centre Roundup

The Guinness World Records Book for The Smallest Audio Recorders In The World!

We at CPIRC are proud to announce that we are now official distributors for the world's smallest audio recorders. These tiny digital voice recorders feature:

- High acoustic sensitivity (up to 7-9 meters)
- Wide dynamic range (up to 72 dB)
- Linear and loop recording modes
- Voice Activation System
- Timer to start recording on a present time, once and repeatedly
- Built-in real time clock and calendar
- Watermark protection
- Power supply from rechargeable batteries, solar batteries, and batteries
- Much more

We currently have a limited time promotion on 3 different digital voice recorders. Please visit www.cpirc.com/specials.html for more details.

New stories and Publications of Interest that you'll find in the Resource Centre

- Audio Forensics Experts Reveal (Some) Secrets
- Cellphone Jammers
- CIA Plans Social Networking Site For Spies
- Companies Turn To Private Spies
- How To Surf The Web Anonymously With Proxies
- Tenants Find Eavesdropping Bug In Cabinet

Sending Self Destructing Emails

Email may seem like a private communication. In reality, it is anything but. Your email can be copied, stored and forwarded. Messages can be forwarded to others without your permission. Stored email can return to haunt you, long after you've forgotten it. What can you do? Try blowing 'em up!

Click on the FREE [Self Destructing Email](#) links found in the "[Free Investigative Software & Publication Downloads](#)" category in the Resource Centre.

Interrogation Procedures: Promises of Leniency

For a confession to be admissible as evidence it must not only be trustworthy, but also voluntary. The test of voluntariness answers the question, “was a statement made of the suspect’s free will?” The concept of “free will” has a somewhat different meaning in law than it does in psychology. A psychologist would argue that if a person is able to make any behavioral choice he is operating from his own free will. Legally, however, the concept of free will relates to whether a statement was made in the absence of threats or other inducements. These “other inducements” generally refer to promises of leniency.

Promises of leniency occur on a continuum ranging from statements that clearly offer a lesser sentence, “If you confess, I will make sure you don’t do hard time,” to statements that merely imply leniency in exchange for a confession, e.g., “I want to help you out on this thing.” The Canadian Supreme Court has established a quid pro quo guideline in evaluating promises of leniency. In other words, only statements that clearly offer the suspect leniency in exchange for a confession are prohibited.[1] The U.S. Supreme Court will consider even implied promises of leniency as part of the totality of circumstances in determining a confession’s admissibility.

The courts’ concern over promises of leniency is that an innocent suspect who is caught in a web of circumstantial evidence may decide to falsely confess to avoid a more significant punishment. There is no doubt that decreasing consequences is a tremendously powerful inducement to confess. An example of this occurs on rare occasions when we are permitted to interrogate suspects on behalf of a defense attorney. Because we are operating under privileged communication, anything the suspect tells us cannot be used against him in a court of law. Once we mention this during the interrogation, almost all of these suspects confess within a short period of time.

What is not established is that promises of leniency cause false confessions. An attempt has been made to address this question through laboratory studies, [2] but there is no empirical or statistical data that supports the premise that in real life interrogations promises of leniency increase the prevalence of false confessions. Our belief is that a promise of leniency, in and of itself, would not be likely to cause an innocent person to confess. On the other hand, when a promise of leniency is coupled with a threat of more significant consequences, we believe there may be a significant risk of a false confession.

Even the courts seem to acknowledge that a promise of leniency, if made under proper circumstances, is permissible. For example, it is a common practice for a prosecutor to offer a plea bargain to a defendant. Under this arrangement, the defendant agrees to plead guilty in exchange for leniency. The leniency may involve reducing the number of criminal charges against the defendant, decreasing the charge e.g., rape to battery, or a lesser sentence, e.g., life in prison vs. execution. To guard against innocent suspects entering into this agreement, courts generally require that the defendant confess details of his crime during the hearing.

Seeing the ease at which prosecutors obtain confessions by offering defendants plea bargains has caused some investigators to try the same tactic during an interrogation, e.g., “Joe, you can avoid a first degree murder charge if you tell me that you didn’t plan this out.”[3] The investigator is then bewildered when the court suppresses the defendant’s confession. The rule of law is very simple: An investigator cannot offer the suspect a promise he cannot keep. Our criminal justice system affords prosecutors and investigators different powers in the effort to obtain evidence against a defendant. Prosecutors alone have the authority to make charging decisions and sentencing recommendations. Even if the investigator is best friends with the prosecutor and is almost certain that the prosecutor will go along with the suggested leniency, the promise is still impermissible because the investigator does not have the legal authority to offer it.

In an attempt to get around this legal technicality, investigators have made statements designed to allow the suspect to perceive possible leniency in exchange for a confession. Especially when an interrogator repeatedly mentions implied leniency, a court may suppress the confession.[4] Examples of statements that courts have ruled communicate an implied promise of leniency include:

“The best thing you can do is to confess.”

“It would be far better for you if you tell the truth.”

“I want to help you out on this thing.”

“I want to be an advocate for you on this matter.”

“It will go worse for you if you don’t confess.”

On the other hand, courts have not objected to interrogation techniques designed to reduce the perceived moral seriousness of a crime. Some of these permissible techniques include expressing understanding toward the suspect’s decision to commit the crime, e.g., “Joe I can understand why this thing happened”; referring to the crime with soft language, e.g., causing the death vs. murder; avoiding any mention of possible consequences the suspect faces if he confesses. Similarly, courts have not objected to the phrase, “I want to get something working on your side” or, “I want to work with you to get this matter straightened out.”

Furthermore, there are unique circumstances where investigators can legally make a promise to a suspect because the investigator has the authority to keep the promise. For example, in a correctional setting, an inmate may be promised certain privileges in exchange for truthful information. A corporate investigator may be able to promise an employee that he will not be prosecuted. Under this principle a police officer could make the following statement:

“Joe, I’m not going to arrest you tonight. You can go home and put your personal affairs in order and you can tell your wife whatever you want. Tomorrow morning I will stop by your house and I’ll take you into custody at that time.”

This exception, of course, is only true if the investigator keeps his promise, e.g., provides the inmate with privileges; does not prosecute the employee; allows the suspect to leave following the interrogation.

Applying the same principle, we believe the following statements are each permissible during an interrogation because the investigator is able to keep the promise:

“I’m not going to call up your wife and tell her that you are some sort of monster.”

“I’m not going to announce this to your co-workers or post it on the bulletin board.”

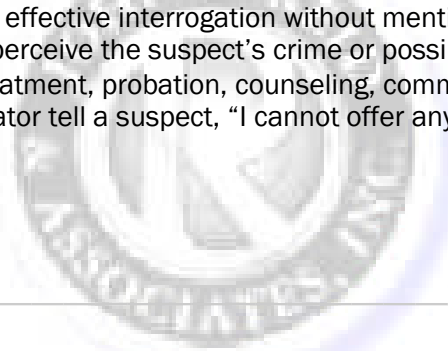
“I will include in my report that you were cooperative and that this is the first time you’ve done something like this.”

Promises of leniency are often introduced during an interrogation when the suspect asks the investigator, “What would happen to me if I told you I did this?” The following response in no way implies leniency and satisfies most suspects:

“Jim, I don’t have the authority to tell you and I’m not going to lie to you and say that I do. My job is to collect and analyze evidence. After that I just turn in my report and let other people act on my findings. I would like to be able to include your explanation in my report, which is why I am talking to you now.”

If the investigator slips up and finds himself making a statement that may be perceived as an implied promise of leniency, often the damage can be repaired by making a prophylactic statement, essentially setting the suspect straight by telling the suspect that the investigator does not have control over the consequences the suspect may face.

In conclusion, especially with the increased practice of electronically recording interrogations, investigators need to be very cautious not to make statements that may be construed as direct or implied promises of leniency. It is our general recommendation not to bring up the criminal justice system at all during an interrogation. An investigator can conduct a very effective interrogation without mentioning possible criminal charges, how the prosecutor, judge or jury may perceive the suspect’s crime or possible consequences for the suspect’s actions such as substance abuse treatment, probation, counseling, community service, etc. Courts will be favorably impressed to hear the investigator tell a suspect, “I cannot offer any promises about what will happen to you if you tell me the truth.”



The topic covered in this web tip is derived from information covered during our advanced course on interviewing and interrogation. If you have attended our basic course and are ready to enhance your ability to detect deception and elicit confessions, check our course calendar for the location of the advanced course nearest to you.

For further information on interrogation or interviewing techniques consider attending our advanced course on interviewing and interrogation. All CPIRC members get discounts on Reid seminars.

This article was prepared by John E. Reid and Associates, Inc. as their Monthly Web Tip and was reprinted on our web site with their permission. For additional Monthly Web Tips, go to www.reid.com and click on “Helpful Info”.

Resource Centre Roundup

Manitoba Sex Offender Database

The province of Manitoba has an online database of the most serious sex offenders. The police consider these offenders to be such a high risk to re-offend that Manitobans should be warned about them.

The Current Notifications section will display all the media releases issued by the police in the past year about high-risk sex offenders. The background material will vary from case to case, but it will normally include information about:

1. The past offences committed by the offender.
2. The area of the province where the offender is expected to reside.
3. The type of person who is at risk from the offender (e.g. adult females, children).

Click on the [Manitoba Sex Offender Notification](#) link found in the “Military/Law Enforcement/Crime/Firearms/Forensic” category in the Resource Centre.

Alberta High-risk offenders Database

The purpose of this site is to provide information on high-risk offenders in Alberta to help protect children and other vulnerable groups, and to enhance public safety.

This web site contains only the most serious offenders who are deemed to present a risk of significant harm to the safety of the public. Please note that not all dangerous or serious offenders are included on this web site.

What information about the offender is included?

1. Physical description and photograph of the offender.
2. Information about the offences the offender has committed.
3. The general area in which the offender lives.
4. Contact name at the appropriate police service.

Click on the [Alberta High-risk offenders Database](#) link found in the “Military/Law Enforcement/Crime/Firearms/Forensic” category in the Resource Centre.

GlobalIncidentMap.com

A Global Display of Terrorism And Other Suspicious Events

Prior to commencing any personal protection (bodyguard) contract the advance team is busily gathering information analyzing the threat risk to the client and the protection team.

The **Global Incident Map** is a great tool in preparing the threat risk analysis. This free public service website was created to give the public, law enforcement, military, and government individuals a new way to visualize, and become instantly aware of terrorism and security incidents across the world.

It has a great interactive map of the world allowing one to move your mouse over an incident icon and a short description of the event will appear. Click the icon to be taken to the full incident description and a more precise satellite/map image.

The Global Incident Map can be found at GlobalIncidentMap.com

HOW TO CONTACT US



Monday to Friday	09:00 -17:00 (Eastern Standard Time)
Saturday & Sunday	Via Email Only
Canadian Statutory Holidays	Closed

Telephone:	(514) 373-8191
Fax Inquiries:	(514) 303-8841
Mailing Address:	CPIRC 2348 Chemin Lucerne, Suite #506 Ville Mont-Royal, QC H3R 2J8 Canada

To contact CPIRC via email please [click here](#).

www.cpirc.com

