

s.13(1)(a)

s.15(1) - Int'l

s.16(1)(b)

s.16(1)(c) **BRIEFING NOTE**

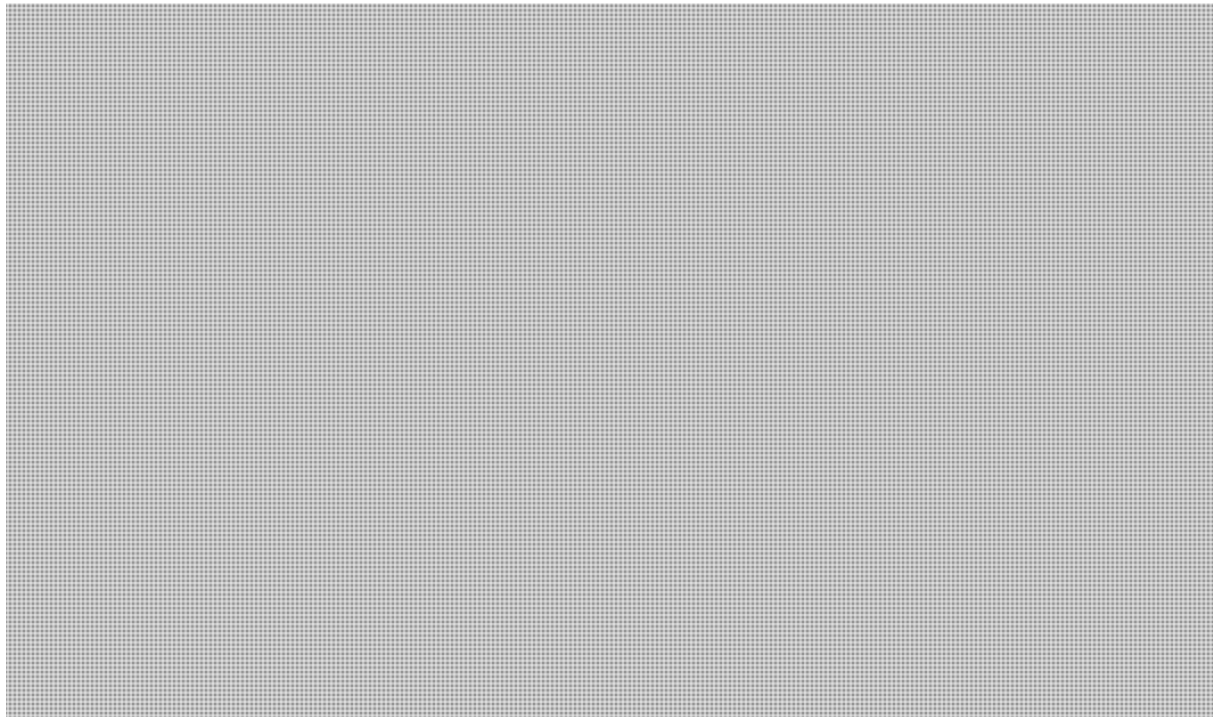
UNCLASSIFIED

APPLICATION SERVICE PROVIDERS

STRATEGIC OBJECTIVES

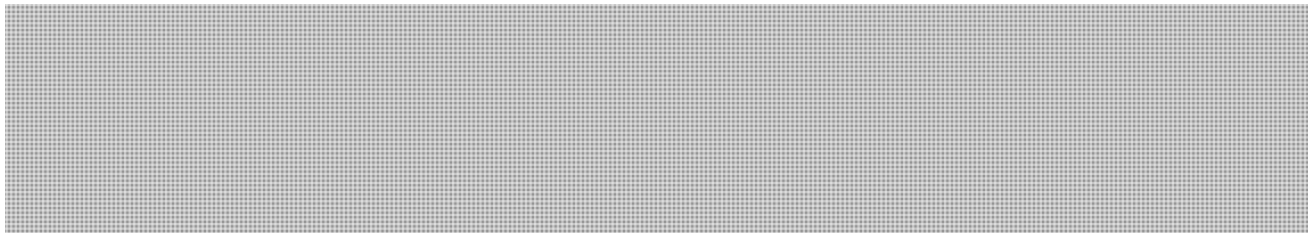
- Ensure that work to address challenges posed by Application Service Providers (ASPs) incorporate policy, legal and operational considerations.
- Ensure that any new initiative to address this issue will align with and build on ongoing multilateral efforts.

CONSIDERATIONS



BACKGROUND

ASPs are web-based services, such as Voice Over Internet Protocol (VoIP) and webmail (Hotmail, Gmail), that are accessed or downloaded by users over the Internet. The number and use of ASPs is growing as a result of the popularity of services such as Skype, FaceTime and other newer forms of communication.



- s.13(1)(a)
- s.14(a)
- s.15(1) - Int'l
- s.16(1)(b)
- s.16(1)(c)

UNCLASSIFIED

[REDACTED]

There is no formal mechanism for Canada to obtain intercepted communications or electronic data from other countries. In fact, the legislative framework of some countries (e.g. U.S.) prevents service providers from conducting interceptions for or sharing personal information on their customers with foreign countries.

[REDACTED]

The interception capability requirement included in Bill C-30, the *Protecting Children From Internet Predators Act*, would have applied to Canadian ASPs, and thus would have compelled those companies to assist agencies in obtaining intercepted communications or other electronic data.

[REDACTED]

CURRENT STATUS

[REDACTED]

UNCLASSIFIED

TALKING POINTS

- Obtaining information and interceptions of communications from Application Services Providers is a growing operational challenge for Canadian law enforcement and national security agencies, especially regarding encrypted communications.
- I understand that officials from our respective security and legal communities are already working together to tackle this issue. We welcome any further suggestions to help address this complex challenge in an effective and timely manner.

**Pages 4 to / à 15
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(c), 14, 16(2), 21(1)(b)

**of the Access to Information
de la Loi sur l'accès à l'information**

Background Information on Bill C-30 (*Protecting Children from Internet Predators Act*)

Q1. What is Bill C-30?

- Bill C-30, the *Protecting Children From Internet Predators Act*, (also known as the “lawful access legislation”), proposes to create one new statute, the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA), and introduce various amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act*.
- Collectively, this Bill aims to ensure that law enforcement and national security agencies have the technical and legal ability to investigate crimes effectively despite the continuous introduction of new technologies.
- The Bill strikes an appropriate balance between providing authorities with the means to investigate crime in the 21st century, and respecting the privacy of Canadians.
- The new statute, IPCECA, will require telecommunications service providers (TSPs) to:
 - Implement and maintain systems capable of lawfully intercepting private communications; and
 - Provide basic subscriber information in a timely and consistent fashion, upon request, to designated police, CSIS and Competition Bureau officials, and to any police officer in specific emergency situations.
- The amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act* include:
 - Some revisions to the application process for court orders and warrants related to a wiretap investigation to permit a streamlining of the process;
 - Modernizing some investigative powers and certain offences to better reflect the new technological reality;
 - Creating new, carefully tailored investigative powers to deal with digital evidence, and to prevent its destruction when it is needed for an investigative purpose;
 - Introducing safeguards, including notification and reporting obligations for the use of an interception of private communications conducted in exceptional circumstances (s.184.4 of the *Criminal Code*); and
 - Amendments to enable the ratification of the Council of Europe’s *Convention on Cybercrime* and its *Additional Protocol (Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems)*.

Q2. Why are telecommunications service providers (TSPs) being required to build and maintain intercept-capable networks?

- Currently, there is no requirement for TSPs to develop and maintain systems that provide intercept capability.
- This means that in many instances, despite the fact that the police and CSIS have been legally authorized to intercept communications with a judicial authorization, service providers may not have the capability to carry out the interception.
- The police and CSIS often have to spend a considerable amount of time and resources working with the TSPs to research and develop intercept capability solutions, often when time is of the essence.
- Criminals and terrorist groups are able to take advantage of this capability gap to prevent detection of their illegal activities.
- Therefore, IPCECA will place some requirements on telecommunications service providers (TSPs) to build and maintain intercept-capable networks.

Q3. What is basic subscriber information?

- Basic subscriber information refers to the basic identifying information about a customer that is held by a telecommunications service provider. It is limited to a subscriber's name, address, telephone number, email address, and the Internet Protocol (IP) address and local service provider identifier (LSPID) associated with the subscriber's service or equipment. It does **not** include any information about the websites that a subscriber visited, the contents of emails, or the phone calls either made or received.

Q4. Why do the police, CSIS and the Competition Bureau require telecommunications service providers to provide basic subscriber information?

- Law enforcement and CSIS require basic subscriber information in a timely fashion in a wide variety of situations, ranging from performing general policing duties to conducting investigations, including ones related to serious threats to the safety and security of Canadians.
- Obtaining basic subscriber information is particularly relevant in the online context, as criminals use the Internet to operate with anonymity.
- For example, in cases where a child is lured over the Internet by a sexual predator, often the only clue authorities have as to the identity of the perpetrator is an IP address associated to a chat room communication. In these situations, authorities need to quickly establish the identity of the suspect based on the IP address. Once they have obtained that information, they may obtain court authority, such as a warrant, to seize additional information with a greater privacy expectation as the investigation proceeds.

- Some other examples of situations where basic subscriber information is used by law enforcement include:
 - investigating Internet fraud and other online crimes;
 - notifying next-of-kin after a traffic accident;
 - addressing suicide threats over crisis lines;
 - returning stolen property to its rightful owner; and
 - investigating threats posted on or sent over the Internet.
- Currently, basic subscriber information can be requested without a warrant under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). However, compliance is voluntary, which results in varying practices across the country. Some providers release information immediately upon request; others provide it at their convenience, often following considerable delays; while others do not release the information voluntarily.
- The regime operating today lacks reliability and accountability. The voluntary aspect can impede investigations; there are no requirements on law enforcement or CSIS to record requests or to conduct oversight, and no limit on the number of officials who can request the basic subscriber information.
- Bill C-30 will address these inconsistencies, clarify responsibilities, and put into place a system of accountability. The new Act will clarify that TSPs must provide this information, upon request, to a very specific, limited list of designated police, CSIS and Competition Bureau officials, and to police officers in specific emergency situations, and subject these requests to regular internal audits.

Q5. How will basic subscriber information requests be protected from abuse?

- IPCECA respects laws protecting the privacy of Canadians and is consistent with the *Canadian Charter of Rights and Freedoms*.
- Compared to the current regime (in the *Personal Information and Electronic Documents Act* / PIPEDA), IPCECA would provide **more** checks and balances relating to requests for this type of information. IPCECA will include the following safeguards:
 - Limiting the number of identifiers which can be requested to name, address, phone number, email, IP address and name of the service provider;
 - Limiting the number of officials who can request basic subscriber information to a maximum of five people per organization, or 5% of the organization's workforce (whichever is greater);

- Putting procedures in place for mandatory record keeping by authorities of all requests for basic subscriber information;
 - Stipulating that basic subscriber information may only be requested in order to perform a duty or function of the agency in which a designated official works;
 - Mandating regular internal audits be conducted by the heads of respective agencies, and requiring that reports on the findings of these audits be provided to the responsible Minister and to the responsible external review bodies; and
 - Requiring that telecommunications service providers comply with the confidentiality and security measures included in the regulations.
- In addition, IPCECA will expressly reconfirm the role of review bodies to audit the basic subscriber information controls of an agency within their jurisdiction – such as the Privacy Commissioner for the RCMP and Competition Bureau, and the Security Intelligence Review Committee for CSIS – at any time.

Q6. Why does the *Criminal Code* need to be updated?

- While Canada was one of the first countries to enact criminal laws in the area of computer crime, no substantial amendments have been made since the 1990s.
- Technology has evolved considerably since then, and Canada's laws have not kept pace. These increasingly complex technologies are challenging conventional investigative methods, and criminals are taking advantage of this situation to assist them in carrying out illicit activities that threaten the safety and security of Canadians.
- To overcome these challenges, legislative tools such as the *Criminal Code* must evolve so that law enforcement can effectively investigate criminal activities while ensuring that Canadians' privacy and civil liberties are respected.

Q7. Why is the judicial authorization process for wiretapping being streamlined?

- Bill C-30 will improve the efficiency of wiretap investigations by permitting investigators who are applying for court authorizations to intercept private communications to simultaneously apply for other warrants and orders for other investigative techniques related to the same investigation, such as dialled number recorders.
- This will ensure that a single judge sees the entire investigative picture. In addition, it will allow for all the warrants and orders to be sealed simultaneously, and allow for harmonized timeframes, where applicable.

Q8. Why is it necessary to amend the provision in the *Criminal Code* that allows for the interception of private communications in exceptional circumstances (s. 184.4)?

- Collectively, these requirements would ensure that persons whose private communications are intercepted under s. 184.4 are notified and that information relating to the number of times police avail themselves of this authority is publicly available. These safeguards will ensure that individual rights and liberties are protected, and will allow for law enforcement's continued reliance on this important investigative tool.
- The amendments proposed in relation to section 184.4 were previously introduced in Parliament as part of former Bill C-31, which died on the Order Paper with the prorogation of Parliament in December 2009, and again in Bill C-50, which did not pass through Parliament prior to the general election in May 2011.
- In *R. v. Tse* the Supreme Court of Canada held that s. 184.4 of the *Criminal Code* is unconstitutional on the basis of the absence of a notification requirement for the authority in s. 184.4. The proposed amendments – which would add both notification and a reporting requirement to s. 184.4 – predate the Supreme Court's ruling in *R. v. Tse*. Even prior to that decision, the Government was concerned, as a matter of policy, with the overall lack of accountability in s. 184.4 of the *Criminal Code*. The Supreme Court's decision amplifies the need for Parliament to pass this amendment into law quickly, as the authority in s. 184.4 will be struck down as unconstitutional should the notification requirement fail to be passed into law by April 2013. This would be a serious public safety issue as it would render this important tool for emergency situations unavailable.

Q9. What is data preservation, and how is it different from data retention?

- Data preservation would allow for the immediate safeguarding of stored computer data already in the control of a person (for example, an employee of a TSP, Internet Service Provider or a content hosting service) related to a specific individual or communication for a limited period of time, in cases where law enforcement officers believe that such data will assist in a specific investigation.
- Data retention is not contemplated in Bill C-30. It refers to a more general obligation that exists in certain States, including those of the European Union, which requires the custodian to collect and store data for a prescribed period of time, typically for all subscribers, regardless of whether or not they are subject to an investigation.

Q10. What is transmission data? In what circumstances can police access it?

- "Transmission data" is routing information for communications. This includes information that identifies the characteristics of the communication, such as origin, destination, direction, date, time, size, duration, termination and type of

communication. It also includes the “provisioning” data which configures a device for network access; that is, the data exchange between the service provider and the device (such as a modem or a cell phone) that permits the device to access the service provider’s network. It explicitly excludes the content of the message.

- The new transmission data production orders and warrants would allow police to obtain, respectively, historical (i.e., already existing) transmission data or transmission data in real time. Such orders are authorized by a judge and are similar to what currently exists with respect to obtaining the telephone number of the telephone from which a telephone call originates or the telephone number at which the communication is received or is intended to be received. With respect to a specific email, for example, transmission data includes certain parts of the header data such as the email address and the mail servers that transmitted the email but it does not include the subject line or what a person types in the body of the email.
- In order to obtain transmission data, the police are required to secure a transmission data recorder warrant or a transmission data production order. These investigative powers would replace the “dialed number recorder” warrant that is presently in the *Criminal Code*. While useful, the dialed number recorder warrant is limited to routing information related to telephone communications. These amendments are required so that police can obtain similar routing information with respect to more contemporary means of communication (e.g., text messaging over the Internet, e-mail, Web sites accessed, etc.). The content is excluded.

Q11. What changes were specifically needed to ratify the Council of Europe’s *Convention of Cybercrime*?

- To ratify the *Convention on Cybercrime*, as well as the *Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Canada’s laws needed to be amended in a few significant ways.
- These include amendments to the *Criminal Code*, both from a substantive and a procedural standpoint and to the *Mutual Legal Assistance in Criminal Matters Act*, that would allow Canada to cooperate with its international partners.
- The primary changes relate to new procedural powers for the investigation of crimes that involve digital evidence (crimes against or using computers, or crimes leaving digital evidence). These include data preservation powers and production orders to track or collect data related to the transmission of modern telecommunications (powers to intercept private communications already exist in the *Criminal Code*).
- Amendments to two *Criminal Code* offences are necessary. The first relates to updates to the *Criminal Code*’s existing “hacking tools” offence, to make

possession of a computer virus an offence and to include additional offences. The second relates to the Additional Protocol and requires a change to the definition of “identifiable group” in the hate speech provisions.

Q12. The Standing Committee on Justice and Human Rights recently released a report that discussed some of the amendments contained in Bill C-30 (“The State of Organized Crime”). What did the Committee say?

- The Committee was supportive of Bill C-30. Several of its recommendations relate to legislative proposals already contained in Bill C-30.
- Some of the Committee’s recommendations do, however, go beyond what is proposed in Bill C-30. In particular, the Committee recommends imposing interception capability not only on TSPs (as is proposed in Bill C-30) but also on telecommunications device manufacturers. The Committee also recommended imposing decryption requirements on both TSPs (beyond what is proposed in Bill C-30) and telecommunications device manufacturers.
- The Committee also recommended that the Government engage in further policy development on the criminal use of prepaid phones and jamming devices. Both of these areas have already been identified as issues of concern requiring further work by the FPT Cybercrime Working Group.

**Pages 23 to / à 29
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(c), 14, 21(1)(b)

**of the Access to Information
de la Loi sur l'accès à l'information**



**International Travel Report
Rapport de voyage international**

Please submit this report to the International Affairs division (international@ps-sp.gc.ca) no later than 10 business days after your return. Veuillez soumettre le rapport à la Division des affaires internationales (international@ps-sp.gc.ca) au plus tard 10 jours ouvrables après votre retour.

Event Title <i>Titre de l'événement</i> ISS World Conference	Date of Event <i>Date de l'événement</i> 2013-06-04 – 2012-06-06	Place (City, Country) <i>Lieu (Ville, Pays)</i> Prague, Czech Republic
Traveller(s)/Voyageur(s)		
Name(s) <i>Nom(s)</i> Marie-Hélène Chayer	Division/Branch <i>Division/Secteur</i> NS Ops, NS	Telephone No. <i>N° de téléphone</i> 949-3181
International Strategic Framework Priorities Priorité selon le Cadre stratégique international		
Thematic Priority(ies)* <i>Priorité thématique**</i>	Bilateral Priority(ies)* <i>Priorité bilatérale**</i>	Multilateral Priority(ies)* <i>Priorité multilatérale**</i>
National Security Countering Crime	N/A	Tier 2 - International Law Enforcement Seminar
<p>*Indicate ALL of the thematic, bilateral, or multilateral priorities from the ISF that apply (see below). **Indiquez TOUTES les priorités thématiques, bilatérales ou multilatérales du CSI relatives au voyage (voir en bas de page).</p>		

Description – Description:

Please outline the meetings and/or events attended during your travel, and identify the key outcomes of each.***

*Veillez nommer les réunions ou événements auxquels vous avez participé pendant votre voyage, et préciser les principaux résultats de chacun d'eux.*****

The Intelligence Support Systems (ISS) World Conferences are the world's largest public gathering of law enforcement practitioners, intelligence analysts and telecommunications operators. These conferences focus on the methodologies and tools that public safety agencies can use to counter crime in today's telecommunications environment. Most presentations specifically pertain to technical interception solutions, and metadata collection and analysis. As such, the Prague conference offered an opportunity to gather valuable and up-to-date information on techniques and solutions that other countries and telecommunications companies are contemplating to address law enforcement and national security agencies' needs with respect to lawful interception, electronic investigations and intelligence gathering. It also allowed the Director of Investigative Technology and Telecommunications Policy (ITTP) to discuss current and emerging challenges related to lawful interception with international experts.

Relevance – Pertinence:

Why are these outcomes important to Public Safety? How do they promote the priorities identified in the RPP, IHRBP, or your Branch Business Plan?***

*Pourquoi ces résultats sont-ils importants pour Sécurité publique Canada? Comment favorisent-ils la mise en œuvre des priorités établies dans le RPP, le PIRHA ou le Plan d'activités du Secteur?*****

The Department identified advancing lawful interception legislative and regulatory initiatives as a means to achieve a robust approach to addressing national security threats. The ISS Prague Conference helped identify areas of interest for research, and potential policy and legislative proposals in support of lawful interception and other investigative techniques. Topics of particular relevance included:

Social Networks (SN) Proliferation: The use of SN has been exponentially increasing over the past decade. For instance, there are now over 1.1 billion profiles on Facebook. This shift is presenting both opportunities and challenges to investigators. While a significant amount of information can more easily be found on the web, the content of some profiles and the communications supported by these networks are often encrypted. As well, since they fall outside most interception legislation, SN usually do not respond efficiently to authorities' requests for information (e.g. Facebook's response time to such requests averages between 4 to 6 weeks.) Vendors and authorities are



therefore focusing increasingly on developing capabilities to collect and analyze metadata and communications data, which however raises significant privacy concerns from the public.

Legislative Gaps: While many countries have legislation requiring telecommunications service providers to maintain interception capable systems, most laws do not apply to application service providers (ASP) and do not include data retention obligations. As a result, it is often impossible for investigators to decrypt the communications using applications, and to obtain communications data. In addition to privacy concerns from the public, part of the challenge in developing legislation that would fill these gaps is the fact that applications are borderless and that ASP are often outside the requesting authorities' jurisdiction. The European Telecommunications Standards Institute (ETSI) has been developing a directive that would allow investigating bodies to request assistance (including decryption) from any ASP, provided that the requesting agency would have a valid warrant (i.e. valid in the agency's home country), that the traffic would go through the requesting authority's jurisdiction, and the target's traffic could be isolated. ETSI is facing significant challenges in moving the Directive forward, including pertaining to European countries' various legislative frameworks and criticism from privacy advocates. The issue of data retention raises similar concerns and challenges.

Technical Solutions to Encrypted Communications: In some circumstances, IT Intrusion (e.g. the use of Trojan by authorities to intercept a target's communications at the source) allows to overcome some encryption challenges, and law enforcement and intelligence agencies are increasingly investing in this investigative technique. IT Intrusion, however, is not without operational and legal challenges. First, it does not always enable authorities to intercept unencrypted communications. Second, such solutions are not easy to use: they are expensive, difficult to implement (authorities need to access or get close to a target's devices), often require infecting all the target's devices, and necessitate intensive monitoring. Third, they may leave "traces" and compromise investigations. Fourth, they present serious legal challenges in that information obtained through IT intrusion may not always be used for prosecution.

Data Volume: With increasing computing power and internet speed, users are downloading and uploading significantly large volumes of data. Investigative bodies are now challenges with collecting, storing, processing and analyzing enormous amounts of information. To overcome these challenges, many are using filters to reduce data volumes. While filters may facilitate intelligence analysis, from a legal perspective, however, they may impede prosecution as some legal systems consider filtered data to be "incomplete data" and as such inadmissible in court.

e-Warrant: ETSI is currently developing an e-Warrant system that could eventually be used by European public safety agencies to obtain interceptions from service providers operating on that continent. This initiative could eventually have an impact on Canadian agencies' access to interceptions, especially as pertains to cross-jurisdiction communications.

Privacy Considerations: All the investigative techniques and solutions presented at the conference raise privacy considerations. As privacy is a growing concern in many countries, including Canada, further research, analysis and engagement with like-minded countries and privacy stakeholders will be required to strike the right balance between privacy considerations and operational needs in the years to come.

Next Steps/Action Required - Prochaines étapes / mesures à prendre:

What actual or potential commitments were made on behalf of Canada, Other Government Departments, Public Safety, or the Portfolio Agencies? What must be done or decided in light of this travel?* *Quels engagements actuels ou éventuels ont-ils été pris au nom du gouvernement du Canada, de Sécurité publique Canada, d'autres ministères fédéraux ou d'organismes du Portefeuille? Quelles décisions doivent être prises et quelles mesures doivent être entreprises à la lumière de ce voyage?*******

The information gathered at the conference will help further ongoing policy development work to address lawful interception and other investigative challenges for Canadian law enforcement and national security agencies. ITTP will also monitor ETSI's work on e-Warrant and ASP, and determine how Canadian authorities could benefit from these initiatives. For additional information, please contact ITTP.



* See International Strategic Framework (ISF) 2011-2013 for country and multilateral priorities. Thematic priorities can include: Border Security; Corrections; Crime Prevention; Cyber Security; Emergency Management; Executive (Multiple Themes); Learning & Development; Migrant Smuggling/Trafficking; National Security; Organized Crime; Security System Reform.

** Consultez le Cadre stratégique international (CSI) 2011-2013 pour le pays et les priorités multilatérales. Les priorités thématiques peuvent inclure Cybersécurité; Exécutif (Thèmes multiples); Formation et développement; Gestion des urgences; Prévention du crime; Réforme des systèmes de sécurité; Sécurité à la frontière; Services correctionnels.

*** To assist readers, please **bold** important words or information (e.g. mentions of PS, Portfolio Agencies, OGDs, GoC, ISF themes, countries, or institutions; etc...)

**** *Pour aider les lecteurs, veuillez mettre les mots ou renseignements importants en caractères gras (p. ex. les mentions du Ministère, des organismes du Portefeuille, des autres ministères fédéraux, du gouvernement du Canada, des thèmes énoncés dans le CSI, des pays ou des institutions).*

SECRET

DATE:

File No.: NS 6060 / 390705
RDIMS No.: Dragon 3723

MEMORANDUM FOR THE DIRECTOR GENERAL

A PRIMER ON ENCRYPTION

(Information only)

ISSUE

This memo will provide general information about encryption of telecommunications and discuss the impact on law enforcement and national security of the increasing use of encryption to send messages and store information.

BACKGROUND

This primer was developed by Public Safety officials using open source materials and after consultation with Portfolio engineers.

What is encryption?

Encryption is the process of encoding information in such a way that only the person with the key can decode it. Before digital communications, encryption was principally used by the military. Computer encryption is based on the science of cryptography.

Is there a Government of Canada Policy with respect to the encryption of information and communications?

In 1998, the Government issued a policy framework titled "A Cryptography Policy Framework for Electronic Commerce". Among other things, this framework aimed at encouraging the use of cryptography in Canada to protect businesses and consumers, while deterring criminals from using cryptographic measures for illegal purposes. The Cryptography policy framework informed a number of initiatives, including Lawful Access and anti-SPAM legislation.

How does encryption work?

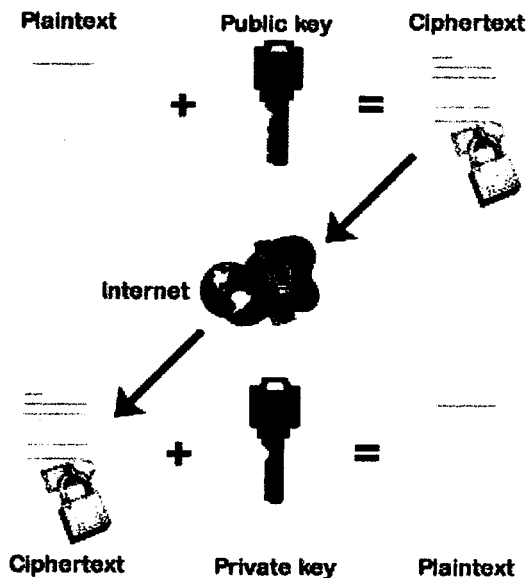
In general, the sender of a message uses a secret key to encode the message so that it appears to be a jumble of characters or numbers. The intended recipient needs to use a compatible secret key to decode the message and turn it into clear text. In digital communications, each packet is encrypted.

What role do "keys" play in encrypted communications? Who has them and where are they stored?

For encryptions using **symmetric keys**, the sender has to share a secret "key" with the recipient to decode the message. In the context of cryptography, a "key" is a long string of random numbers.¹ This "key" is generated by an encryption software and usually resides on a user's computer/device. However, the use of symmetric keys is relatively uncommon because of the challenges associated with exchanging a secret key securely over the Internet or a network, and the need to know the exact device that will be used to read the message.

In encryptions that employ **Asymmetric keys** (used in most common types of encryption— e.g. Public Key, known as PKI), there is a pair of "keys" – a public key and a private key. Both keys "reside" on the user's device. While the private key is known only to the user's device, the public key is made available to anyone who wishes to communicate with the user securely. These keys are generated by an encryption software, whose proprietary algorithm specifies the exact mathematical relationship between them.

The sender of a message encrypts the message using the recipient's public key. The message is then decrypted by the recipient using his/her secret private key, often stored on his/her computer.



How are messages encrypted?

There are two main methods of encrypting a message:

¹ An example of a public key is: 3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

SECRET

-3-

Encryption by the user. In this type of situation, the sender of a message encrypts the message at his/her own computer or device before sending it. A person may do this by using special encryption software (or application for smart phones), or by enabling an encryption feature for an e-mail application. The increasingly popular and readily available encryption applications for smart phones use this type of encryption. Examples include Cellcrypt (for iPhone) or PGP, Enclocked (for PCs and mobile devices).

Encryption with no user intervention. There can also be secure communications where the sender of a message does not need to specifically encrypt it. This situation typically involves a secure website or telecommunications service providers that create encrypted channels for each communication session via software that uses protocols recognized by most common Internet browsers (e.g. Microsoft's Internet Explorer). Corporate Virtual Private Networks (VPNs), on-line banking and most e-commerce web sites use this type of encryption. Computer users will commonly see a "padlock" icon or "https://" in the address line of their Internet browser. All common Internet browsers allow this type of encryption, which is automatically enabled if the computer at the other end of the communication also has this capability. Google now automatically enables HTTPS for all Gmail users and Facebook does this for their users as well.

CURRENT TRENDS IN ENCRYPTION

The use of encryption to protect communications and stored data is growing because of the following factors:

Privacy concerns. Well publicized cyber security incidents and personal data breaches from well known websites have helped raise awareness among the general public about the need to keep their information secure from hackers and eavesdroppers. For example, Facebook's implementation of encrypted channels in 2011 was in response to a cyber attack called Firesheep. Gmail, a popular web-based e-mail service, did the same in 2010. There is also a heightened awareness in the corporate sector that any company may be prey to cyber espionage.

Increased popularity of Cloud Computing. The growing demand for the ability to access one's information anytime from anywhere is increasing the popularity of cloud computing². Encryption of information that is meant to reside in the cloud can be used by a cloud service provider to address customers' privacy and security concerns³. For example, some American cloud service providers are attempting to persuade the U.S. government to focus on encryption to keep U.S. government data secure, rather than imposing requirements on data location and on the personnel handling the data.

Advances in technology and cheaper computing power. Encryption demands a considerable amount of computing resources. Traditionally, this limited the use of encryption to those users who had a powerful enough computer. Today's devices, even

² Web mail such as Gmail, Hotmail or using e-mail on a mobile device employs cloud computing.


³ The current default practice, however, is not to store encrypted information in a cloud unless the client demands it because this requires extra resources.

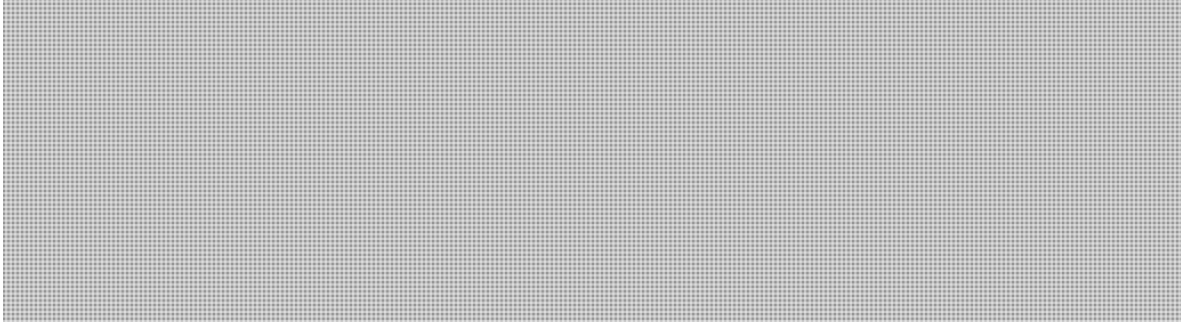
SECRET

-4-

those used by the general public, have enough processing power to handle encryption software. In addition, current programming languages such as Java and the availability of open source codes make encryption applications easier, faster and cheaper to develop and use.


s.15(1) - Sub **ENCRYPTION AND TELECOMMUNICATIONS SERVICE PROVIDERS**
s.16(2)(c)

Increasingly, Telecommunications Service Providers (TSPs) who provide Internet access for users are not the ones encrypting the users' communications. 



IMPLICATIONS FOR LAW ENFORCEMENT AND NATIONAL SECURITY

Encryption is a growing challenge for law enforcement and national security authorities because intercepted encrypted communications are unintelligible without the decryption key, especially since encryption programs are becoming increasingly sophisticated and difficult to crack.



Prepared by: Rana Dincoy
October 24, 2012

000036

**Pages 37 to / à 41
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(c), 14, 21(1)(b)

**of the Access to Information
de la Loi sur l'accès à l'information**

Hawrylak, Maciek

From: Dincoy, Rana
Sent: April-18-13 5:02 PM
To: Chayer, Marie-Helene
Cc: Hawrylak, Maciek; Plunkett, Shawn; Thompson, Julie; Emmett, Jamie
Subject: Info on Snapchat and Wickr

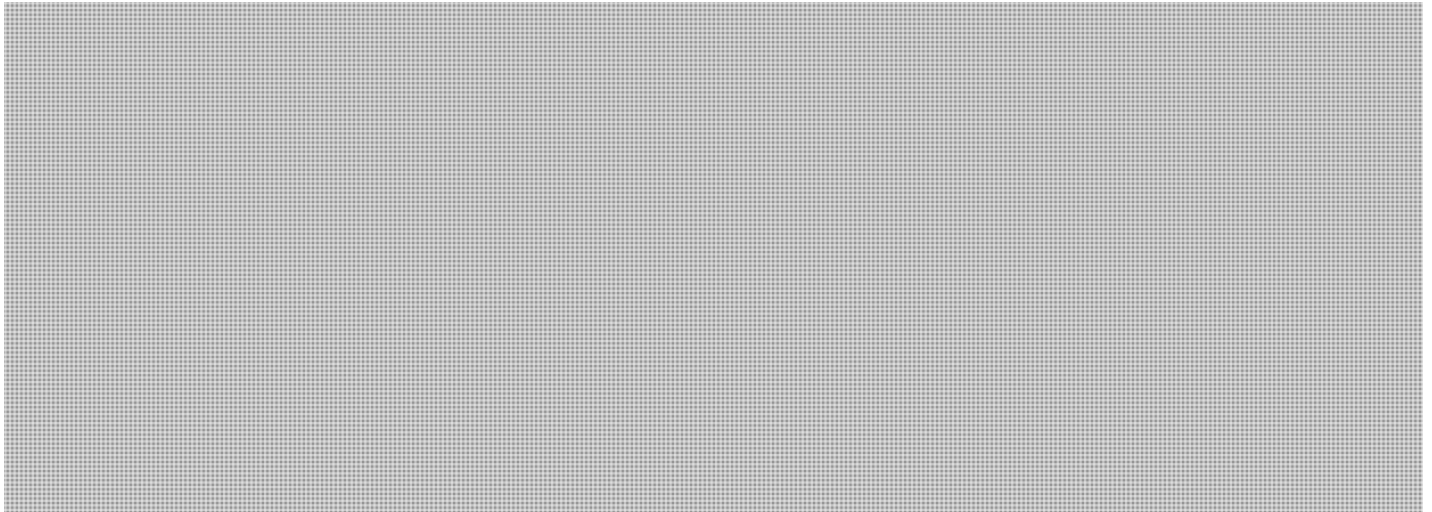
As requested.

SNAPCHAT – the “disappearing” photo app

- *Snapchat* is a mobile messaging application (app) that allows users to send each other photos and videos where they can insert captions (text). These messages self-destruct after a set period of time (up to 10 seconds) after they are received. All traces of the messages are removed from both mobile devices and the company’s servers.
- *Snapchat* is available for mobile devices only. It is available for both iPhone and Android mobile devices (e.g. phones and tablets). It is very popular among young adults.
- The messaging is not encrypted and was never meant to be a secure application. *Snapchat* was released by University of Stanford students in 2011 who have since secured Millions of Dollars in venture capital funding.
- *Snapchat* may be less transient than many realize. Certain users have found a way to let the *Snapchat* message recipient to take a screenshot and save it permanently on a device, or post it online. In response, *Snapchat* has added a feature to their app that lets the sender know whether the recipient has taken a screenshot of their message.
- As of April 2013, *Snapchat* users send 150 million photos per day. That’s triple the amount they sent in December 2012
- Snapchat users just suffered their first spam attack this week (April 18, 2013). They were sent a provocative photo and asked to join the sender on a Skype conversation. Those who did would likely have been invited to click on a malicious link that could have installed malicious software on their phone
- Pictures and screenshots really explain this best. Click on <http://www.cbc.ca/news/yourcommunity/2013/04/beyond-sexting-snapchat-users->

[now-send-150m-photos-per-day.html](#) (I didn't copy/paste any due to copyright concerns)

- There is an equivalent app for adults called *Wickr*, also created by U.S. software developers. However, *Wickr* encrypts its messages and advertises it as a secure way of messaging. Cryptography experts are skeptical about *Wickr's* encryption algorithm because the company has not shared the methodology used, nor its code, which is contrary to industry practice.
- Messages are encrypted on the sender's phone using a private key (sender sets a password), and only the receiver can read them once he or she taps on the unlock button that appears when a message arrives. *Wickr* claims it doesn't store any messages. *Wickr* uses standard cryptography schemes used by companies such as amazon.com. For security reasons, not even your password can be retrieved.



Rana Dincoy

Senior Policy Analyst / Analyste supérieur en politiques

Investigative Technologies and Telecommunications Policy / Politiques sur les technologies d'enquête et les télécommunications

National Security Operations Directorate / Direction des Operations de Sécurité Nationale

Public Safety Canada / Sécurité Publique Canada

Tel : 613-998-8035

Hawrylak, Maciek

From: [REDACTED]
Sent: August-12-13 3:19 PM
To: Gordon KIRK; Karen Audcent; 'Helene Van Dyke'; Geoffrey Crampton; Chayer, Marie-Helene; [REDACTED] Hawrylak, Maciek
Subject: FYI ... 2 E-Mail Services Close and Destroy Data Rather Than Reveal Files

<http://www.telegram.com/article/20130810/NEWS/130819996/1116/mobile&TEMPLATE=MOBILE>

By Somini Sengupta THE NEW YORK TIMES

The shutdown of two small email providers on Thursday illustrates why it is so hard for Internet companies to challenge secret government surveillance: To protect their customers' data from federal authorities, the two companies essentially committed suicide.

Lavabit, a Texas-based service that was reportedly used by Edward J. Snowden, the leaker who had worked as a National Security Agency contractor, announced the suspension of its service Thursday afternoon. In a blog post, the company's owner, Ladar Levison, suggested — though did not say explicitly — that he had received a secret search order and was choosing to shut down the service to avoid being “complicit in crimes against the American people.”

Within hours, a fast-growing Maryland-based startup called Silent Circle also closed its email service and destroyed its email servers. The company said it saw the writing on the wall — while also making it plain that it had not yet received any court orders soliciting user data.

Mike Janke, the chief executive, said the company's customers include heads of state, members of royalty and government agencies. The company will continue its encrypted phone and text messaging service.

In effect, both businesses destroyed their assets — in part or in full — to avoid turning over their customers' data. Such public displays are far more difficult for large companies to make and help explain why the most public efforts to challenge secret government orders have come from small companies and nonprofits.

“Providers are in a bind,” observed Orin Kerr, a law professor who specializes in surveillance law at George Washington University. “They need to respect the privacy rights of customers in order to keep customers, but they also have an obligation to comply with the law. A small company can say, ‘Rather than comply with the law, we will go under.’ But Verizon is not going to do that.”

He added: “The government usually has an easier time with large companies because they have more of a long-term need to have good relations with the government.”

Large Internet companies have moved more quietly and cautiously, addressing consumers' concerns about government requests only after information about secret orders was leaked by Snowden. This week, technology industry executives and lobbyists attended meetings at the White House.

In an effort to address public concern about the government's surveillance programs, President Barack Obama on Friday announced the creation of a task force to advise the government about how to balance security and privacy. He also said he supported a proposal to change the procedures of the secret court that approves electronic spying under the Foreign Intelligence Surveillance Act.

The level of secrecy appeared to be a particular frustration for Levison. On the Lavabit site Thursday afternoon, Levison said he was legally prohibited from explaining why he had been compelled to suspend operations.

"I wish that I could legally share with you the events that led to my decision. I cannot," he wrote.

"This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States," he added.

Silent Circle's chief executive, Janke, said executives at his company — the founders include Philip R. Zimmermann, who created the original email encryption protocol known as Pretty Good Privacy — had opted to follow Lavabit's example, even before being served with a government order.

He said the incident was a reminder of a fundamental flaw with email technology. An "aggressive" government, he said, can extract email data from any company, no matter how good the company's encryption tools. Keys to unlock its customers' encrypted communications had been stored on the company's servers. Silent Circle destroyed that data, the digital equivalent of a library setting fire to its membership records to keep the government from knowing who checked out what books.

Silent Circle's text and phone service uses somewhat different technology. The encryption keys are generated between two users as they are communicating and then destroyed. It is aptly called ephemeral encryption.

Bruce Schneier, a cryptographer, applauded Lavabit's decision, pointing out that its self-destruction was made possible because it had no shareholders to answer to.

"Could you imagine what would happen if Mark Zuckerberg or Larry Page decided to shut down Facebook or Google rather than answer National Security Letters? They couldn't. They would be fired," Schneier wrote on his blog. "When the small companies can no longer operate, it's another step in the consolidation of the surveillance society."

Before Lavabit, there was Calyx Internet Access, a small Internet service provider and Web hosting company, that challenged the constitutionality of a secret National Security Letter in 2004. Four Connecticut librarians likewise won their gag order challenge under a so-called National Security Letter in 2006. And a similar challenge was brought by a nonprofit digital library, called the Internet Archive. The government had sought information about one of its users, and it won its challenge to a gag order in 2008.

The most closely watched ruling on secret orders came this year. The San Francisco-based Electronic Frontier Foundation appealed to a U.S. District judge to lift a gag order issued by the FBI through a national security letter. The court said the gag order was unconstitutional.

Large companies have pushed back more quietly. Yahoo is the only company known to have challenged a gag order from the Foreign Intelligence Surveillance Court. And a coalition of companies, including Google and Microsoft, which sit on a trove of personal communications, have appealed to the Obama administration to be able to disclose just how many Foreign Intelligence Surveillance Act Court orders they receive.

According to Justice Department figures, in 2012, government authorities made 1,856 data requests under the Foreign Intelligence Surveillance Act, the vast majority for electronic surveillance, and another 15,229 requests through National Security Letters.

Nicholas Merrill, the owner of Calyx, received one such letter in early 2004 under the Patriot Act. He closed his business within months. "I was terrified they were going to drag me away," he said Friday.

It took him years to challenge the court order. He still cannot discuss its contents; he can only acknowledge its existence. His actions, he said, were possible only because his company was small and he was not beholden to shareholders.

"In a way, being a small company is quite liberating," he said.

Merrill said he immediately empathized with Levison's plight. "I would imagine he feels so strongly about this that he's willing to sacrifice his own business, and he's willing to risk angering all his client base for this basic principle," he said. "I can totally relate to where he's coming from."

Emmett, Jamie

From: David Vincenzetti <vince@hackingteam.it>
Sent: October-06-13 12:15 AM
To: list@hackingteam.it
Subject: A Few Thoughts on Cryptographic Engineering

A VERY interesting article from <http://blog.cryptographyengineering.com/2013/09/on-nsa.html> . Enjoy the reading!

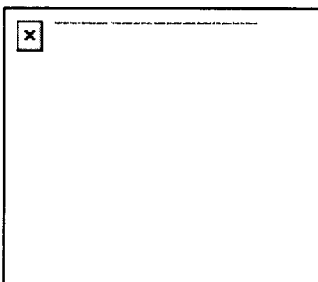
FYI,
David

A Few Thoughts on Cryptographic Engineering

Some random thoughts about crypto. Notes from a course I teach. Pictures of my dachshunds.

Thursday, September 5, 2013

On the NSA



Let me tell you the story of my tiny brush with the biggest crypto story of the year.

A few weeks ago I received a call from a reporter at ProPublica, asking me background questions about encryption. Right off the bat I knew this was going to be an odd conversation, since this gentleman seemed convinced that the NSA had vast capabilities to defeat encryption. And not in a '*hey, d'ya think the NSA has vast capabilities to defeat encryption?*' kind of way. No, he'd already established the defeating. We were just haggling over the details.

Oddness aside it was a fun (if brief) set of conversations, mostly involving hypotheticals. If the NSA could do this, how might they do it? What would the impact be? I admit that at this point one of my biggest concerns was to avoid coming off like a crank. After all, if I got quoted sounding *too much* like an NSA conspiracy nut, my colleagues would laugh at me. Then I might not get invited to the cool security parties.

All of this is a long way of saying that I was totally unprepared for today's bombshell revelations describing the NSA's efforts to defeat encryption. Not only does the worst possible hypothetical I discussed appear to be true, but it's true on a scale I couldn't even imagine. I'm no longer the crank. I wasn't even close to cranky enough.

And since I never got a chance to see the documents that sourced the NYT/ProPublica story -- *and I would give my right arm to see them* -- I'm determined to make up for this deficit with sheer speculation. Which is exactly what this blog post will be.

'Bullrun' and 'Cheesy Name'

If you haven't read the [ProPublica/NYT](#) or [Guardian](#) stories, you probably should. The TL;DR is that the NSA has been doing some very bad things. At a combined cost of \$250 million per year, they include:

1. Tampering with national standards ([NIST](#) is specifically mentioned) to promote weak, or otherwise vulnerable cryptography.
2. Influencing standards committees to weaken protocols.
3. Working with hardware and software vendors to weaken encryption and random number generators.
4. Attacking the encryption used by 'the next generation of 4G phones'.
5. Obtaining cleartext access to 'a major internet peer-to-peer voice and text communications system' (Skype?)
6. Identifying and cracking vulnerable keys.
7. Establishing a Human Intelligence division to infiltrate the global telecommunications industry.
8. And worst of all (to me): somehow decrypting SSL connections.

All of these programs go by different code names, but the NSA's decryption program goes by the name 'Bullrun' so that's what I'll use here.

How to break a cryptographic system

There's almost too much here for a short blog post, so I'm going to start with a few general thoughts. Readers of this blog should know that there are basically three ways to break a cryptographic system. In no particular order, they are:

1. **Attack the cryptography.** This is difficult and unlikely to work against the standard algorithms we use (though there are exceptions like RC4.) However there are many complex protocols in cryptography, and sometimes they are vulnerable.
2. **Go after the implementation.** Cryptography is almost always implemented in software -- and software is a disaster. Hardware isn't that much better. Unfortunately active software exploits only work if you have a target in mind. If your goal is mass surveillance, you need to build insecurity in from the start. That means working with vendors to add backdoors.
3. **Access the human side.** Why hack someone's computer if you can get them to give you the key?

Bruce Schneier, who has seen the documents, says that '*math is good*', but that '*code has been subverted*'. He also says that the NSA is '*cheating*'. Which, assuming we can trust these documents, is a huge sigh of relief. But it also means we're seeing a lot of (2) and (3) here.

So which code should we be concerned about? Which hardware?



SSL Servers by OS type. Source: [Netcraft](#).

This is probably the most relevant question. If we're talking about commercial encryption code, the lion's share of it uses one of a small number of libraries. The most common of these are probably the [Microsoft CryptoAPI](#) (and Microsoft [SChannel](#)) along with the [OpenSSL library](#).

Of the libraries above, Microsoft is probably due for the most scrutiny. While Microsoft employs good (and paranoid!) people to vet their algorithms, their ecosystem is obviously deeply closed-source. You can view Microsoft's code (if you sign enough licensing agreements) but you'll never build it yourself. Moreover they have the market share. If any commercial vendor is weakening encryption systems, Microsoft is probably the most likely suspect.

And this is a problem because Microsoft IIS powers around 20% of the web servers on the Internet -- and nearly forty percent of the SSL servers! Moreover, even third-party encryption programs running on Windows often depend on CAPI components, including the random number generator. That makes these programs somewhat dependent on Microsoft's honesty.

Probably the second most likely candidate is OpenSSL. I know it seems like heresy to imply that OpenSSL -- an open source and widely-developed library -- might be vulnerable. But at the same time it powers an enormous amount of secure traffic on the Internet, thanks not only to the dominance of Apache SSL, but also due to the fact that OpenSSL is *used everywhere*. You only have to glance at the FIPS CMVP validation lists to realize that many 'commercial' encryption products are just thin wrappers around OpenSSL.

Unfortunately while OpenSSL is open source, it periodically coughs up vulnerabilities. Part of this is due to the fact that it's a patchwork nightmare originally developed by a programmer who thought it would be a fun way to learn Bignum division.* Part of it is because *crypto is unbelievably complicated*. Either way, there are very few people who really understand the whole codebase.



On the hardware side (and while we're throwing out baseless accusations) it would be awfully nice to take another look at the Intel Secure Key integrated random number generators that most Intel processors will be getting shortly. Even if there's no problem, it's going to be an awfully hard job selling these internationally after today's news.

Which standards?

From my point of view this is probably the most interesting and worrying part of today's leak. Software is almost always broken, but standards -- in theory -- get read by everyone. It should be extremely difficult to weaken a standard without someone noticing. And yet the Guardian and NYT stories are extremely specific in their allegations about the NSA weakening standards.

The Guardian specifically calls out the National Institute of Standards and Technology (NIST) for a standard they published in 2006. Cryptographers have always had complicated feelings about NIST, and that's mostly because NIST has a complicated relationship with the NSA.

Here's the problem: the NSA ostensibly has both a *defensive* and an *offensive* mission. The defensive mission is pretty simple: it's to make sure US information systems don't get *pwned*. A substantial portion of that mission is accomplished through fruitful collaboration with NIST, which helps to promote data security standards such as the Federal Information Processing Standards (FIPS) and NIST Special Publications.

I said cryptographers have complicated feelings about NIST, and that's because we all know that the NSA has the power to use NIST for good as well as evil. Up until today there's been no real evidence of malice, despite some occasional glitches -- and compelling evidence that at least one NIST cryptographic standard could have contained a backdoor. But now maybe we'll have to re-evaluate that relationship. As utterly crazy as it may

seem.

Unfortunately, we're highly dependent on NIST standards, ranging from pseudo-random number generators to hash functions and ciphers, all the way to the specific elliptic curves we use in SSL/TLS. While the possibility of a backdoor in any of these components does seem remote, trust has been violated. It's going to be an absolute nightmare ruling it out.

Which people?

Probably the biggest concern in all this is the evidence of collaboration between the NSA and unspecified 'telecom providers'. We already know that the major US (and international) telecom carriers routinely assist the NSA in collecting data from fiber-optic cables. But all this data is no good if it's encrypted.

While software compromises and weak standards can help the NSA deal with some of this, by far the easiest way to access encrypted data is to simply ask for -- or steal -- the keys. This goes for something as simple as cellular encryption (protected by a single key database at each carrier) all the way to SSL/TLS which is (most commonly) protected with a few relatively short RSA keys.

The good *and bad* thing is that as the nation hosting the largest number of popular digital online services (like Google, Facebook and Yahoo) many of those critical keys are located right here on US soil. Simultaneously, the people communicating with those services -- *i.e.*, the 'targets' -- may be foreigners. Or they may be US citizens. Or you may not know *who they are* until you scoop up and decrypt all of their traffic and run it for keywords.

Which means there's a circumstantial case that the NSA and GCHQ are either directly accessing Certificate Authority keys** or else actively stealing keys from US providers, possibly (or probably) without executives' knowledge. This only requires a small number of people with physical or electronic access to servers, so it's quite feasible.*** The one reason I would have ruled it out a few days ago is because it seems so obviously immoral if not illegal, and moreover a huge threat to the checks and balances that the NSA allegedly has to satisfy in order to access specific users' data via programs such as PRISM.

To me, the existence of this program is probably the least unexpected piece of all the news today. Somehow it's also the most upsetting.

So what does it all mean?

I honestly wish I knew. Part of me worries that the whole security industry will talk about this for a few days, then we'll all go back to our normal lives without giving it a second thought. I hope we don't, though. Right now there are too many unanswered questions to just let things lie.

The most likely short-term effect is that there's going to be a lot less trust in the security industry. And a whole lot less trust for the US and its software exports. Maybe this is a good thing. We've been saying for years that you can't trust closed code and unsupported standards: now people will have to *verify*.

Even better, these revelations may also help to spur a whole burst of new research and re-designs of cryptographic software. We've also been saying that even *open* code like OpenSSL needs more expert eyes. Unfortunately there's been little interest in this, since the clever researchers in our field view these problems as 'solved' and thus somewhat uninteresting.

What we learned today is that they're solved all right. Just not the way we thought.

Notes:

* The original version of this post repeated a story I heard recently (from a credible source!) about Eric Young writing OpenSSL as a way to learn C. In fact he wrote it as a way to learn Bignum division, which is way cooler. Apologies Eric!

** I had omitted the Certificate Authority route from the original post due to an oversight -- thanks to Kenny Patterson for pointing this out -- but I still think this is a less viable attack for *passive* eavesdropping (that does not involve actively running a man in the middle attack). And it seems that much of the interesting eavesdropping here is passive.

*** The major exception here is Google, which deploys Perfect Forward Secrecy for many of its connections, so key theft would not work here. To deal with this the NSA would have to subvert the software or break the encryption in some other way.

Posted by Matthew Green at 11:27 PM

--
David Vincenzetti
CEO

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Emmett, Jamie

From: David Vincenzetti <d.vincenzetti@hackingteam.com>
Sent: November-17-13 12:55 AM
To: list@hackingteam.it
Subject: Defending Against Crypto Backdoors

[REDACTED] in the following Bruce Schneier's article from his latest CRYPTO-GRAM newsletter.



Enjoy the reading.

FYI,
David

** **

Defending Against Crypto Backdoors

We already know the NSA wants to eavesdrop on the Internet. It has secret agreements with telcos to get direct access to bulk Internet traffic. It has massive systems like TUMULT, TURMOIL, and TURBULENCE to sift through it all. And it can identify ciphertext -- encrypted information -- and figure out which programs could have created it.

But what the NSA wants is to be able to read that encrypted information in as close to real-time as possible. It wants backdoors, just like the cybercriminals and less benevolent governments do.

And we have to figure out how to make it harder for them, or anyone else, to insert those backdoors.

How the NSA Gets Its Backdoors

The FBI tried to get backdoor access embedded in an AT&T secure telephone system in the mid-1990s. The Clipper Chip included something called a LEAF: a Law Enforcement Access Field. It was the key used to encrypt the phone conversation, itself encrypted in a special key known to the FBI, and it was transmitted along with the phone conversation. An FBI eavesdropper could intercept the LEAF and decrypt it, then use the data to eavesdrop on the phone call.

But the Clipper Chip faced severe backlash, and became defunct a few years after being announced.

Having lost that public battle, the NSA decided to get its backdoors through subterfuge: by asking nicely, pressuring, threatening, bribing, or mandating through secret order. The general name for this program is BULLRUN.

Defending against these attacks is difficult. We know from subliminal channel and kleptography research that it's pretty much impossible to guarantee that a complex piece of software isn't leaking secret information. We know from Ken Thompson's famous talk on "trusting trust" (first delivered in the ACM Turing Award Lectures) that you can never be totally sure if there's a security flaw in your software.

Since BULLRUN became public last month, the security community has been examining security flaws discovered over the past several years, looking for signs of deliberate tampering. The Debian random number flaw was probably not deliberate, but the 2003 Linux security vulnerability probably was. The DUAL_EC_DRBG random number generator may or may not have been a backdoor. The SSL 2.0 flaw was probably an honest mistake. The GSM A5/1 encryption algorithm was almost certainly deliberately weakened. All the common RSA moduli out there in the wild: we don't know. Microsoft's _NSAKEY looks like a smoking gun, but honestly, we don't know.

How the NSA Designs Backdoors

While a separate program that sends our data to some IP address somewhere is certainly how any hacker -- from the lowliest script kiddie up to the NSA -- spies on our computers, it's too labor-intensive to work in the general case.

For government eavesdroppers like the NSA, subtlety is critical. In particular, three characteristics are important:

- * Low discoverability. The less the backdoor affects the normal operations of the program, the better. Ideally, it shouldn't affect functionality at all. The smaller the backdoor is, the better. Ideally, it should just look like normal functional code. As a blatant example, an email encryption backdoor that appends a plaintext copy to the encrypted copy is much less desirable than a backdoor that reuses most of the key bits in a public IV (initialization vector).

- * High deniability. If discovered, the backdoor should look like a mistake. It could be a single opcode change. Or maybe a "mistyped" constant. Or "accidentally" reusing a single-use key multiple times. This is the main reason I am skeptical about _NSAKEY as a deliberate backdoor, and why so many people don't believe the DUAL_EC_DRBG backdoor is real: they're both too obvious.

- * Minimal conspiracy. The more people who know about the backdoor, the more likely the secret is to get out. So any good backdoor should be known to very few people. That's why the recently described potential vulnerability in Intel's random number generator worries me so much; one person could make this change during mask generation, and no one else would know.

These characteristics imply several things:

- * A closed-source system is safer to subvert, because an open-source system comes with a greater risk of that subversion being discovered. On the other hand, a big open-source system with a lot of developers and sloppy version control is easier to subvert.

- * If a software system only has to interoperate with itself, then it is easier to subvert. For example, a closed VPN encryption system only has to interoperate with other instances of that same proprietary system. This is easier to subvert than an industry-wide VPN standard that has to interoperate with equipment from other vendors.

- * A commercial software system is easier to subvert, because the profit motive provides a strong incentive for the company to go along with the NSA's requests.

* Protocols developed by large open standards bodies are harder to influence, because a lot of eyes are paying attention. Systems designed by closed standards bodies are easier to influence, especially if the people involved in the standards don't really understand security.

* Systems that send seemingly random information in the clear are easier to subvert. One of the most effective ways of subverting a system is by leaking key information -- recall the LEAF -- and modifying random nonces or header information is the easiest way to do that.

Design Strategies for Defending against Backdoors

With these principles in mind, we can list design strategies. None of them is foolproof, but they are all useful. I'm sure there's more; this list isn't meant to be exhaustive, nor the final word on the topic. It's simply a starting place for discussion. But it won't work unless customers start demanding software with this sort of transparency.

* Vendors should make their encryption code public, including the protocol specifications. This will allow others to examine the code for vulnerabilities. It's true we won't know for sure if the code we're seeing is the code that's actually used in the application, but surreptitious substitution is hard to do, forces the company to outright lie, and increases the number of people required for the conspiracy to work.

* The community should create independent compatible versions of encryption systems, to verify they are operating properly. I envision companies paying for these independent versions, and universities accepting this sort of work as good practice for their students. And yes, I know this can be very hard in practice.

* There should be no master secrets. These are just too vulnerable.

* All random number generators should conform to published and accepted standards. Breaking the random number generator is the easiest difficult-to-detect method of subverting an encryption system. A corollary: we need better published and accepted RNG standards.

* Encryption protocols should be designed so as not to leak any random information. Nonces should be considered part of the key or public predictable counters if possible. Again, the goal is to make it harder to subtly leak key bits in this information.

This is a hard problem. We don't have any technical controls that protect users from the authors of their software.

And the current state of software makes the problem even harder: Modern apps chatter endlessly on the Internet, providing noise and cover for covert communications. Feature bloat provides a greater "attack surface" for anyone wanting to install a backdoor.

In general, what we need is assurance: methodologies for ensuring that a piece of software does what it's supposed to do and nothing more. Unfortunately, we're terrible at this. Even worse, there's not a lot of practical research in this area -- and it's hurting us badly right now.

Yes, we need legal prohibitions against the NSA trying to subvert authors and deliberately weaken cryptography. But this isn't just about the NSA, and legal controls won't protect against those who don't follow the law and ignore international agreements. We need to make their job harder by increasing their risk of discovery. Against a risk-averse adversary, it might be good enough.

This essay previously appeared on [Wired.com](http://www.wired.com).

<http://www.wired.com/opinion/2013/10/how-to-design-and-defend-against-the-perfect-backdoor/> or <http://tinyurl.com/o3uu76x>

The NSA's secret agreements:

https://www.schneier.com/blog/archives/2013/09/senator_feinste.html

Clipper Chip:

<http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html> or <http://tinyurl.com/m7fse2w>

How the NSA get around encryption:

<http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html> or <http://tinyurl.com/m9chca6>

<http://mashable.com/2013/09/11/fbi-microsoft-bitlocker-backdoor/>

http://news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys/ or <http://tinyurl.com/l2nam6s>

http://www.wired.com/threatlevel/2013/10/lavabit_unsealed

<http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html> or <http://tinyurl.com/lz2moej>

<http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html> or <http://tinyurl.com/lz2moej>

BULLRUN:

<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> or <http://tinyurl.com/m47p5dc>

<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> or <http://tinyurl.com/m47p5dc>

Subliminal channels:

https://en.wikipedia.org/wiki/Subliminal_channel

Kleptography:

<https://en.wikipedia.org/wiki/Kleptography>

Trusting trust:

<http://cm.bell-labs.com/who/ken/trust.html>

Debian bug:

<https://freedom-to-tinker.com/blog/kroll/software-transparency-debian-openssl-bug/> or <http://tinyurl.com/o28vmhg>

<https://freedom-to-tinker.com/blog/kroll/software-transparency-debian-openssl-bug/> or <http://tinyurl.com/o28vmhg>

Linux backdoor:

<https://freedom-to-tinker.com/blog/felten/the-linux-backdoor-attempt-of-2003> or <http://tinyurl.com/l3o3e7s>

DUAL_EC_DRBG:

<http://www.wired.com/threatlevel/2013/09/nsa-backdoor/all/>

SSL 2.0 flaw:

<http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html>

GSM A5/1 flaw:

<http://www.cs.technion.ac.il/users/wwwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf> or <http://tinyurl.com/3cskp3>

<http://www.cs.technion.ac.il/users/wwwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf> or <http://tinyurl.com/3cskp3>

Common RSA moduli:

<http://eprint.iacr.org/2012/064.pdf>


NSAKEY:
<http://en.wikipedia.org/wiki/NSAKEY>

NSA attacks Tor:
<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity> or <http://tinyurl.com/onbjqu>

Possible Intel RNG backdoor:
<https://www.schneier.com/blog/archives/2013/09/surreptitiously.html>

Nonces:
http://en.wikipedia.org/wiki/Cryptographic_nonce

Assurance:
<https://www.schneier.com/blog/archives/2007/08/assurance.html>

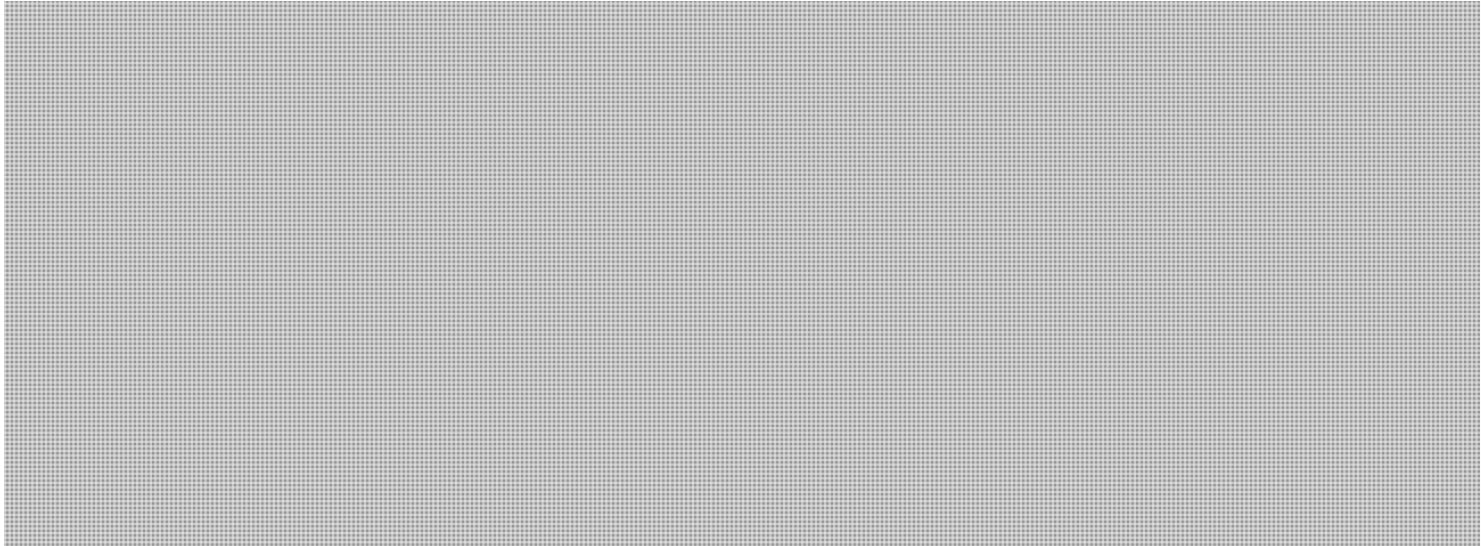
 If you can think of an example, please post a description and reference in the comments below. Please explain why you think the vulnerability could be intentional. Thank you.

FYI,
David
--
David Vincenzetti
CEO

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Emmett, Jamie

From: David Vincenzetti <d.vincenzetti@hackingteam.com>
Sent: November-23-13 10:40 PM
To: list@hackingteam.it
Subject: [REDACTED] N.S.A. Report Outlined Goals for More Power



This NYT article is [REDACTED] Enjoy the reading!

From yesterday's NYT, FYI,
David

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL



(U) SIGINT Strategy

2012-2016
23 February 2012



[Please check the the full document in plain text format at the end of this posting — if you are subscribed to the NYT, the article is available at <http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html? r=0>]

N.S.A. Report Outlined Goals for More Power

By JAMES RISEN and LAURA POITRAS

Published: November 22, 2013

WASHINGTON — Officials at the National Security Agency, intent on maintaining its dominance in intelligence collection, pledged last year to push to expand its surveillance powers, according to a top-secret strategy document.

In a February 2012 paper laying out the four-year strategy for the N.S.A.'s signals intelligence operations, which include the agency's eavesdropping and communications data collection around the world, agency officials set an objective to "aggressively pursue legal authorities and a policy framework mapped more fully to the information age."

Written as an agency mission statement with broad goals, the five-page document said that existing American laws were not adequate to meet the needs of the N.S.A. to conduct broad surveillance in what it cited as "the golden age of Sigint," or signals intelligence. "The interpretation and guidelines for applying our authorities,

and in some cases the authorities themselves, have not kept pace with the complexity of the technology and target environments, or the operational expectations levied on N.S.A.'s mission," the document concluded.

Using sweeping language, the paper also outlined some of the agency's other ambitions. They included defeating the cybersecurity practices of adversaries in order to acquire the data the agency needs from "anyone, anytime, anywhere." The agency also said it would try to decrypt or bypass codes that keep communications secret by influencing "the global commercial encryption market through commercial relationships," human spies and intelligence partners in other countries. It also talked of the need to "revolutionize" analysis of its vast collections of data to "radically increase operational impact."

The strategy document, provided by the former N.S.A. contractor Edward J. Snowden, was written at a time when the agency was at the peak of its powers and the scope of its surveillance operations was still secret. Since then, Mr. Snowden's revelations have changed the political landscape.

Prompted by a public outcry over the N.S.A.'s domestic operations, the agency's critics in Congress have been pushing to limit, rather than expand, its ability to routinely collect the phone and email records of millions of Americans, while foreign leaders have protested reports of virtually unlimited N.S.A. surveillance overseas, even in allied nations. Several inquiries are underway in Washington; Gen. Keith B. Alexander, the N.S.A.'s longest-serving director, has announced plans to retire; and the White House has offered proposals to disclose more information about the agency's domestic surveillance activities.

The N.S.A. document, titled "Sigint Strategy 2012-2016," does not make clear what legal or policy changes the agency might seek. The N.S.A.'s powers are determined variously by Congress, executive orders and the nation's secret intelligence court, and its operations are governed by layers of regulations. While asserting that the agency's "culture of compliance" would not be compromised, N.S.A. officials argued that they needed more flexibility, according to the paper.

Senior intelligence officials, responding to questions about the document, said that the N.S.A. believed that legal impediments limited its ability to conduct surveillance of terrorism suspects inside the United States. Despite an overhaul of national security law in 2008, the officials said, if a terrorism suspect who is under surveillance overseas enters the United States, the agency has to stop monitoring him until it obtains a warrant from the Foreign Intelligence Surveillance Court.

"N.S.A.'s Sigint strategy is designed to guide investments in future capabilities and close gaps in current capabilities," the agency said in a statement. "In an ever-changing technology and telecommunications environment, N.S.A. tries to get in front of issues to better fulfill the foreign-intelligence requirements of the U.S. government."

Critics, including some congressional leaders, say that the role of N.S.A. surveillance in thwarting terrorist attacks — often cited by the agency to justify expanded powers — has been exaggerated. In response to the controversy about its activities after Mr. Snowden's disclosures, agency officials claimed that the N.S.A.'s sweeping domestic surveillance programs had helped in 54 "terrorist-related activities." But under growing scrutiny, congressional staff members and other critics say that the use of such figures by defenders of the agency has drastically overstated the value of the domestic surveillance programs in counterterrorism.

Agency leaders believe that the N.S.A. has never enjoyed such a target-rich environment as it does now because of the global explosion of digital information — and they want to make certain that they can dominate "the Sigint battle space" in the future, the document said. To be "optimally effective," the paper said, "legal, policy and process authorities must be as adaptive and dynamic as the technological and operational advances we seek to exploit."

Intent on unlocking the secrets of adversaries, the paper underscores the agency's long-term goal of being able to collect virtually everything available in the digital world. To achieve that objective, the paper suggests that the N.S.A. plans to gain greater access, in a variety of ways, to the infrastructure of the world's telecommunications networks.

Reports based on other documents previously leaked by Mr. Snowden showed that the N.S.A. has infiltrated the cable links to Google and Yahoo data centers around the world, leading to protests from company executives and a growing backlash against the N.S.A. in Silicon Valley.

Yet the paper also shows how the agency believes it can influence and shape trends in high-tech industries in other ways to suit its needs. One of the agency's goals is to "continue to invest in the industrial base and drive the state of the art for high performance computing to maintain pre-eminent cryptanalytic capability for the nation." The paper added that the N.S.A. must seek to "identify new access, collection and exploitation methods by leveraging global business trends in data and communications services."

And it wants to find ways to combine all of its technical tools to enhance its surveillance powers. The N.S.A. will seek to integrate its "capabilities to reach previously inaccessible targets in support of exploitation, cyberdefense and cyberoperations," the paper stated.

The agency also intends to improve its access to encrypted communications used by individuals, businesses and foreign governments, the strategy document said. The N.S.A. has already had some success in defeating encryption, The New York Times has reported, but the document makes it clear that countering "ubiquitous, strong, commercial network encryption" is a top priority. The agency plans to fight back against the rise of encryption through relationships with companies that develop encryption tools and through espionage operations. In other countries, the document said, the N.S.A. must also "counter indigenous cryptographic programs by targeting their industrial bases with all available Sigint and Humint" — human intelligence, meaning spies.

The document also mentioned a goal of integrating the agency's eavesdropping and data collection systems into a national network of sensors that interactively "sense, respond and alert one another at machine speed." Senior intelligence officials said that the system of sensors is designed to protect the computer networks of the Defense Department, and that the N.S.A. does not use data collected from Americans for the system.

One of the agency's other four-year goals was to "share bulk data" more broadly to allow for better analysis. While the paper does not explain in detail how widely it would disseminate bulk data within the intelligence community, the proposal raises questions about what safeguards the N.S.A. plans to place on its domestic phone and email data collection programs to protect Americans' privacy.

N.S.A. officials have insisted that they have placed tight controls on those programs. In an interview, the senior intelligence officials said that the strategy paper was referring to the agency's desire to share foreign data more broadly, not phone logs of Americans collected under the Patriot Act.

Above all, the strategy paper suggests the N.S.A.'s vast view of its mission: nothing less than to "dramatically increase mastery of the global network."

Other N.S.A. documents offer hints of how the agency is trying to do just that. One program, code-named Treasure Map, provides what a secret N.S.A. PowerPoint presentation describes as "a near real-time, interactive map of the global Internet." According to the undated PowerPoint presentation, disclosed by Mr. Snowden, Treasure Map gives the N.S.A. "a 300,000 foot view of the Internet."

Relying on Internet routing data, commercial and Sigint information, Treasure Map is a sophisticated tool, one that the PowerPoint presentation describes as a “massive Internet mapping, analysis and exploration engine.” It collects Wi-Fi network and geolocation data, and between 30 million and 50 million unique Internet provider addresses — code that can reveal the location and owner of a computer, mobile device or router — are represented each day on Treasure Map, according to the document. It boasts that the program can map “any device, anywhere, all the time.”

The documents include addresses labeled as based in the “U.S.,” and because so much Internet traffic flows through the United States, it would be difficult to map much of the world without capturing such addresses.

But the intelligence officials said that Treasure Map maps only foreign and Defense Department networks, and is limited by the amount of data available to the agency. There are several billion I.P. addresses on the Internet, the officials said, and Treasure Map cannot map them all. The program is not used for surveillance, they said, but to understand computer networks.

The program takes advantage of the capabilities of other secret N.S.A. programs. To support Treasure Map, for example, the document states that another program, called Packaged Goods, tracks the “traceroutes” through which data flows around the Internet. Through Packaged Goods, the N.S.A. has gained access to “13 covered servers in unwitting data centers around the globe,” according to the PowerPoint. The document identifies a list of countries where the data centers are located, including Germany, Poland, Denmark, South Africa and Taiwan as well as Russia, China and Singapore.

Despite the document’s reference to “unwitting data centers,” government officials said that the agency does not hack into those centers. Instead, the officials said, the intelligence community secretly uses front companies to lease space on the servers.

Despite the N.S.A.’s broad surveillance powers, the strategy paper shows that N.S.A. officials still worry about the agency’s ability to fend off bureaucratic inertia while keeping pace with change.

“To sustain current mission relevance,” the document said, Signals Intelligence Directorate, the N.S.A.’s signals intelligence arm, “must undertake a profound and revolutionary shift from the mission approach which has served us so well in the decades preceding the onset of the information age.”

James Risen reported from Washington, and Laura Poitras from Berlin.

A version of this article appears in print on November 23, 2013, on page A1 of the New York edition with the headline: N.S.A. Report Outlined Goals For More Power.

[Page 1/5]

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) SIGINT Strategy

2012-2016

23 February 2012

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

[Page 2/5]

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) Vision

(U) Ensure Signals Intelligence provides THE decisive edge in advancing the full spectrum of U.S. national

security interests.

(U) Mission

(U) Defend the nation through SIGINT-derived advantage with a skilled work force trained, equipped and

empowered to access and unlock the secrets of our adversaries.

(U) Values

(U) We will constantly strive to improve our knowledge, our people, our technology, and our products.

Through innovation and personalization, we will advance the SIGINT system. Our customers and

stakeholders can rely on us to provide timely, high quality products and services, because we never stop

innovating and improving, and we never give up!

(U) The Environment

(U//FOUO) For decades, Signals Intelligence has sustained deep and persistent access to all manner of

adversaries to inform and guide the actions and decisions of Presidents,
military commanders, policy

makers and clandestine service officers. As the world has changed, and global
interdependence and the

advent of the information age have transformed the nature of our target space,
we have adapted in

innovative and creative ways that have led some to describe the current day as
"the golden age of

SIGINT."

(U//FOUO) That reputation was hard-won, but will only endure if we keep sight
of the dynamic and

increasingly market driven forces that continue to shape the SIGINT battle
space. We must proactively

position ourselves to dominate that environment across discovery, access,
exploitation, analysis,

collaboration and in the products and services we provide. The SIGINT system
and our interaction

therein must be as agile and dynamic as the information space we confront.

(U//FOUO) The mission space for SIGINT in the years ahead will continue to
grow at a rapid pace

amidst a dramatically new set of challenges:

(U//FOUO) The interpretation and guidelines for applying our authorities, and in some cases the

authorities themselves, have not kept pace with the complexity of the technology and target

environments, or the operational expectations levied on NSA's mission.

- (U) Digital information created since 2006 grew tenfold, reaching 1.8 exabytes in 2011, a trend

projected to continue; ubiquitous computing is fundamentally changing how people interact as

individuals become untethered from information sources and their communications tools; and the

traces individuals leave when they interact with the global network will define the capacity to locate,

characterize and understand entities¹.

1

(U) Center for the Study of Intelligence (2010) Where Tomorrow Will Take Us: The New Environment for Intelligence. August 2010

2

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

[Page 3/5]

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) Vision

(U) Ensure Signals Intelligence provides THE decisive edge in advancing the full spectrum of U.S. national

security interests.

(U) Mission

(U) Defend the nation through SIGINT-derived advantage with a skilled work force trained, equipped and

empowered to access and unlock the secrets of our adversaries.

(U) Values

(U) We will constantly strive to improve our knowledge, our people, our technology, and our products.

Through innovation and personalization, we will advance the SIGINT system. Our customers and

stakeholders can rely on us to provide timely, high quality products and services, because we never stop

innovating and improving, and we never give up!

(U) The Environment

(U//FOUO) For decades, Signals Intelligence has sustained deep and persistent access to all manner of

adversaries to inform and guide the actions and decisions of Presidents, military commanders, policy

makers and clandestine service officers. As the world has changed, and global interdependence and the

advent of the information age have transformed the nature of our target space, we have adapted in

innovative and creative ways that have led some to describe the current day as "the golden age of

SIGINT."

(U//FOUO) That reputation was hard-won, but will only endure if we keep sight of the dynamic and

increasingly market driven forces that continue to shape the SIGINT battle space. We must proactively

position ourselves to dominate that environment across discovery, access, exploitation, analysis,

collaboration and in the products and services we provide. The SIGINT system and our interaction

therein must be as agile and dynamic as the information space we confront.

(U//FOUO) The mission space for SIGINT in the years ahead will continue to grow at a rapid pace

amidst a dramatically new set of challenges:

(U//FOUO) The interpretation and guidelines for applying our authorities, and in some cases the

authorities themselves, have not kept pace with the complexity of the technology and target

environments, or the operational expectations levied on NSA's mission.

- (U) Digital information created since 2006 grew tenfold, reaching 1.8 exabytes in 2011, a trend

projected to continue; ubiquitous computing is fundamentally changing how people interact as

individuals become untethered from information sources and their communications tools; and the

traces individuals leave when they interact with the global network will define the capacity to locate,

characterize and understand entities¹.

1

(U) Center for the Study of Intelligence (2010) Where Tomorrow Will Take Us: The New Environment for Intelligence. August 2010

2

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

[Page 4/5]

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

SIGINT Goals for 2012-2016

1. (U//FOUO) Revolutionize analysis - fundamentally shift our analytic approach from a production to

a discovery bias, enriched by innovative customer/partner engagement, radically increasing

operational impact across all mission domains.

1.1. (U//FOUO) Through advanced tradecraft and automation, dramatically increase mastery of the

global network

1.2. (U//FOUO) Conduct original analysis in a collaborative information space that mirrors how people

interact in the information age

1.3. (U//FOUO) Disseminate data at its first point of relevance, share bulk data, and enable customers

to address niche requirements

1.4. (U//FOUO) Drive an agile technology base mapped to the cognitive processes that underpin large

scale analysis, discovery, compliance and collaboration

2. (U//FOUO) Fully leverage internal and external NSA partnerships to collaboratively discover targets,

find their vulnerabilities, and overcome their network/communication defenses.

2.1. (U//FOUO) Bolster our arsenal of capabilities against the most critical cryptanalytic challenges

2.1.1. (S//SI//REL) Employ multidisciplinary approaches to cryptanalytic problems, leveraging and

integrating mid-point and end-point capabilities to enable cryptanalysis

2.1.2. (S//REL) Counter the challenge of ubiquitous, strong, commercial network encryption

2.1.3. (TS//SI//REL) Counter indigenous cryptographic programs by targeting their industrial bases

with all available SIGINT and HUMINT capabilities

2.1.4. (TS//SI//REL) Influence the global commercial encryption market through commercial

relationships, HUMINT, and second and third party partners

2.1.5. (S//SI//REL) Continue to invest in the industrial base and drive the state of the art for High

Performance Computing to maintain pre-eminent cryptanalytic capability for the nation

2.2. (TS//SI//REL) Defeat adversary cybersecurity practices in order to acquire the SIGINT data we

need from anyone, anytime, anywhere

2.3. (S//SI) Enable discovery capabilities and advanced tradecraft in the collection architecture to

enable the discovery of mission-critical persona, networks, accesses, signals and technologies

2.4. (S//SI) Integrate capabilities into the mission architecture, deepen workforce skill base in

advanced network and signals analysis, and optimize processes and policies for the benefit of discovery

3. (S//SI//REL) Dynamically integrate endpoint, midpoint, industrial-enabled, and cryptanalytic

capabilities to reach previously inaccessible targets in support of exploitation, cyber defense, and cyber

operations

3.1. (C//REL) Drive the SIGINT mission architecture to underpin synchronized,
integrated,

multi-capability operations, extending it to mission partners

3.2. (TS//SI//REL) Integrate the SIGINT system into a national network of
sensors which interactively

sense, respond, and alert one another at machine speed

3.3. (U//FOUO) Continuously rebalance our portfolio of accesses and access
capabilities based on

current and projected contributions to key SIGINT missions

3.4. (S//SI//REL) Identify new access, collection, and exploitation methods by
leveraging global

business trends in data and communications services

4

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

[Page 5/5]

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) In order to achieve these three mission goals, we must collectively liberate the innovation and

creativity of our workforce through technology, policies, and business processes - hence, the following

two goals have been set:

4. (U) Collectively foster an environment that encourages and rewards diversity, empowerment,

innovation, risk-taking and agility

4.1. (U) Empower employees to make decisions and drive change; invest in and reward innovation,

risk-taking, and teaming

4.2. (U//FOUO) Build compliance into systems and tools to ensure the workforce operates within the

law and without worry

4.3. (U) Work together to detail, implement, and evolve the strategy

4.4. (U) Provide everyone with the training and experiences necessary to lead the world's most capable

SIGINT service and be competitive for Intelligence Community leadership positions

5. (U) Enable better, more efficient management of the mission and business by establishing new,

modifying current, and eliminating inefficient, business processes; by strengthening customer

relationships; and by building necessary internal and external partnerships.

5.1. (U//FOUO) Pursue, develop, and implement policy consistent with the pace and scope of

operations

5.2. (U//FOUO) Build into systems and tools, features that enable and automate end-to-end

value-based assessment of SIGINT products and services

5.3. (U//FOUO) Create and sustain a mission management environment that is autonomic and agile

5.4. (U//FOUO) Synchronize mission, budget and acquisition, and technology and research activities to

deliver the capabilities required to keep SIGINT relevant

5.5. (U) Align and standardize administrative business processes throughout
the SIGINT enterprise to

reduce the bureaucratic burden on the enterprise

5.6. (U//FOUO) Champion the development of a unified NSA/CSS U.S. customer
engagement strategy

that streamlines processes, increases resource efficiencies, eliminates
redundancies, and strengthens

NSA relationships

5

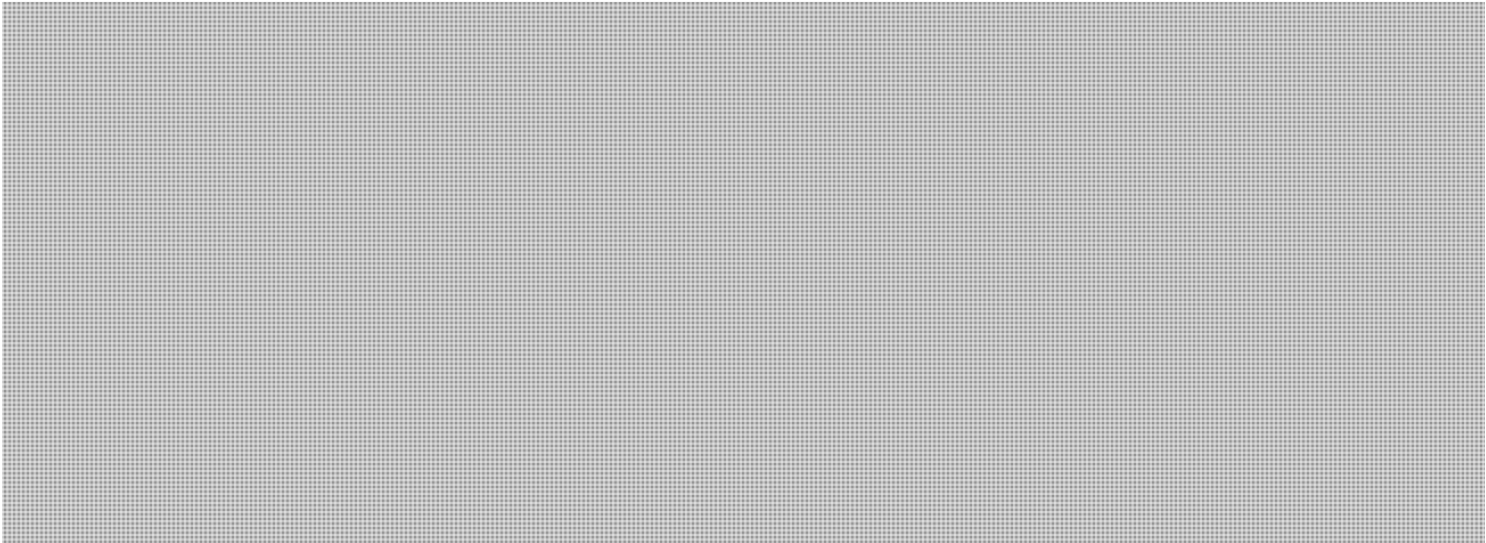
TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

--
David Vincenzetti
CEO

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Emmett, Jamie

From: David Vincenzetti <d.vincenzetti@hackingteam.com>
Sent: November-24-13 10:20 PM
To: list@hackingteam.it
Subject: MANDATORY offensive technologies (was: Twitter Also Beefs Up Encryption After NSA Leaks)



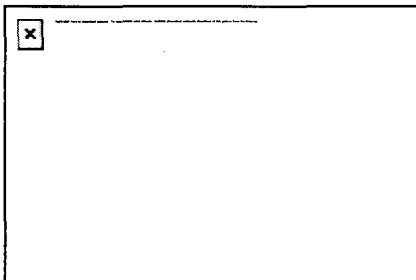
From Friday's [NYT.com](#), FYI,
David

Nov 22, 2013 | 7:50 pm

Privacy

Twitter Also Beefs Up Encryption After NSA Leaks

By [Danny Yadron](#)



National Security Agency headquarters at Fort Meade, Md.

Danny Yadron

Twitter on Friday became the latest tech giant to beef up encryption in response to disclosures about government eavesdroppers scooping up Web traffic.

A technology being adopted by the micro-blogging service makes it much harder for outsiders that intercept private Twitter content—whether they are hackers or employees of a three-letter agency—to make sense of what they've gathered.

The technology is called Perfect Forward Secrecy, and before Edward Snowden, it was mostly known in the tight-knit world of security nerds. But following a string of disclosures by the former National Security Agency contractor, security measures once thought to be only for the paranoid have become commonplace.

A obvious response is encryption, a venerable tool that uses mathematical processes to turn text into gibberish. But standard forms of encryption take extra computing power, cost money and slows traffic down. That “friction,” as people put it Silicon Valley, has deterred its use.

But Perfect Forward Secrecy has shown a minimal effect on a customer's experience. Google adopted the scheme two years ago and Facebook is now using it for most of its traffic.

Here's how it works:

Some conventional forms of encryption use a key—a special string of numbers—to lock and unlock messages sent by a particular sender. That means that someone who cracks or steals that key could use it to read a large volume of messages—including those going forward and those from the past.

The NSA has collected this type of encrypted data in bulk off of fiber optic cable lines, only to be able decrypt all of it later if they obtain the key, according to documents leaked by Snowden.

With Perfect Forward Secrecy, company systems randomly create new parts of the key for each session. So if someone obtained Twitter's private encryption key and wanted to go back read old direct messages, they would need to crack the encryption key for each of those sessions.

(Twitter, of course, could still be served with a court order demanding it turn over decrypted messages for specific users.)

Perfect Forward Secrecy prevents government from doing “dragnet” surveillance of Internet users and moves it “to being a targeted thing,” said Parker Higgins, a spokesman for the Electronic Frontier Foundation. “This is great news,” he said.

The New York Times earlier reported Twitter's move. Twitter engineers told the Times that the project did not gain much support internally until after the Snowden leaks.

--
David Vincenzetti
CEO


Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Emmett, Jamie

From: David Vincenzetti <d.vincenzetti@hackingteam.com>
Sent: December-24-13 11:21 PM
To: list@hackingteam.it
Subject: How does the NSA break SSL?

"A few weeks ago I wrote a long post about the NSA's 'BULLRUN' project to subvert modern encryption standards. I had intended to come back to this at some point, since I didn't have time to discuss the issues in detail. But then things got in the way. A *lot* of things, actually. Some of which I hope to write about in the near future."

"You see, the NSA BULLRUN briefing sheet mentions that NSA has been breaking quite a few encryption technologies, some of which are more interesting than others. One of those technologies is particularly surprising to me, since I just can't figure how NSA might be doing it. In this extremely long post I'm going to try to dig a bit deeper into the most important question facing the Internet today.

Please find  article on how the NSA might crack SSL-protected communications.

By Matthew Green,  also available at <http://blog.cryptographyengineering.com/2013/12/how-does-nsa-break-ssl.html> .

Enjoy the reading!

FYI,
David

Monday, December 2, 2013

How does the NSA break SSL?



A few weeks ago I wrote a long post about the NSA's 'BULLRUN' project to subvert modern encryption standards. I had intended to come back to this at some point, since I didn't have time to discuss the issues in detail. But then things got in the way. A *lot* of things, actually. Some of which I hope to write about in the near future.

But before I get there, and at the risk of boring you all to tears, I wanted to come back to this subject at least one more time, if only to pontificate a bit about a question that's been bugging me.

You see, the NSA BULLRUN briefing sheet mentions that NSA has been breaking quite a few encryption technologies, some of which are more interesting than others. One of those technologies is particularly surprising to me, since I just can't figure how NSA might be doing it. In this extremely long post I'm going to try to dig a bit deeper into the most important question facing the Internet today.

Specifically: *how the hell is NSA breaking SSL?*

restricted to those specifically indoctrinated for BULLRUN. **The various types of security covered by BULLRUN include, but are not limited to, TLS/SSL, https (e.g. webmail), SSH, encrypted chat, VPNs and encrypted VOIP.** The specific instances of these technologies that can be exploited will be published in a separate Annexe (available to BULLRUN indoctrinated staff).

Section of the BULLRUN briefing sheet. Source: New York Times.
To keep things on target I'm going to make a few basic ground rules.

First, I'm well aware that NSA can install malware on your computer and pwn any cryptography you choose. That doesn't interest me at all, for the simple reason that *it doesn't scale well*. NSA can do this to you, but they can't do it for an entire population. And that's really what concerns me about the recent leaks: the possibility that NSA is breaking encryption for the purposes of mass surveillance.

For the same reason, we're not going to worry about man-in-the-middle (MITM) attacks. While we know that NSA does run these, they're also a very targeted attack. Not only are MITMs detectable if you do them at large scale, they don't comport with what we know about how NSA does large-scale interception -- mostly via beam splitters and taps. In other words: we're really concerned about passive surveillance.

The rules above aren't absolute, of course. We will consider limited targeted attacks on servers, provided they later permit passive decryption of large amounts of traffic; e.g., decryption of traffic to major websites. We will also consider arbitrary modifications to software and hardware -- something we know NSA is already doing.

One last point: to keep things from going off the rails, I've helpfully divided this post into two sections. The first will cover attacks that use only known techniques. Everything in this section can be implemented by a TAO employee with enough gumption and access to software. The second section, which I've titled the '*Tinfoil Hat Spectrum*' covers the fun and speculative stuff -- ranging from new side channel attacks all the way to that huge quantum computer the NSA keeps next to BWI.

We'll start with the 'practical'.

Attacks that use Known Techniques

Theft of RSA keys. The most obvious way to 'crack' SSL doesn't really involve cracking anything. Why waste time and money on cryptanalysis when you can just steal the keys? This issue is of particular concern in servers configured for the TLS RSA handshake, where a single 128-byte server key is all you need to decrypt *every past and future connection* made from the device.

In fact, this technique is so obvious that it's hard to imagine NSA spending a lot of resources on sophisticated cryptanalytic attacks. We know that GCHQ and NSA are perfectly comfortable suborning even US providers overseas. And inside our borders, they've demonstrated a willingness to obtain TLS/SSL keys using subpoena powers and gag orders. If you're using an RSA connection to a major website, it may be sensible to assume the key is already known.

Of course, even where NSA doesn't resort to direct measures, there's always the possibility of obtaining keys via a remote software exploit. The beauty is that these attacks don't even require remote code execution. Given the right vulnerability, it may simply require a handful of malformed SSL requests to map the full contents of the OpenSSL/SChannel heap.



Suborning hardware encryption chips. A significant fraction of SSL traffic on the Internet is produced by hardware devices such as SSL terminators and VPN-enabled routers. Fortunately we don't have to speculate about the security of these devices -- we already know NSA/GCHQ have been collaborating with hardware manufacturers to 'enable' decryption on several major VPN encryption chips.

The NSA documents aren't clear on how this capability works, or if it even involves SSL. If it does, the obvious guess is that each chip encrypts and exfiltrates bits of the session key via 'random' fields such as IVs and handshake nonces. Indeed, this is relatively easy to implement on an opaque hardware device. The interesting question is how one ensures these backdoors can only be exploited by NSA -- and not by rival intelligence agencies. (Some thoughts on that [here](#).)

Side channel attacks. Traditionally when we analyze cryptographic algorithms we concern ourselves with the expected inputs and outputs of the system. But real systems leak all kinds of extra information. These '*side channels*' -- which include operation time, resource consumption, cache timing, and RF emissions -- can often be used to extract secret key material.

The good news is that most of these channels are only exploitable when the attacker is in physical proximity to a TLS server. The bad news is that there are conditions in which the attacker *can* get close. The most obvious example involves virtualized TLS servers in the cloud setting, where a clever attacker may share physical resources with the target device.

A second class of attack uses remote timing information to slowly recover an RSA key. These attacks can be disabled via countermeasures such as RSA blinding, though amusingly, some 'secure' hardware co-processors may actually turn these countermeasures off by default! At very least, this makes the hardware vulnerable to attacks by a local user, and could even facilitate remote recovery of RSA keys.

Weak random number generators. Even if you're using strong Perfect Forward Secrecy ciphersuites, the security of TLS depends fundamentally on the availability of unpredictable random numbers. Not coincidentally, tampering with random number generator standards appears to have been a particular focus of NSA's efforts.

Random numbers are critical to a number of elements in TLS, but they're particularly important in three places:

1. *On the client side, during the RSA handshake.* The RNG is used to generate the RSA pre-master secret and encryption padding. If the attacker can predict the output of this generator, she can subsequently decrypt the entire session. Ironically, a failure of the server RNG is much less devastating to the RSA handshake.*
2. *On the client or server side, during the Diffie-Hellman handshake(s).* Since Diffie-Hellman requires a contribution from each side of the connection, a predictable RNG on either side renders the session completely transparent.
3. *During long-term key generation, particularly of RSA keys.* If this happens, you're screwed.

And you just don't need to be that sophisticated to weaken a random number generator. These generators are already surprisingly fragile, and it's awfully difficult to detect when one is broken. Debian's maintainers made this point beautifully back in 2008 when an errant code cleanup reduced the effective entropy of OpenSSL to

just 16 bits. In fact, RNGs are so vulnerable that the challenge here is not *weakening* the RNG -- any idiot with a keyboard can do that -- it's doing so without making the implementation trivially vulnerable to everyone else.

The good news is that it's relatively easy to tamper with an SSL implementation to make it encrypt and exfiltrate the current RNG seed. This still requires someone to physically alter the library, or install a persistent exploit, but it can be done cleverly without even adding much new code to the existing OpenSSL code. (OpenSSL's love of function pointers makes it particularly easy to tamper with this stuff.)

If tampering isn't your style, why not put the backdoor in plain sight? That's the approach NSA took with the Dual_EC RNG, standardized by NIST in Special Publication 800-90. There's compelling evidence that NSA deliberately engineered this generator with a backdoor -- one that allows them to break any TLS/SSL connection made using it. Since the generator is (was) the default in RSA's BSAFE library, you should expect every TLS connection made using that software to be potentially compromised.

And I haven't even mentioned Intel's plans to replace the Linux kernel RNG with its own hardware RNG.

Esoteric Weaknesses in PFS systems. Many web servers, including Google and Facebook, now use Perfect Forward Secrecy ciphersuites like ephemeral Diffie-Hellman (DHE and ECDHE). In theory these ciphersuites provide the best of all possible worlds: keys persist for one session and then disappear once the connection is over. While this doesn't save you from RNG issues, it does make key theft a whole lot more difficult.

PFS ciphersuites are a good thing, but a variety of subtle issues can cramp their style. For one thing, the session resumption mechanism can be finicky: session keys must either be stored locally, or encrypted and given out to users in the form of session tickets. Unfortunately, the use of session tickets somewhat diminishes the 'perfectness' of PFS systems, since the keys used for encrypting the tickets now represent a major weakness in the system. Moreover, you can't even keep them internal to one server, since they have to be shared among all of a site's front-end servers! In short, they seem like kind of a nightmare.

A final area of concern is the validation of Diffie-Hellman parameters. The current SSL design assumes that DH groups are always honestly generated by the server. But a malicious implementation can violate this assumption and use bad parameters, which enable third party eavesdropping. This seems like a pretty unlikely avenue for enabling surveillance, but it goes to show how delicate these systems are.

The Tinfoil Hat Spectrum

I'm going to refer to the next batch of attacks as '*tinfoil hat*' vulnerabilities. Where the previous issues all leverage well known techniques, each of the following proposals require totally new cryptanalytic techniques. All of which is a way of saying that the following section is *pure speculation*. It's fun to speculate, of course. But it requires us to assume facts not in evidence. Moreover, we have to be a bit careful about where we stop.

So from here on out we are essentially conducting a thought-experiment. Let's imagine the NSA has a passive SSL-breaking capability; and furthermore, that it *doesn't* rely on the tricks of the previous section. What's left?

The following list begins with the most 'likely' theories and works towards the truly insane.

Breaking RSA keys. There's a persistent rumor in our field that NSA is cracking 1024-bit RSA keys. It's doubtful this rumor stems from any real knowledge of NSA operations. More likely it's driven by the fact that cracking 1024-bit keys is highly feasible for an organization with NSA's resources.

How feasible? Several credible researchers have attempted to answer this question, and it turns out that the cost is lower than you think. Way back in 2003, Shamir and Tromer estimated \$10 million for a purpose-built

machine that could factor one 1024-bit key per year. In 2013, Tromer reduced those numbers to about \$1 million, factoring in hardware advances. And it could be significantly lower. This is pocket change for NSA.

Along similar lines, Bernstein, Heninger and Lange examined at the feasibility of cracking RSA using distributed networks of standard PCs. Their results are pretty disturbing: in principal, a cluster about the size of the real-life Conficker botnet could do serious violence to 1024-bit keys.

Given all this, you might ask why this possibility is even in the '*tinfoil hat*' category. The simple answer is: *because nobody's actually done it*. That means it's at least conceivable that the estimates above are dramatically too high -- or even too low. Moreover, RSA-1024 keys are being rapidly being phased out. Cracking 2048 bit keys would require significant mathematical advances, taking us much deeper into the tin foil hat.**

Cracking RC4. On paper, TLS supports a variety of strong encryption algorithms. In practice, about half of all TLS traffic is secured with the creaky old RC4 cipher. And this should worry you -- because RC4 is starting to show its age. In fact, as used in TLS it's already vulnerable to (borderline) practical attacks. Thus it seems like a nice candidate for a true cryptanalytic advance on NSA's part.

Unfortunately the problem with this theory is that we *simply don't know of any attack* that would allow the NSA to usefully crack RC4! The known techniques require an attacker to collect thousands or millions of ciphertexts that are either (a) encrypted with related keys (as in WEP) or (b) contain the same plaintext. The best known attack against TLS takes the latter form -- it requires the victim to establish billions of sessions, and even then it only recovers fixed plaintext elements like cookies or passwords.

The counterargument is that the public research community hasn't been thinking very hard about RC4 for the past decade -- in part because we thought it was so broken people had stopped using it (oops!) If we'd been focusing all our attention on it (or better, the NSA's attention), who knows what we'd have today.

If you told me the NSA had one truly *new* cryptanalytic capability, I'd agree with Jake and point the finger at RC4. Mostly because the alternatives are far scarier.

New side-channel attacks. For the most part, remote timing attacks appear to have been killed off by the implementation of countermeasures such as RSA blinding, which confound timing by multiplying a random blinding factor into each ciphertext prior to decryption. In theory this should make timing information essentially worthless. In practice, many TLS implementations implement compromises in the blinding code that might resurrect these attacks, things like squaring a blinding factor between decryption operations, rather than generating a new one each time. It's quite unlikely there are attacks here, but who knows.

Goofy stuff. Maybe NSA does have something truly amazing up its sleeve. The problem with opening this Pandora's box is that it's really hard to get it closed again. Did Jerry Solinas really cook the NIST P-curves to support some amazing new attack (which NSA knew about way back in the late 1990s, but we have not yet discovered)? Does the NSA have a giant supercomputer named TRANSLTR that can brute-force any cryptosystem? Is there a giant quantum computer at the BWI Friendship annex? For answers to these questions you may as well just shake the Magic 8-Ball, cause I don't have a clue.

Conclusion

We don't know and can't know the answer to these things, and honestly it'll make you crazy if you start thinking about it. All we can really do is take NSA/GCHQ at their word when they tell us that these capabilities are '*extremely fragile*'. That should at least give us hope.

The question now is if we can guess well enough to turn that fragility from a warning into a promise.

Notes:

* A failure of the server RNG could result in some predictable values like the ServerRandom and session IDs. An attacker who can predict these values may be able to run active attacks against the protocol, but -- in the RSA ciphersuite, at least -- they don't admit passive compromise.

** Even though 1024-bit RSA keys are being eliminated, many servers still use 1024-bit for Diffie-Hellman (mostly for efficiency reasons). The attacks on these keys are similar to the ones used against RSA -- however, the major difference is that fresh Diffie-Hellman 'ephemeral' keys are generated for each new connection. Breaking large amounts of traffic seems quite costly.

Posted by Matthew Green at 8:55 PM

--
David Vincenzetti
CEO

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Emmett, Jamie

From: David Vincenzetti <d.vincenzetti@hackingteam.com>
Sent: December-31-13 10:11 PM
To: list@hackingteam.it
Subject: A few more notes on NSA random number generators

Please find an [REDACTED] article by Matthew Green, [REDACTED] also available at his blog at <http://blog.cryptographyengineering.com/2013/12/a-few-more-notes-on-nsa-random-number.html> .

"Last Friday, Joseph Menn from Reuters published an article claiming that **RSA, the pioneering security firm and division of EMC, accepted \$10 million dollars to include as the default the Dual_EC_DRBG random number generator in their flagship BSAFE library.** I've written a bit about Dual_EC on this blog, so readers will know that I don't think very highly of it. **For one thing, it's a rotten choice to use in a cryptographic library simply due to its lousy software performance. Much worse: it may introduce a practical backdoor into any system that uses it."**

"In point of fact, **the possibility of a backdoor was known to at least some members of the ANSI X9.82 standardization committee as far back in January 2005. This surprising news comes via a patent application filed by Certicom employees Dan Brown and Scott Vanstone.** The application claims a priority date of January 2005. **Here's the scary part:**

[...] Therefore, if the ECRNG is used to generate the encryption key K , then it may be possible that the escrow key e can be used to recover the encryption key K . Escrow keys can provide other functionality, such as for use in a wiretap. In this case, trusted law enforcement agents may need to decrypt encrypted traffic of criminals, and to do this they may want to be able to use an escrow key to recover an encryption key. [...]"

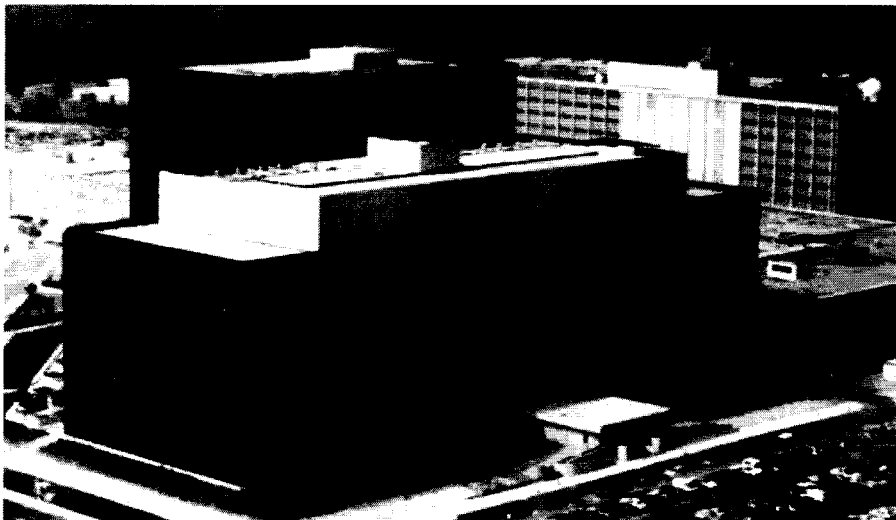
[REDACTED]

[REDACTED]

FYI,
David

Saturday, December 28, 2013

A few more notes on NSA random number generators



Last Friday, Joseph Menn from Reuters published an article claiming that RSA, the pioneering security firm and division of EMC, accepted \$10 million dollars to include as the default the Dual_EC_DRBG random number generator in their flagship BSAFE library. I've written a bit about Dual_EC on this blog, so readers will know that I don't think very highly of it. For one thing, it's a rotten choice to use in a cryptographic library simply due to its lousy software performance. Much worse: it may introduce a practical backdoor into any system that uses it.

Given the numerous problems with Dual_EC it's baffling to me that RSA would select it as the default for their software, particularly as BSAFE is designed for use in Java-based and embedded systems -- where performance truly is at a premium. And none of this can be explained by the needs of a single client since those could be satisfied merely by making BSAFE an *option*, rather than the default.

Of course there have been many people who had already looked askance at RSA's decisions. Indeed, various unsupported rumors have been floating around for some time. What's new this time is that apparently there's enough evidence for those allegations to show up in a Reuters exclusive.

Only time will tell how things go with RSA. In the meantime I have a few small facts to add to this discussion, so I thought I'd sketch them out in yet another blog post.

#1: Dual_EC_DRBG's 'backdoor' was known as of January 2005

It's widely believed that the 'vulnerability' in Dual_EC was first identified by Microsoft employees Dan Shumow and Niels Ferguson in the summer of 2007. Tanja Lange (and nymble) recently tipped me off to the fact that this isn't precisely true.

In point of fact, the *possibility* of a backdoor was known to at least some members of the ANSI X9.82 standardization committee as far back in January 2005. This surprising news comes via a patent application filed by Certicom employees Dan Brown and Scott Vanstone. The application claims a priority date of January 2005. Here's the scary part:

If P and Q are established in a security domain controlled by an administrator, and the entity who generates Q for the domain does so with knowledge of e (or indirectly via knowledge of d). The administrator will have an escrow key for every ECRNG that follows that standard.

Escrow keys are known to have advantages in some contexts. They can provide a backup functionality. If a cryptographic key is lost, then data encrypted under that key is also lost. However, encryption keys are generally the output of random number generators. Therefore, if the ECRNG is used to generate the encryption key K, then it may be possible that the escrow key

e can be used to recover the encryption key K. Escrow keys can provide other functionality, such as for use in a wiretap. In this case, trusted law enforcement agents may need to decrypt encrypted traffic of criminals, and to do this they may want to be able to use an escrow key to recover an encryption key.

...

For example, in the SSL and TLS protocols, which are used for securing web (HTTP) traffic, a client and server perform a handshake in which their first actions are to exchange random values sent in the clear.

This patent also describes a number of ways to *close* the backdoor in Dual_EC_DRBG. Indeed, it may be due to Brown and Vanstone that the NIST standard includes an alternative method to close the backdoor (by generating a random Q point).

The existence of this patent does *not* mean that Brown and Vanstone were responsible for Dual_EC. In fact, the generator was developed at NSA. What it does show is that some members of the ANSI X9.82 standardization committee, of which RSA was also a member, had reason to at least suspect that Dual_EC could be used to create a wiretapping backdoor. (*Update: John Kelsey confirms this.*) It would be curious to know how widely this information was shared, and whether anyone on the committee (listed below) inquired as to the provenance of the default parameters.

#2. Dual_EC_DRBG is not really a NIST standard.

This one is hardly a secret, but it's something that isn't widely acknowledged in the press. Dual_EC_DRBG is generally viewed as a NIST standard, since it was published in NIST Special Publication 800-90. But that's not the only place it appears, nor was it developed at NIST.

A complete history of Dual_EC_DRBG would begin with NSA's drive to include it in the ANSI X9.82 DRBG standard, with a standardization process kicked off in the early 2000s. The draft ANSI standard includes Dual_EC_DRBG with all of the known parameters, along with several additional elliptic curve parameters that were not included in the NIST standards.

ization

om Corporation
om Corporation
unications Security Establishment of Canada
t
t
-Card
al Institute of Standards and Technology
al Institute of Standards and Technology
al Institute of Standards and Technology
al Institute of Standards and Technology
al Security Agency
al Security Agency

Bowes, Inc.
Bowes, Inc.
The Security Division of EMC
The Security Division of EMC
The Security Division of EMC

Representa

Dan Brown
Scott Vansto
Bridget Wals
Don Johnso

Miles Smid
Mike Ward
Elaine Barko
Lily Chen
Morris Dwor
John Kelsey
Paul Timme
Michael Boy
William Why
Matt Campa
Rick Ryan
James Ranc
Burt Kaliski
Steve Schm

Members of the ANSI X9F1 Tool Standards and Guidelines Group which wrote ANSI X9.82.

You'll also find Dual_EC_DRBG in the international standard ISO 18031. In other words, Dual_EC was widely propagated in numerous standards long before NIST finalized it, and it is hardly limited to US borders. The ANSI and ISO standards are in some sense worse, since they don't include any technique for generating your own *Q* parameter.

#3. Dual_EC_DRBG is not the only asymmetric random number generator in the ANSI and ISO standards.

Cryptographers generally think of Dual_EC as the only 'public key' random number generator to be widely standardized. We also point to NSA's generation of the public parameters as evidence that Dual_EC may be compromised.

But in point of fact, the ANSI X9.82 and ISO standards each propose a *second* generator based on public key cryptographic techniques. And just like Dual_EC, this one ships with a complete set of default parameters! The additional generator is based on an algorithm due to Micali and Schnorr, and relies for its security on assumptions related hardness of factoring large composite numbers. It requires an RSA-type modulus, several of which are conveniently provided in the specification.

ulus is of the form $n = pq$ with $p = 2p_1 + 1$, $q = 2q_1 + 1$, where p_1 and q_1 are $(\lg(n)/2 - 1)$ -t

ault modulus n of size 1024 bits

ecimal value of the modulus n is:

```
fda fbac2fd8 2eb13dc4 4fa170ff c9f7c7b5 1d55b214 4cc2257b 2
158 0753f304 a671ff8b 55dd8abf b53d31ab a0ad742f 21857acf 8
771 a61eca54 e62bfd5 85c311b0 58e9cd3f aab758a5 e2896849 6
aa1 55d4d912 6140dcfa b9b03f62 a5032d06 536d8574 0988f384 2
```

ault modulus n of size 2048 bits

ecimal value of the modulus n is:

```
1f2 5daf396a a927157b af6f504f 78cba324 57b58c6b f7d851af 4
6f4 1f6d47ab 1b3a2c12 17d14d15 070c9da5 24734ada 2fe17a95 e
a66 96661e40 7d3043ec d1023126 5d8ea0d1 81cf23c6 dd3dec9e b
9bb cca63dee 435a2251 ad0765d4 9d29db2e f5aba161 279aeb5f 6
36c 1fb13086 d9231b6b 925a8495 4ba0fbca fea844ea 77a9f852 f
0ba b9b269c3 9a7a827a 41311ffa 4470140c 8b6509fe 5dbd39e3 e
e13 0e07e233 06a39b18 db0e8efe 64418880 81ac3673 2b4091f6 6
d74 371a20fc 3e214bce 7ed0e797 5ea44453 cd161d32 e8185204 5
```

Two default MS-DRBG moduli from the ISO 18031 specification.

There's no reason to suspect that MS-DRBG is used by any real products, let alone that there's a backdoor in the standard. In fact, a curious thing is that it's not obvious from the public literature how one would attack this generator even if one knew the factorization of the n values above, though it seems intuitive that an attack does exist. Solving this problem would be a fun project for an enthusiastic mathematician.

Since MS-DRBG comes from the same people who brought you Dual_EC, if you *are* using it you might want to think twice.

Posted by Matthew Green at 10:00 AM

--
David Vincenzetti
CEO

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Thompson, Julie

From: David Vincenzetti <d.vincenzetti@hackingteam.it>
Sent: Tuesday, April 01, 2014 10:40 PM
To: list@hackingteam.it
Subject: The Continuing Public/Private Surveillance Partnership

Please find a [REDACTED] essay by Bruce Schneier on the US IT corporations involvement in the NSA scandal.

[REDACTED]

"If you've been reading the news recently, you might think that corporate America is doing its best to thwart NSA surveillance."

[REDACTED]

"These companies are certainly pissed that the publicity surrounding the NSA's actions is undermining their users' trust in their services, and they're losing money because of it. Cisco, IBM, cloud service providers, and others have announced that they're losing billions, mostly in foreign sales."

"These companies are doing their best to convince users that their data is secure. But they're relying on their users not understanding what real security looks like. IBM's letter to its clients last week is an excellent example. The letter lists five "simple facts" that it hopes will mollify its customers, but the items are so qualified with caveats that they do the exact opposite to anyone who understands the full extent of NSA surveillance. And IBM's spending \$1.2B on data centers outside the U.S. **will only reassure customers who don't realize that National Security Letters require a company to turn over data, regardless of where in the world it is stored."**

"Google's recent actions, and similar actions of many Internet companies, will definitely improve its users' security against surreptitious government collection programs -- both the NSA's and other governments' -- but **their assurances deliberately ignores the massive security vulnerability built into its services by *design* [italics is mine]**. Google, and by extension, the U.S. government, still has access to your communications on Google's servers."

"Google could change that. It could encrypt your e-mail so only you could decrypt and read it. It could provide for secure voice and video so no one outside the conversations could eavesdrop."

"It doesn't. And neither does Microsoft, Facebook, Yahoo, Apple, or any of the others."

"Why not? They don't partly because

[#1] They want to keep the ability to eavesdrop on your conversations [...] "because the U.S. government won't permit it [otherwise]" [...]

[And #2 because they do not want] "to forgo data mining your e-mail and video conversations in exchange for the marketing advantage it would give it over Microsoft [...]"

This article is also available at https://www.schneier.com/blog/archives/2014/03/the_continuing_.html .

Enjoy the reading!

FYI,
David

The Continuing Public/Private Surveillance Partnership

If you've been reading the news recently, you might think that corporate America is doing its best to thwart NSA surveillance.

Google just announced that it is encrypting Gmail when you access it from your computer or phone, and between data centers. Last week, Mark Zuckerberg personally called President Obama to complain about the NSA using Facebook as a means to hack computers, and Facebook's Chief Security Officer explained to reporters that the attack technique has not worked since last summer. Yahoo, Google, Microsoft, and others are now regularly publishing "transparency reports," listing approximately how many government data requests the companies have received and complied with.

On the government side, last week the NSA's General Counsel Rajesh De seemed to have thrown those companies under a bus by stating that -- despite their denials -- they knew all about the NSA's collection of data under both the PRISM program and some unnamed "upstream" collections on the communications links.

Yes, it may seem like the the public/private surveillance partnership has frayed -- but, unfortunately, it is alive and well. The main focus of massive Internet companies and government agencies both still largely align: to keep us all under constant surveillance. When they bicker, it's mostly role-playing designed to keep us blasé about what's really going on.

The U.S. intelligence community is still playing word games with us. The NSA collects our data based on four different legal authorities: the Foreign Intelligence Surveillance Act (FISA) of 1978, Executive Order 12333 of 1981 and modified in 2004 and 2008, Section 215 of the Patriot Act of 2001, and Section 702 of the FISA Amendments Act (FAA) of 2008. Be careful when someone from the intelligence community uses the caveat "not under this program" or "not under this authority"; almost certainly it means that whatever it is they're denying is done under some other program or authority. So when De said that companies knew about NSA collection under Section 702, it doesn't mean they knew about the other collection programs.

The big Internet companies know of PRISM -- although not under that code name -- because that's how the program works; the NSA serves them with FISA orders. Those same companies did not know about any of the other surveillance against their users conducted on the far more permissive EO 12333. Google and Yahoo did not know about MUSCULAR, the NSA's secret program to eavesdrop on their trunk connections between data centers. Facebook did not know about QUANTUMHAND, the NSA's secret program to attack Facebook users. And none of the target companies knew that the NSA was harvesting their users' address books and buddy lists.

These companies are certainly pissed that the publicity surrounding the NSA's actions is undermining their users' trust in their services, and they're losing money because of it. Cisco, IBM, cloud service providers, and others have announced that they're losing billions, mostly in foreign sales.

These companies are doing their best to convince users that their data is secure. But they're relying on their users not understanding what real security looks like. IBM's letter to its clients last week is an excellent example. The letter lists five "simple facts" that it hopes will mollify its customers, but the items are so qualified with caveats that they do the exact opposite to anyone who understands the full extent of NSA surveillance. And IBM's spending \$1.2B on data centers outside the U.S. will only reassure customers who don't realize that National Security Letters require a company to turn over data, regardless of where in the world it is stored.

Google's recent actions, and similar actions of many Internet companies, will definitely improve its users' security against surreptitious government collection programs -- both the NSA's and other governments' -- but their assurances deliberately ignores the massive security vulnerability built into its services by design. Google, and by extension, the U.S. government, still has access to your communications on Google's servers.

Google could change that. It could encrypt your e-mail so only you could decrypt and read it. It could provide for secure voice and video so no one outside the conversations could eavesdrop.

It doesn't. And neither does Microsoft, Facebook, Yahoo, Apple, or any of the others.

Why not? They don't partly because they want to keep the ability to eavesdrop on your conversations. Surveillance is still the business model of the Internet, and every one of those companies wants access to your communications and your metadata. Your private thoughts and conversations are the product they sell to their customers. We also have learned that they read your e-mail for their own internal investigations.

But even if this were not true, even if -- for example -- Google were willing to forgo data mining your e-mail and video conversations in exchange for the marketing advantage it would give it over Microsoft, it still won't offer you real security. It can't.

The biggest Internet companies don't offer real security because the U.S. government won't permit it.

This isn't paranoia. We know that the U.S. government ordered the secure e-mail provider Lavabit to turn over its master keys and compromise every one of its users. We know that the U.S. government convinced Microsoft -- either through bribery, coercion, threat, or legal compulsion -- to make changes in how Skype operates, to make eavesdropping easier.

We don't know what sort of pressure the U.S. government has put on Google and the others. We don't know what secret agreements those companies have reached with the NSA. We do know the NSA's BULLRUN program to subvert Internet cryptography was successful against many common protocols. Did the NSA demand Google's keys, as it did with Lavabit? Did its Tailored Access Operations group break into to Google's servers and steal the keys?

We just don't know.

The best we have are caveat-laden pseudo-assurances. At SXSW earlier this month, CEO Eric Schmidt tried to reassure the audience by saying that he was "pretty sure that information within Google is now safe from any government's prying eyes." A more accurate statement might be, "Your data is safe from governments, except for the ways we don't know about and the ways we cannot tell you about. And, of course, we still have complete access to it all, and can sell it at will to whomever we want." That's a lousy marketing pitch, but as long as the NSA is allowed to operate using secret court orders based on secret interpretations of secret law, it'll never be any different.

Google, Facebook, Microsoft, and the others are already on the record as supporting these legislative changes. It would be better if they openly acknowledged their users' insecurity and increased their pressure on the government to change, rather than trying to fool their users and customers.

This essay previously appeared on TheAtlantic.com.

Posted on March 31, 2014 at 9:18 AM

--

David Vincenzetti
CEO

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com