The control of Cryptography Past, Present and Future Intelligence versus Forensics Aspects

Eric Filiol filiol@esiea.fr
ESIEA - Operational cryptology and Virology Lab (C + V)^{O}
https://sites.google.com/site/ericfiliol

Agenda

- Introduction: The Past and Present Context
- History and Legal
- Case studies of the control nowadays
- Case of Non Connected/Non-classical Environments
- Conclusion

About the Speaker

- Background in mathematics and computer science (Ing. – Ph D – Prof.)
- 22 years in the French Army (Infantry/Marine Corps) half part in technical intelligence (SIGINT)
- Since 2008, heading a non profit R & D lab in offensive security
  - Connection with the French DoJ (forensics analysis of terrorist case mostly) and with the French DoD

INTRODUCTION

70 years of Cryptography Control – The Context.

Aim ot the Keynote

- Understand why criminal investigations are bound to fail everytime strong cryptography is used by clever criminals
- Understand why National Security Issues are and will always be prevalent over DoJ/Police concerns

Aim ot the Keynote

- My keynote will be more intelligence-oriented
- Refer to my past talks at HIP 2013, PhDays 2014 and my paper in the Journal of Information Warfare for more technical details
- Contact me for other cases studies, examples…

What is the Situation

- Past and present
  - Criminals use cryptography in a dummy and weak way… or simply do not use it at all
  - Crypto forensics is often possible due to the weakness of the systems and/or the stupidity of attackers
- Present and future
  - Strong crypto, strong systems, educated and cautious attackers/criminals
- The situation is worsening (e.g. recent protest of US Justice against Google/Apple) due to Snowden's leaks
- Interesting case: TOR network

- Past
  - C… veak way… or si…
  - C… weakness of th…
- Pres…
  - St… and cautious at…
- The … otest of US Just… vden's leaks
- Inte…

The New York Times

The Opinion Pages | OP-ED CONTRIBUTORS

When Phone Encryption Blocks Justice

By CYRUS R. VANCE Jr., FRANÇOIS MOLINS, ADRIAN LEPPARD and JAVIER ZARAGOZA AUG. 11, 2015

Sébastien Thibault

Email

In June, a father of six was shot dead on a Monday afternoon in Evanston, Ill., a suburb 10 miles north of Chicago. The Evanston police believe that

LAW & DISORDER / CIVILIZATION & DISCONTENTS

FBI busts through huge Tor-hidden child porn site using questionable malware

US security service seized server, let site run for two weeks before shutting it down.

by Cyrus Farivar and Sean Gallagher (US) - Jul 16, 2015 5:25pm CEST

Teymur Madjderey

Email

Ill., a suburb 10 miles north of Chicago. The Evanston police believe that

The Reality Behind Cybercriminality

- Until around 2010, conducted by real criminals
- Since 2010, most of the G-20 countries entered also into the game and are also conducting cyber attacks/cybercriminality for National Security reasons
- What is illegal in Europe or in India may be seen as legal by the USA/NSA-CIA or by the China/GUOANBU!

The Context

- The control techniques depend on the target context/environment

Type	Data	NSA Programs	Techniques	Examples
Connected	Plaintext	PRISM, Xkeyscore…	Data collection, wiretapping, eavesdropping, agreements with industry/providers….	Google, Facebook, Apple, Microsoft (including Skype)…
	Ciphertext	Bullrun/Edgehill…	Malware, 0-day exploitation, random generator control, security standards control, controlling CAs, bugging software, applied cryptanalysis…	Heartbleed, RSA, Google/ANSSI, Mail.ru, Alibaba…
Connected by private network	Ciphertext	Cottonmouth, Godsurge, TOR attack, Quantum, Foxacid, Firework, Bulldozer…	Malware, 0-day exploitation, random generator control, controlling CAs, security standards control, bugging software, hardware bugs, mathematical trapdoors…	TOR network, Gasprom, Petrobras, French MFA, Aeroflot, Total. Airbus, SWIFT…
Non-connected (offline)	Ciphertext	TAO, still unknown projects???	Tempest techniques, mathematical backdoors, hardware bugging, Humint	Hans Buehler Case (1995). Gov, MIL, Sensitive companies

Facts

- Many things are technically possible
- Many things are not politically desirable
- We face a real, global and fierce war against cybercriminals…
- … but in the context of the supremacy/hegemony of one superpower (the USA) and tomorrow of two superpowers (USA and China)

Facts

- In the context of international cooperation between countries (police, defence), as soon as cryptography is concerned, there is no longer cooperation but national interests

« *Sharing information with allied countries is no longer possible as soon as it becomes a National Security matter* »

Stacy M. Arruda, Supervisory Special Agent, Cyber Crime Squad, FBI at Virus Bulletin Conference 2007 – Vienna

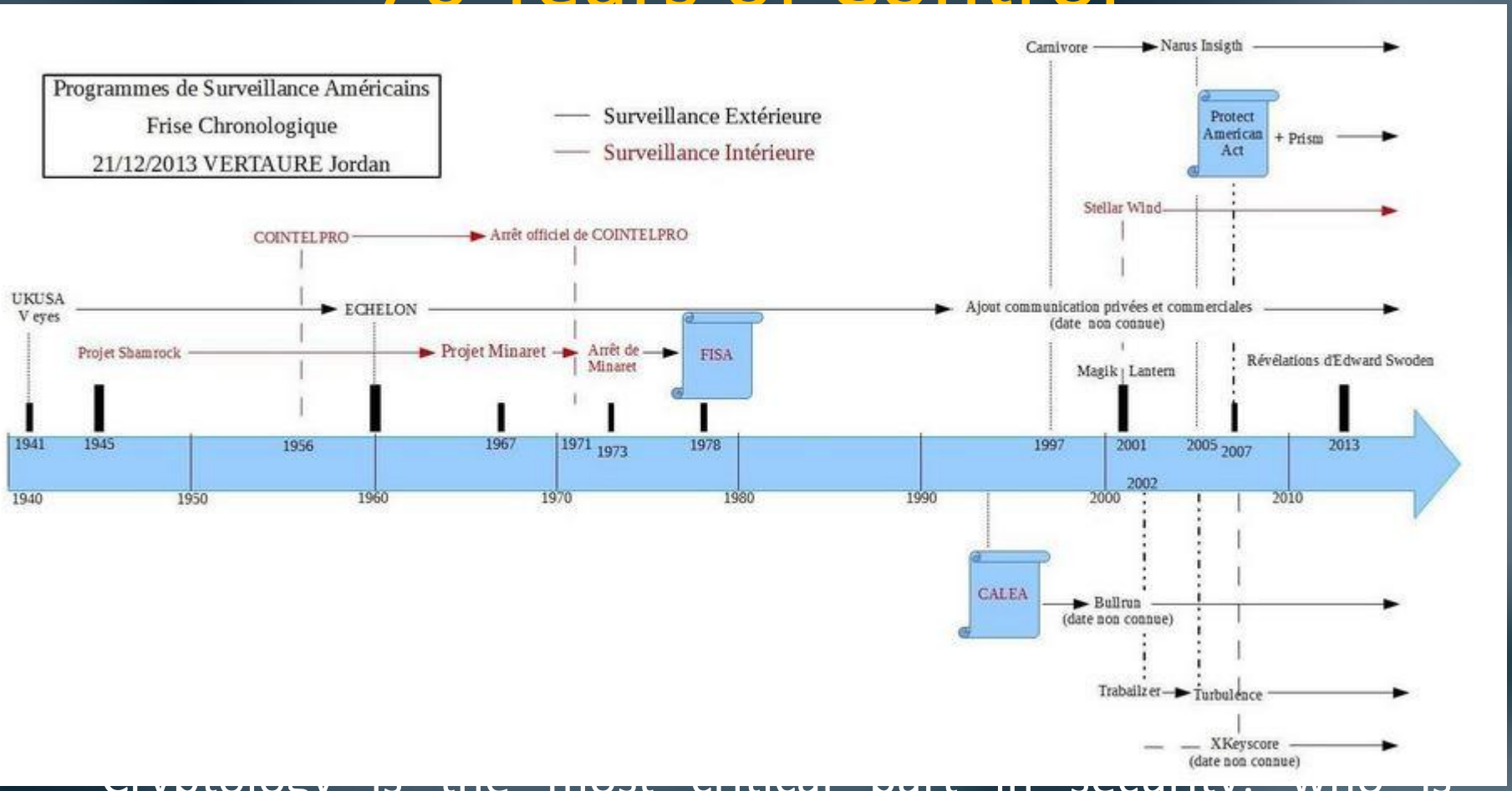
- Nothing has changed since.

HISTORY & LEGAL

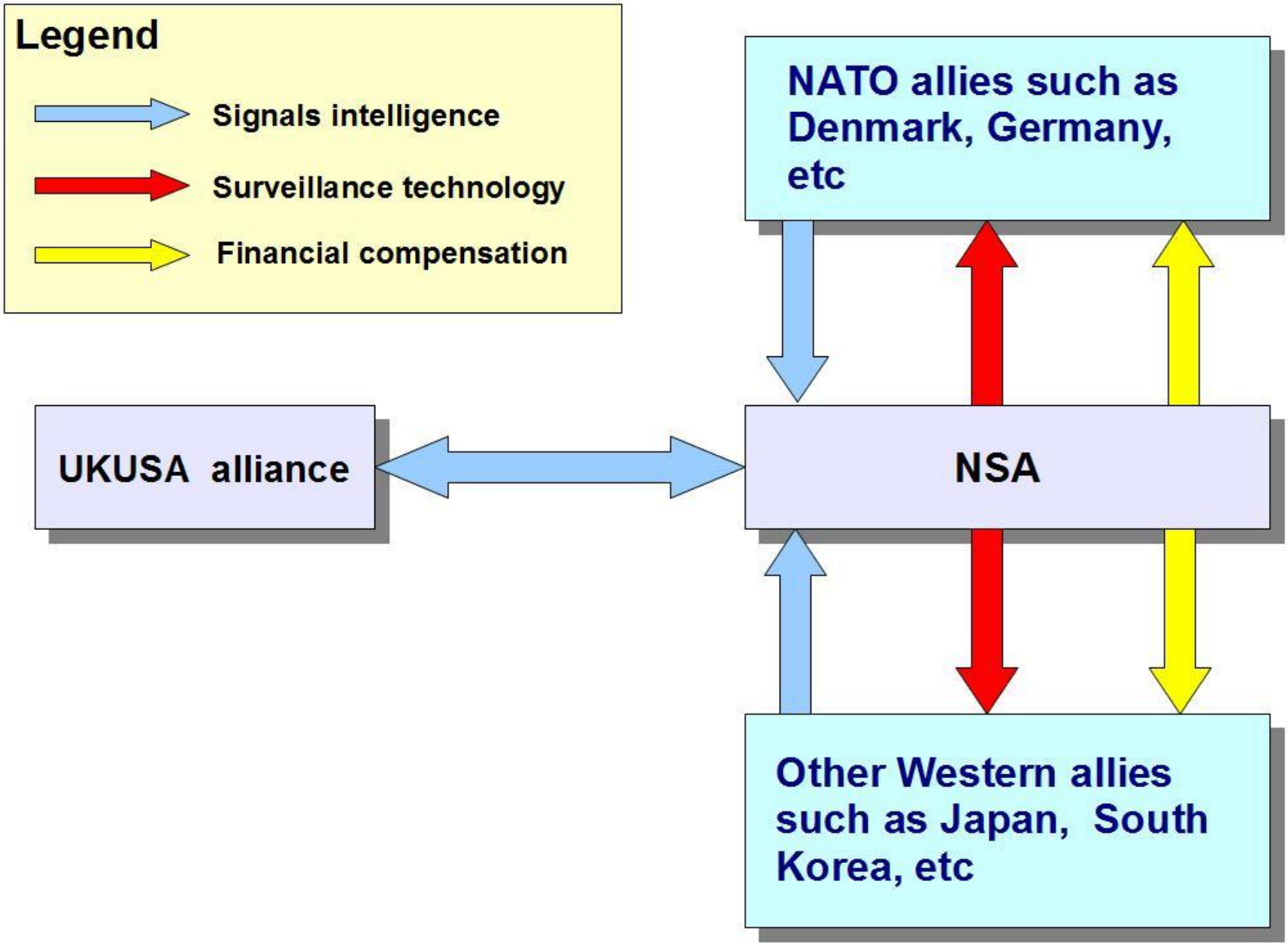
70 Years of Control

- Since the end of WWII, cryptology is under control. This control has never weakened
- UKUSA (5 eyes)/9 eyes/14 eyes – SIGINT Seniors Europe…
  - Which European country will become the 6th eye?
- International Traffic in Arms regulations (ITAR, part 121) and subsequent regulations (Wassenaar…)
  - If cryptology is allowed/free of use, then it is under control.
  - 1997 is a key year (withdrawn from ITAR) and early 2000s in Europe: the rise of connected world. The control will be far easier (computer, OS, network…)
  - Since the early 2000s, cryptography is available to anyone
- Cryptology is the most critical part in security: who is controlling cryptology, is controlling everything

70 Years of Control



Cryptology is the most critical part in security. Who is controlling cryptology, is controlling everything


Legend
Signals intelligence
Surveillance technology
Financial compensation
NATO allies such as Denmark, Germany, etc
UKUSA alliance
NSA
Other Western allies such as Japan, South Korea, etc

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE

Font-size: A Print:

Latest News / Top Stories

- Is the West "Directly" Responsible for the Massacres In Ukraine?
- Oligarch Ihor Kolomoyskyi: Washington's "Man in Ukraine"
- Justifying the Unjustifiable. How the UN Defines "Human Rights"
- America Brings Hell to Ukraine as Part of its Plan for World Domination
- Turkish Mine Explosion, Predicted in 2010
- Fatal Car Crashes in America: US Government Whitewashes GM's Responsibility for Deadly Ignition Defect
- Ukraine: Oligarch Ihor Kolomoisky Offers $1 Million to Murder Federalist Leader Oleg Tsarev

All Articles

NEWS
MOST POPULAR
GEOGRAPHIC REGIONS
THEMES
I-BOOKS SERIES
IN-DEPTH REPORTS
THE GLOBAL RESEARCH NEWS HOUR

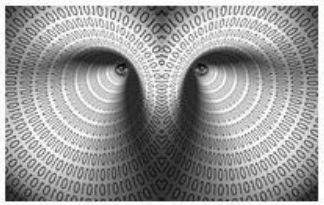
Global Research Newsletter:
enter your email GO

ible for the Massacres In Ukraine? Justifying the Unjustifiable. How the UN Defines "Human Rights"

Swedish Intelligence Service Spying on Russia for US National Security Agency

By Jordan Shilton
Global Research, December 30, 2013
World Socialist Web Site

Region: Europe, Russia and FSU
Theme: Intelligence



Documents released by Edward Snowden reveal that Sweden's National Defence Radio Establishment (FRA) has been collecting large quantities of communications data from Russia, which it has passed to the American National Security Agency (NSA).

The revelations confirm that such collaboration goes back for decades.

According to one document published by public broadcaster SVT December, Stockholm signed a top-secret cooperation agreement in 1954 with the United States, Britain, Australia, New Zealand and Canada—the so-called Five Eyes—to exchange intelligence information. This was replaced in 2004 by bilateral agreements with each country, which saw the collaboration intensify. Throughout the Cold War, FRA passed information obtained from the Soviet Union to its Western allies.

"The relationship with Sweden is protected on the top-secret level because of the country's political neutrality," a 2006 NSA document noted.

Due to its geographic location, the FRA has access to Russian communications, including those from "high priority" targets from politics and areas of economic interest, such as the energy sector. Estimates from *Russia Today* put the amount of communications data from Russia that passes through Sweden at 80 percent. A recent NSA document from April 2013 states, "FRA provided NSA (with a) unique collection on high-priority Russian targets, such as leadership, internal politics."

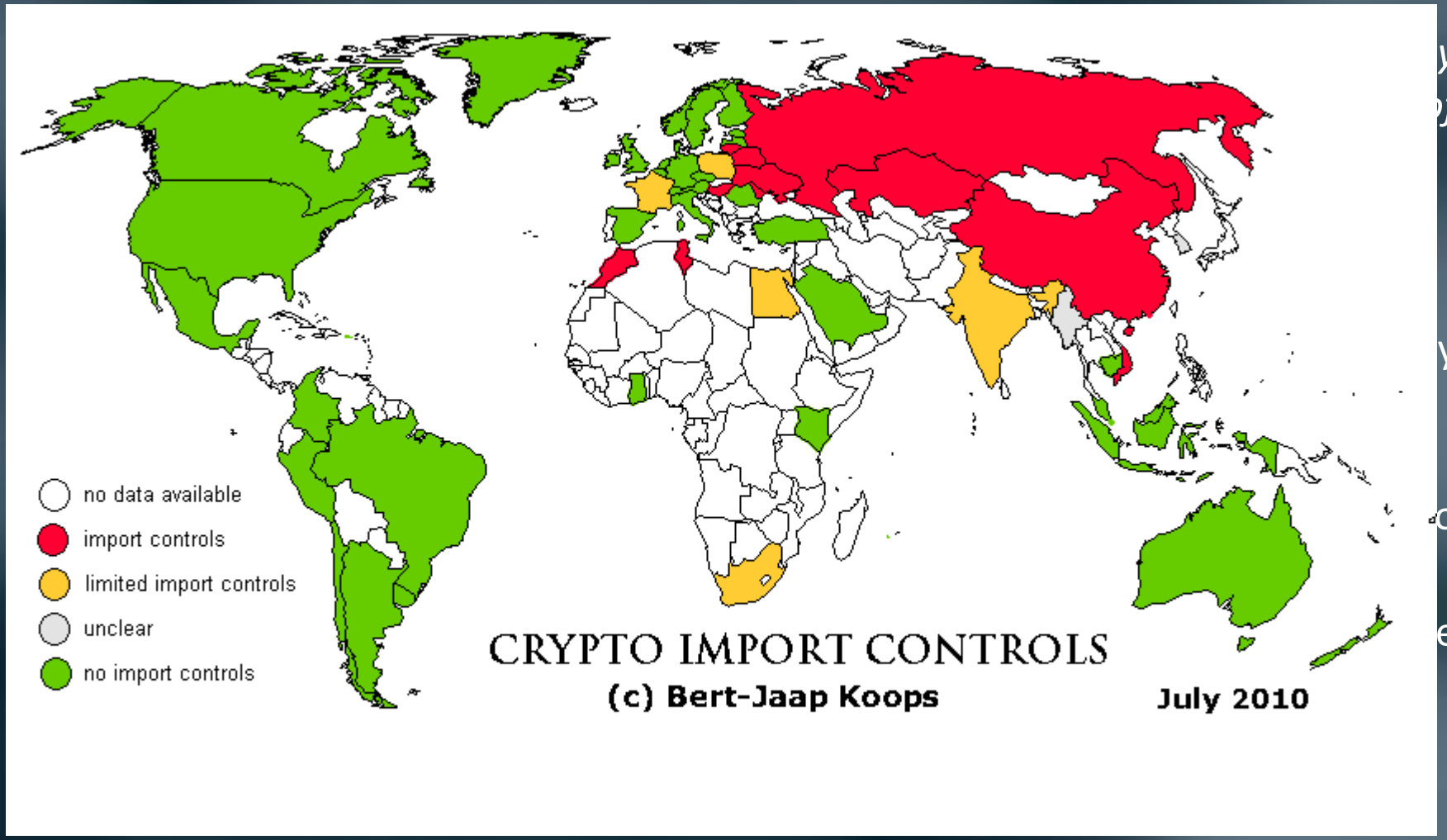
The cooperation between FRA and the NSA was expanded significantly in 2011, with the NSA gaining access to FRA's network of cables. This included the ability to intercept communications from the Baltic countries through under-sea cables controlled by Sweden.

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

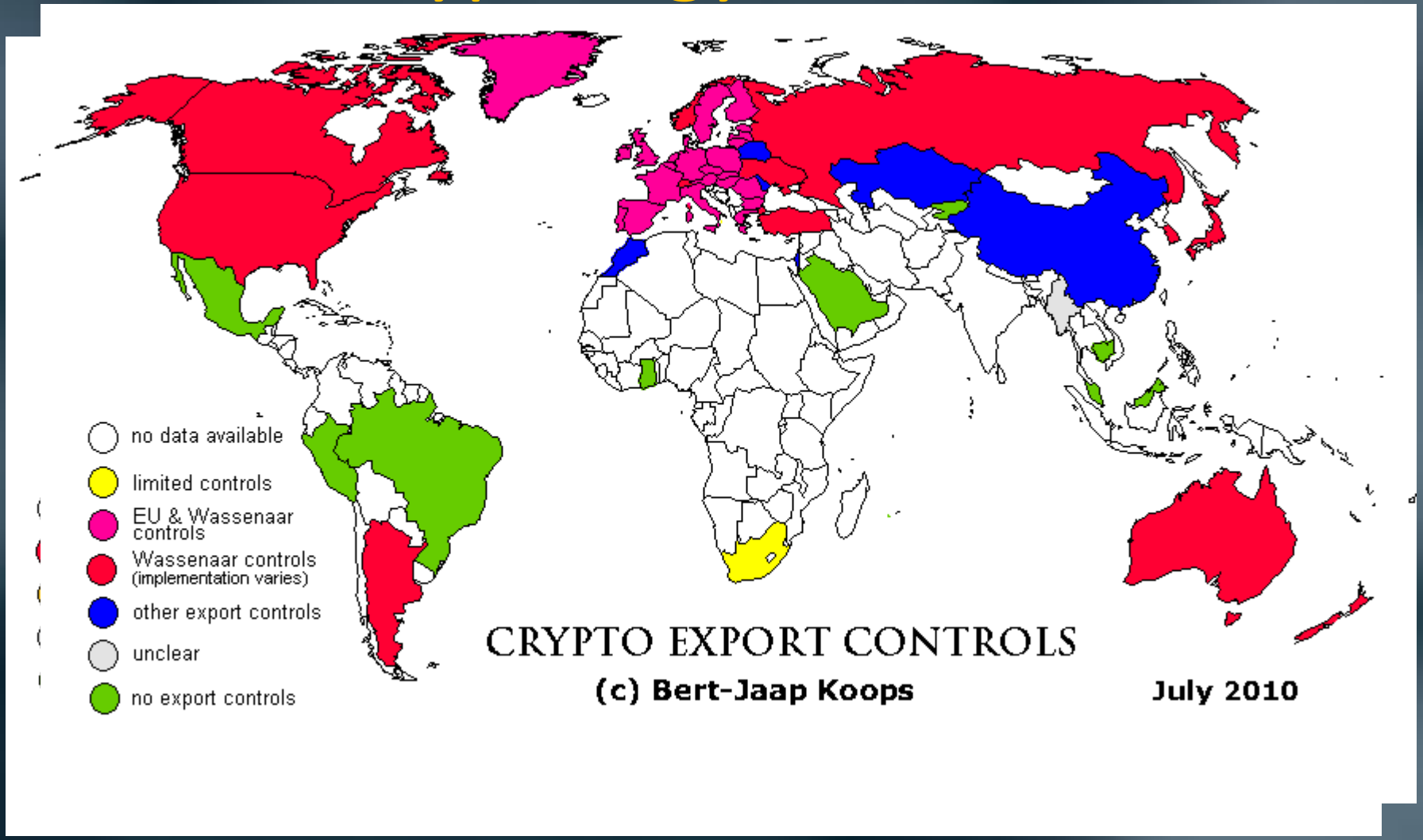
Cryptology Control

- *Who would be so naive to believe that free, strong and secure cryptography algorithms would be made widely available to anyone without some of control, especially in the context of cold war, of ever-growing terrorism…?*
- Cryptology is still under a strong control
- http://rechten.uvt.nl/koops/cryptolaw/
- Almost all G-20 countries have a national regulation regarding cryptology (use/import/export) or at least have signed an international regulation
  - India is close to French regulations.
- The question is: can we accept to sub-contract our cryptographic security to one single nation?
  - **It must be a national issue**, not an international issue (General de Gaulle's decision in France)!

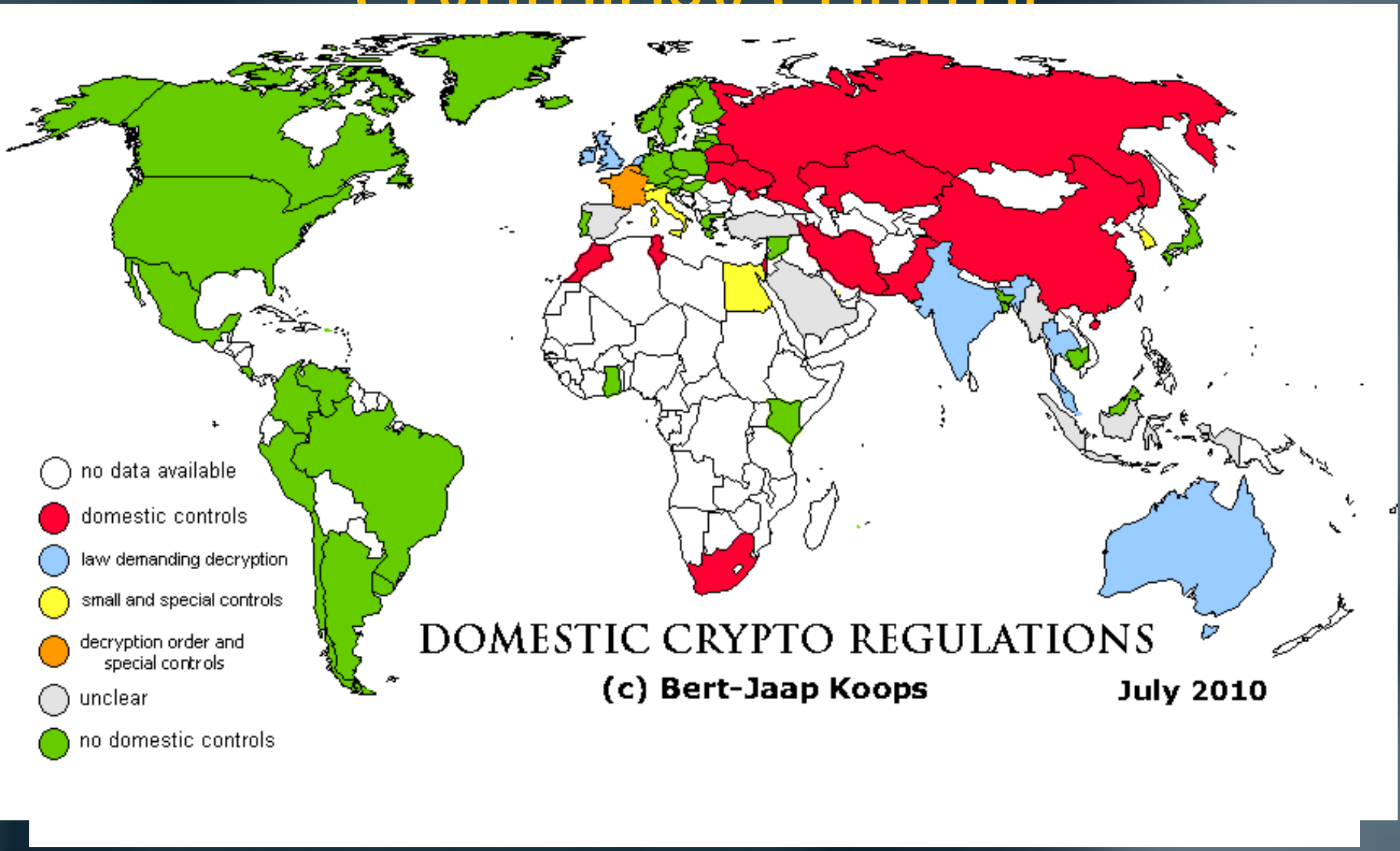
Cryptology Control



Cryptology Control



Cryptology Control



The Wassenaar Agreement

- http://www.wassenaar.org/
- 42 members (India is not a member)
- Cryptology is listed in part 5b
- First level of control:
  - « Good/fair » countries vs other countries (the rest of the world)
- If you analyze the regulations, exporting encryption algorithms with key size greater than 56 bits is subject to export control!
- The world diffusion of the AES (key size ≥ 128 bits) would be hence a clear violation of the Wassenaar agreement…unless some sort of “other” control has been organized/enforced.
- Revised in Dec 2013: 0-days, exploit and attack software are now under export control as well (list 4).
- Sharing technical information is considered as technology export

France’s Translation of Wassenaar

- Similar to Western countries application (including the USA).

Exportation et transfert de moyens de cryptologie depuis la France

Moyen de cryptologie (la catégorie signalée fait référence aux annexes du décret n° 2007-663)	**TRANSFERT VERS UN ÉTAT MEMBRE DE LA COMMUNAUTÉ EUROPÉENNE**	**EXPORTATION VERS SEPT ÉTATS IDENTIFIÉS (1)**	**EXPORTATION VERS D'AUTRES ÉTATS**
- assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité - de type : cartes à puce (carte bancaire, gsm, décodeur tv...), récepteurs de télévision ou de radiodiffusion, protection contre la duplication, lecteurs dvd... (catégories 1 à 7 de l'annexe 1) - transporté par une personnalité sur invitation officielle ou par une personne physique pour son usage exclusivement personnel (catégorie 8 de l'annexe 1) - employant des clés cryptographiques de taille restreinte (catégorie 13 de l'annexe 1)	LIBRE		
- de type grand public (catégorie 3 de l'annexe 2)	DECLARATION		
- employant des clés cryptographiques de grande taille (catégorie 1 de l'annexe 2)	DECLARATION	DECLARATION [Licence générale communautaire]	AUTORISATION [Licence individuelle ou globale]
- permettant la cryptanalyse	AUTORISATION [Licence individuelle ou globale]		

(1) Australie, Canada, États-Unis d'Amérique, Japon, Nouvelle-Zélande, Norvège et Suisse

Exportation et transfert de moyens de cryptologie depuis la France

Moyen de cryptologie (la catégorie signalée fait référence aux annexes du décret n° 2007-663)	TRANSFERT VERS UN ÉTAT MEMBRE DE LA COMMUNAUTÉ EUROPÉENNE	EXPORTATION VERS SEPT ÉTATS IDENTIFIÉS (1)	EXPORTATION VERS D'AUTRES ÉTATS
- assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité - de type : cartes à puce (carte bancaire, gsm,			

CATEGORIE : 13
Moyens de cryptologie ne mettant en oeuvre aucun algorithme cryptographique présentant l'une des caractéristiques suivantes :
a) un algorithme cryptographique symétrique employant une clé de longueur supérieure à 56 bits ;
b) un algorithme cryptographique asymétrique fondé soit sur la factorisation d'entiers de taille supérieure à 512 bits, soit sur le calcul de logarithme discret dans un groupe multiplicatif d'un corps fini de taille supérieure à 512 bits ou dans un autre type de groupe de taille supérieure à 112 bits.

- de type grand public (catégorie 3 de l'annexe 2)	DECLARATION		
- employant des clés cryptographiques de grande taille (catégorie 1 de l'annexe 2)	DECLARATION	DECLARATION [Licence générale communautaire]	AUTORISATION [Licence individuelle ou globale]
- permettant la cryptanalyse	AUTORISATION [Licence individuelle ou globale]		

(1) Australie, Canada, États-Unis d'Amérique, Japon, Nouvelle-Zélande, Norvège et Suisse

Second Level of Control

- USA vs the rest of the world
- « *The power of a country lies in its ability to impose standards* »

  Bernard Carayon (French MP)
- US Cryptographic standards everywhere!
- During the AES contest, block cipher technology was the only standard authorized.
- The issue for the USA is hence to control norms and standards (e.g ISO)
- The Gost Case and the ISO/IEC 18033-3 (2012). See my talk at RusKrypto 2014.

Cryptography Industry after WWII

- Producing countries of crypto:
  - UK (Racal), D (Siemens), S (Ericsson), CH (Gretag, Crypto AG), FR (Sagem, Thales, Matra), SF (Nokia), Hungary…
  - Guess which is missing?
- In Switzerland, Crypto AG/Gretag hold more than 90 % of the world market (since 1945) of Govt Encryption Devices
  - Almost all countries/organizations (130 in 1995 including India) were buying cryptomachines for {gvt, mil, diplomatic, economic} needs except a very few.
- 1995 The Hans Buehler case changed the cryptologic face of the world and forces NSA/UKUSA to change the rules of the game.

The Hans Buehler Case

- Crypto AG's top marketing representative arrested in Teheran in 1992.
- Leaks in the Press (Berlin Club bombing, Chapur Bakhtiar assassination in Paris) by Gov. officials that gave hints to Iranian government that cryptography was probably trapdoored.
- 9 months in Iranian jails
- Reveals the scandal: NSA, BND and others have infiltrated Crypto AG. Gretag and others to put trapdoors in export versions of crypto machines systematically (**India was a client of Crypto AG and maybe still is**).
- The USA were able to read openly most of the world encrypted traffic during nearly 50 years for nearly 130 countries and world organizations
- Consequences: confidence in cryptography industry is severely weakened
- **Interesting point**: from the early 90s a significant number of trapdoored algorithms were block ciphers!

HOW TO CONTROL CRYPTO NOWADAYS CASE STUDIES

Issues like Bullrun, XKeyScore, RSA Dual_EC_DRBG, Heartblead, Windows oddities, Google vs ANSSI…

Bullrun/Edgehill Programs

- Goal: bypass operationally any cryptology protection
- Applied cryptanalysis more that cryptanalysis
  - Tampering with national standards (NIST is specifically mentioned) to promote weak, or otherwise vulnerable cryptography (e.g Dual_EC_DRBG, AES ?)
  - Influencing standards committees to weaken protocols (or influencing to bar strong algorithms [Gost])
  - Working with hardware and software vendors to weaken encryption and random number generators (Microsoft)
  - Attacking the encryption used by GSM phones.
  - Identifying and cracking vulnerable keys
  - Establishing a Human Intelligence division to infiltrate the global telecommunications industry
  - Bypassing SSL connections
- Annual budget: 250 millions $ per year.

ms

- Goal: k
- Applie
  - Tan
    pro
    Dua
  - Infl
    to k
  - Wo
    and
  - Att
  - Ide
  - Est
    tele
  - Byp
- Annua

y mentioned) to
otography (e.g

s (or influencing

aken encryption

rate the global

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | T

News › World news › The NSA files

Series: Glenn Greenwald on security and liberty

Previous | Next | Index

Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

- Q&A: submit your questions for our privacy experts

James Ball, Julian Borger and Glenn Greenwald
Guardian Weekly, Friday 6 September 2013
Jump to comments (4142)

Through covert partnerships with tech companies, the spy agencies have inserted secret vulnerabilities into encryption software. Photograph: Kacper Pempel/Reuters

US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails.

Article history

The NSA Files: Decoded

What the surveillance revelations mean for you

World news
The NSA files · NSA · Surveillance · United States · US national security · Privacy

UK news
GCHQ

Technology
Internet · Data protection

Dual_EC_RDBG – RSA B-Safe

- Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG). Used to generate random keys. ISO and ANSI standards
- Used in many environments (Blackberry, SSL/TLS…)
- Fixed choice of constants P and Q makes most of the backdoor (see http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html)
- Shumow-Ferguson Crypto 2007
- Nobody knows where Dual_EC_RDBG parameters came from
- In SSL/TLS, NSA can recover the pre-master secret (RSA handshake) easily

A.1 Constants for the Dual_EC_DRBG

The **Dual_EC_DRBG** requires the specifications of an elliptic curve and two points on the elliptic curve. One of the following NIST **approved** curves with associated points **shall** be used in applications requiring certification under [FIPS 140]. More details about these curves may be found in [FIPS 186]. If alternative points are desired, they **shall** be generated as specified in Appendix A.2.

Each of following curves is given by the equation:

$$y^2 = x^3 - 3x + b \pmod{p}$$

Notation:

p - Order of the field F_p , given in decimal

n - Order of the Elliptic Curve Group, in decimal .

a – (-3) in the above equation

b - Coefficient above

The x and y coordinates of the base point, i.e., generator G, are the same as for the point P.

A.1.1 Curve P-256

p = 115792089210356248762697446949407573530086143415290314195533631308867097853951

n = 115792089210356248762697446949407573529996955224135760342422259061068512044369

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

Px = 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

Py = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

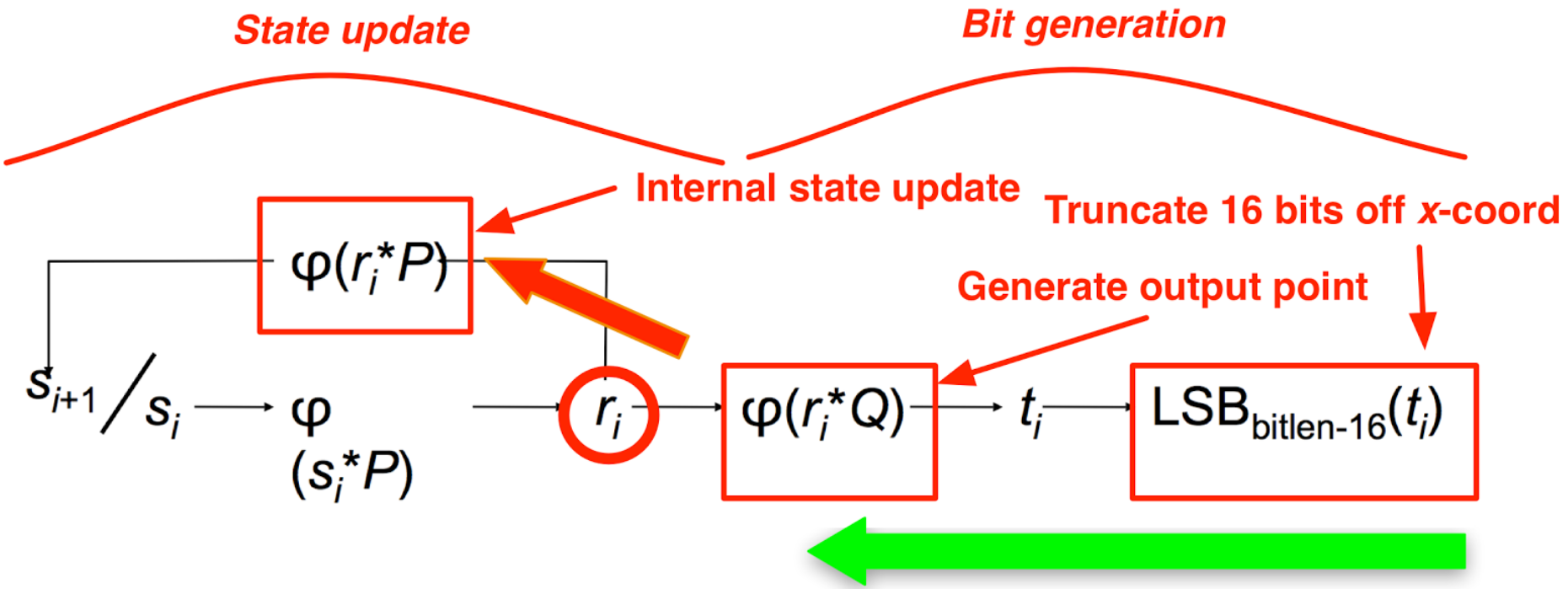
Qx = c97445f4 5cdef9f0 d3e05e1e 585fc297 235b82b5 be8ff3ef ca67c598 52018192

Qy = b28ef557 ba31dfcb dd21ac46 e2a91e30 7f2bec89 b2d8238b 87058ada 2cb81515 1e610046

A.1 Constants for the Dual_EC_DRBG

The **Dual_EC_DRBG** requires the specifications of an elliptic curve and two points on the elliptic curve. One of the following NIST **approved** curves with associated points **shall** be used in applications requiring certification under [FIPS 140]. More details about these curves may be found in [FIPS 186]. If alternative points are desired, they **shall** be generated as specified in Appendix A.2.

Each of following curves is given by the equation:



- In
ha

(RSA

```
      f4a13945 d898c296

Py = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece
     cbb64068 37bf51f5

Qx = c97445f4 5cdef9f0 d3e05e1e 585fc297 235b82b5 be8ff3ef
     ca67c598 52018192

Qy = b28ef557 ba31dfcb dd21ac46 e2a91e30 7f4f6ea5 87058ada
     2cb81515 1e610046
```

Dual_EC_RDBG Timeline

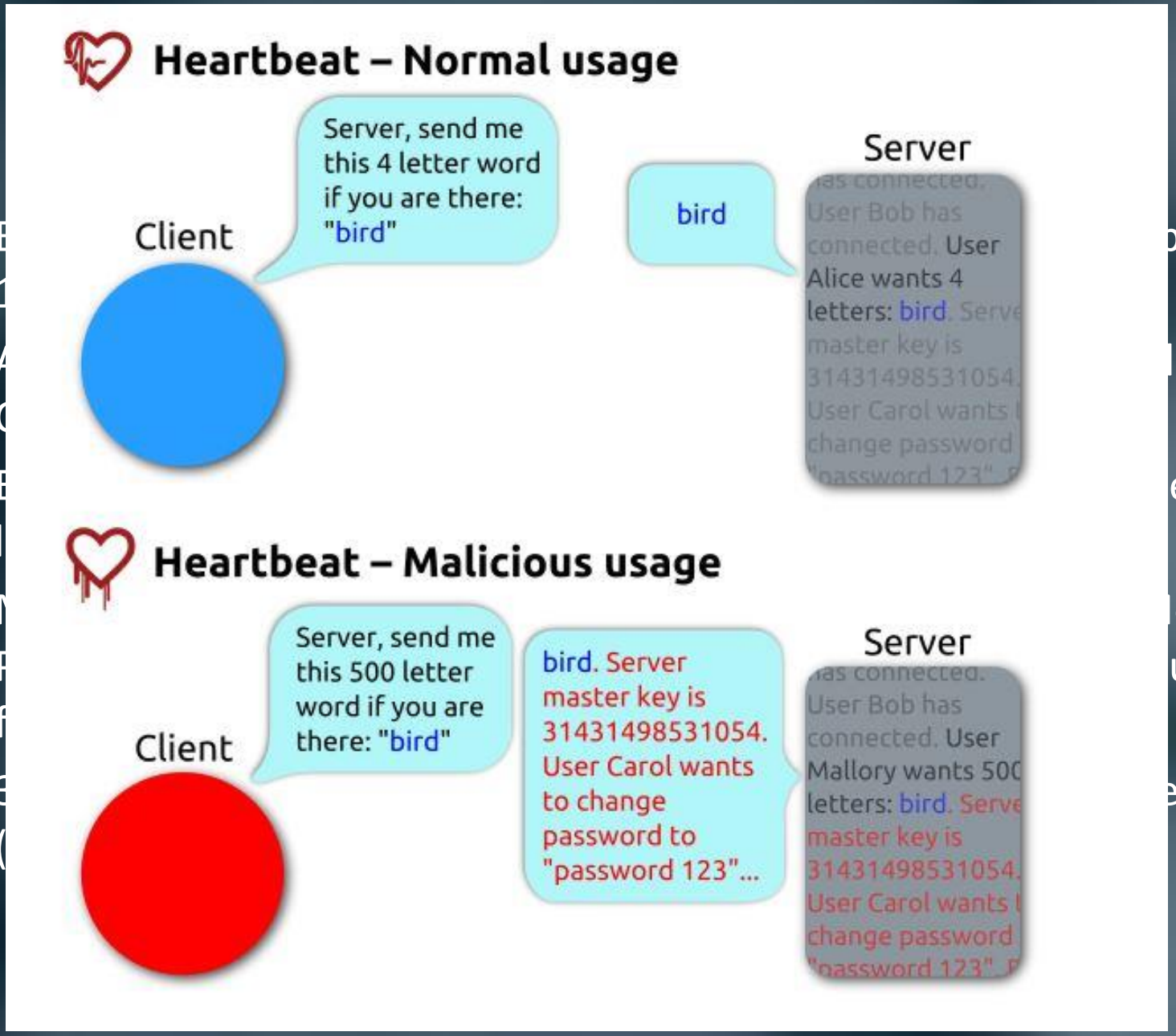
- 2004 - RSA makes Dual_EC_DRBG the default CSPRNG in BSAFE
- 2005 - ISO/IEC 18031:2005 is published, and includes Dual_EC_DRBG. The first draft of NIST SP 800-90A is released to the public, includes Dual_EC_DRBG
- 2006 – 2007 – Works suggesting the existence of a NSA backdoor (K. Gjosteen, Berry Schoenmakers and Andrey Sidorenko, Shumow/Fergusson…)
- June 2006 - NIST SP 800-90A is published, includes Dual_EC_DRBG with the defects pointed out by Kristian Gjøsteen and Berry Schoenmakers and Andrey Sidorenko not having been fixed.
- June/Sep. 2013 – Snowden leak about Bullrun and Dual_EC_DRBG
- 19 Sep. 2013 - RSA Security advises its customers to stop using Dual_EC_DRBG in RSA Security's *BSAFE* toolkit
- Dec. 2013 - Reuters reports this is a result of a secret $10 million deal with NSA
- April 21st, 2014, Following a public comment period and review, NIST removed Dual_EC_DRBG as a cryptographic algorithm from its draft guidance on random number generators, recommending "that current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible
- Has NIST still the legitimacy and technical ability to impose standards to the rest of the world? What about the AES?

Hot Issue

- Specific subtle formulation in the NIST standard meant that you could only get the crucial FIPS 140-2 validation (Cryptographic Module Validation Program) of your implementation if you used the original compromised *P* and *Q* values
- This includes the FIPS 140-2 statistical test suite (now NIST STS) which are THE *de facto* world standard for cryptography statistical evaluation/validation
  - Passing successfully the tests does mean your generator is secure
- Up to me, FIPS 140-2 tests are "backdoored" (they are purposely non significant enough by not including a few additional testing techniques)
- Issue of statistical test simulability (Filiol, 2006): "*if I know your tests, I can simulate and bypass them*"
- Cryptography statistical validation should use a secret national process/set of tests (as it is the case in France)

Heartbleed

- Buffer over-read vulnerability introduced by mistake in OpenSSL 1.0.1 (validated Dec. 31st, 2011, issued March 14th, 2012)
- April 2014, vulnerability disclosed independently by Google and Codenomicon (CVE-2014-0160). Corrected by April 7th, 2014
- Enable to recover sensitive information through server memory leak (password, SSL keys…)
- Many victims (Amazon, Github, hotmail, LibreOffice, McAfee, Password managers, Android 4.1.1, CISCO firmware, Juniper firmware, WD firmware…)
- 30,000 X.509 certificates compromised while only a few revoked (source Netcraft)


Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". R
Heartbeat – Malicious usage
Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". R

Heartbleed Issues

- According to Bloomberg, NSA has exploited CVE-2014-0160 at least for 2 years
- Exploitation of 0-day confirmed by the USA (http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities)
- Backdoor could be disguised as intended vulnerabilities/bugs (invoke the incompetence of programmers)
- Most of the IT US firms communicate 0-day to NSA days before disclosure
- They do not need to put backdoors, 0-days do the job (dynamic management of security holes)

- Acc… …160 at leas…
- Exp… …USA (htt… …eed-und…
- Bac… …s/bugs (inv…
- Mos… …A days befo…
- The… …ne job (dyr…

Bloomberg News Quick Markets Personal Finance Tech U.S. Politics Sustainability Luxury Vide

NSA Said to Exploit Heartbleed Bug for Intelligence for Years

Save +

By Michael Riley | Apr 12, 2014 6:00 AM GMT+0200 **597 Comments** **Email** **Print**

The U.S. National Security Agency knew for at least two years about a flaw in the way that many websites send sensitive information, now dubbed the Heartbleed bug, and regularly used it to gather critical intelligence, two people familiar with the matter said.

Photographer: Brooks Kraft/Corbis

The National Security Agency in Fort Meade, Maryland.

The agency's reported decision to keep the bug secret in pursuit of national security interests threatens to renew the rancorous debate over the role of the government's top computer experts. The NSA, after declining to comment on the report, subsequently denied that it was aware of Heartbleed until the vulnerability was made public by a private security report earlier this month.

"Reports that NSA or any other part of the government were aware of the so-called Heartbleed vulnerability before 2014 are wrong," according to an e-mailed statement from the Office of the Director of National Intelligence.

Related:

- **Millions of Android Devices Vulnerable to Heartbleed Bug**
- **Heartbleed Found in Cisco, Juniper Networking Products**
- **Opinion: Heartbleed's Password Heartbreak**
- **Video: What the NSA Knew and When**

Heartbleed appears to be one of the biggest flaws in the Internet's history, affecting the basic security of as many as two-thirds of the world's websites. Its discovery and the creation of a fix by researchers five days ago prompted consumers to change their passwords, the Canadian government to suspend electronic tax filing and computer companies including **Cisco Systems Inc.** to Juniper Networks Inc. to provide patches for their systems.

- Acc… …160 at leas…
- Exp… …USA (htt… …eed-und…
- Bac… …s/bugs (inv…
- Mos… …A days befo…
- The… …he job (dyr…

NSA gets early access to zero-day data from Microsoft, others

Meant to help secure network, data could be used to attack foreign governments

by **Sean Gallagher** - June 14 2013, 6:55pm +0200

CYBERWAR PRIVACY WHITE HAT 82

The National Security Agency (NSA) has used sensitive data on network threats and other classified information as a carrot to gain unprecedented access to information from thousands of companies in technology, telecommunications, financial, and manufacturing companies, according to a report by Michael Riley of Bloomberg. And that data includes information on "zero-day" security threats from Microsoft and other software companies, according to anonymous sources familiar with the data-swapping program.

The NSA isn't alone in the business of swapping secrets with the corporate world. The FBI, CIA, and Department of Defense (DOD) also have programs enabling them to exchange sensitive government information with corporate "partners" in exchange for access to things like information on cyberattacks, traffic patterns, and other information that relate to network security.

NSA LEAKS

- Journalists who got Snowden docs arrive in US for first time in months
- NSA denies report that it knew about Heartbleed from the start [Updated]
- If President Obama wanted the NSA to quit storing phone metadata, he'd act now
- Google tells Supreme Court it's legal to packet sniff open Wi-Fi networks
- What, besides phone records, does the NSA collect in bulk?

View all...

The NSA's dual role as the security arbiter for many government networks and as point organization for the US government's offensive cyberwarfare capabilities means that the information it gains from these special relationships could be used to craft exploits to gain access to the computer systems and networks of foreign governments, businesses, and individuals. But it remains unclear just how much of a head start information about bugs actually gives NSA or whether companies actually delay posting fixes on the NSA's behalf.

Unlocking Windows

According to Bloomberg's sources, Microsoft provides information about security flaws and other bugs in its software in advance of public releases of fixes. The information provides the government an important early warning about potential attacks on systems, especially DOD networks. The military is Microsoft's single largest customer; systems on both its unclassified and secret networks (NIPRNET and SIPRNET) use Microsoft software. Microsoft has similar early-access programs for other customers, and it often deploys patches to large customers for testing prior to pushing them out on its monthly "Patch Tuesday" schedule.

Kraft/Corbis

NSA gets early access to zero-day data from Microsoft, others

Meant to help secure network, data could be used to attack foreign governments

Microsoft Bugs

In addition to private communications, information about equipment specifications and... **Read More**

Microsoft Corp. (MSFT), the world's largest software company, provides intelligence agencies with information about bugs in its popular software before it publicly releases a fix, according to two people familiar with the process. That information can be used to protect government computers and to access the computers of terrorists or military foes.

Redmond, Washington-based Microsoft and other software or Internet security companies have been aware that this type of early alert allowed the U.S. to exploit vulnerabilities in software sold to foreign governments, according to two U.S. officials. Microsoft doesn't ask and can't be told how the government uses such tip-offs, said the officials, who asked not to be identified because the matter is confidential.

Frank Shaw, a spokesman for Microsoft, said those releases occur in cooperation with multiple agencies and are designed to give government "an early start" on risk assessment and mitigation.

In an e-mailed statement, Shaw said there are "several programs" through which such information is passed to the government, and named two which are public, run by Microsoft and for defensive purposes.

Photographer: Scott Eells/Bloomberg

Microsoft Corp., the world's largest software

Microsoft's single largest customer, systems on both its unclassified and secret networks (NIPRNET and SIPRNET) use Microsoft software. Microsoft has similar early-access programs for other customers, and it often deploys patches to large customers for testing prior to pushing them out on its monthly "Patch Tuesday" schedule.

The GOOGLE vs ANSSI Case

- On Dec. 2013. Google accused ANSSI (French Agency for ICS Security) to perform a MitM attack against Google services (e.g. Google, Gmail…) by using a rogue X509 Certificate signed by the French CA O=IGC/A
- In fact, MINEFI (French Dept. of Treasure) was performing SSL Proxy forwarding to prevent leaks, malware attacks and to control traffic towards risky services (Gmail, Yahoo, Hotmail…) on its **private network only!**
  - MINEFI users were aware (internal security policy)

The GOOGLE vs ANSSI Case

A virtual server configured with Client and Server SSL profiles for SSL forward proxy functionality

1. Client establishes three-way handshake and SSL connection with wildcard IP address.
2. NA system establishes three-way handshake and SSL connection with server.
3. NA system validates a server certificate (Certificate A), while maintaining the separate connection with the client.
4. NA system creates different server certificate (Certificate B) and sends it to client.

- The error lies in the fact that MINEFI used IGC/A certificates to sign external domains
  - It was not a MitM attack
  - ANSSI's missions is devoted to Cyberdefense only

The GOOGLE vs ANSSI Case

- The problem was not ANSSI/MINEFI but Google:
  - How Google detected the internal use of ANSSI certificates?
  - The only web browser used is Firefox
    - not Chrome (strictly forbidden). So no PK pinning was possible
  - The only explanation is the existence of some hidden mechanism inside Firefox that transparently sends information about certificates to Google!
    - Covert channel-like mechanism causing a security breach (maybe through the safe browsing mechanism to sb.google.com/safebrowsing/update?version=goog-black-url:1:1) ?
    - Remind that Google has given millions of $ fund to the Mozilla foundation!
  - We have to take the greatest care of browsers in the future
- This issue sheds also a new light on CA authorities. Who is controlling them?

Are Vulnerabilities Really Necessary?

- The design of systems can enable the use of dynamic resources that can
  - transparently,
  - without any evidence/traces let into the system,
  - for a limited period of time

  be added to the system with preemptive rights
  - E.g. shim mechanism (refer our talk at PhDays 2014), ghost API added on-the-fly…
- Used in Cryptographic Dynamic Backdoors (my talk at CanSecWest 2011) among many other possibilities
- Everything occurs in memory only using legitimate Windows mechanisms only

Remarks

- You do not really need vulnerabilities when weak architecture design choices exist
- It is obvious that there is a strong will not to provide a high-level security with respect to cryptography mechanisms
- Any “vulnerability” can be seen as an intended backdoor
  - It is easier to invoke programmers’ deficiency that acknowledging to have put backdoors
  - Can be changed frequently (dynamic management, make forensics people always have a time delay)

SPYING NON-CONNECTED PEOPLE/NON-CLASSIC ENVIRONMENTS

Issues like mathematical trapdoors, TAO project and hardware bugs, sophisticated malware…

The Issue

- How to target environments which are never connected to networks or non-classical environments (telex, fax, highly secure LAN, embedded crypto [ASICS]…)?
  - Either you need a physical access (Peter Wright, 1987)
  - Or you need to have mathematical and/or hardware backdoors in those systems (especially for offline encryption)
  - Or use exotic approaches (Tempest, tempest-like techniques with malware, electronic warfare techniques…)
- Tailored Access Operations (TAO), NSA Ant catalog
- Refer to Appelbaum's 30C3 talk [5]

What is possible ?

- What Snowden did not reveal about (yet)?
  - Tempest like techniques. Former Soviet Union was the leading country for years and very likely still is
  - Use of very dynamic sophisticated malware
    - My talk at Black USA 2008 (using covert channels)
    - My talk at CanSecWest 2011 (dynamic cryptographic backdoors)
  - Low-level hardware trapdoors (e.g. processors, dynamic microcode malicious updates…)
  - Mathematical trapdoors (encryption algorithms may be put into question after the dual_EC_RDBG case with respect to standardization entities)

The Reality

Except in very special cases and specifically protected environments, there is no such things as totally disconnected systems, or totally isolated systems

Any physical access to a system enables to corrupt it in a few seconds

« Physical access » includes material world AND the etheric world (e.g. EM emanations)

The Reality

TOP SECRET//COMINT-GAMMA//ORCON/NOFORN

National Security Agency

Global SIGINT Highlights

Executive Edition

TUESDAY, 22 MAY 2012 — INFORMATION AS OF 0200Z

(U//FOUO) THE INFORMATION IN THIS REPORT IS PROVIDED FOR INTELLIGENCE PURPOSES ONLY BUT MAY BE USED TO DEVELOP POTENTIAL INVESTIGATIVE LEADS. NO INFORMATION CONTAINED IN THIS REPORT, NOR ANY INFORMATION DERIVED THEREFROM, MAY BE USED IN ANY PROCEEDING (WHETHER CRIMINAL OR CIVIL), TO INCLUDE ANY TRIAL, HEARING, OR OTHER PROCEEDING BEFORE ANY COURT, DEPARTMENT, AGENCY, REGULATORY BODY, OR OTHER AUTHORITY OF THE UNITED STATES WITHOUT THE ADVANCE APPROVAL OF THE ATTORNEY GENERAL AND/OR THE AGENCY OR DEPARTMENT WHICH ORIGINATED THE INFORMATION CONTAINED IN THIS REPORT. ANY REPRODUCTION, DISSEMINATION, OR COMMUNICATION (INCLUDING, BUT NOT LIMITED TO, ORAL BRIEFINGS) OF THIS INFORMATION MUST BE ACCOMPANIED BY A STATEMENT OF THESE RESTRICTIONS.

French President Approves Secret Eurozone Consultations, Meeting With German Opposition

(TS//SI-G//OC/NF)

(TS//SI-G//OC/NF) French President Francois Hollande has approved holding secret meetings in Paris to discuss the eurozone crisis, particularly the consequences of a Greek exit from the eurozone. On 18 May, Hollande directed Prime Minister (PM) Jean-Marc Ayrault to set up a meeting at the Office of the President (the Elysee) for the following week. Hollande, Ayrault, and "appropriate ministers" would attend, and special emphasis would be given to consequences for the French economy in general and for French banks in particular. Hollande stressed that the meeting would be secret. (**COMMENT:** The French president seems worried that if word were to get out that Paris is seriously considering the possibility of a Greek exit, it would deepen the crisis.) In addition, secret meetings are to be held in Paris between French officials and members of the German Social Democratic Party (SPD). Hollande assured the PM that hosting the meeting at the Elysee was "doable," although Ayrault warned the president to keep the event a secret so as to avoid diplomatic problems. (**COMMENT:** By "diplomatic problems," Ayrault is referring to what could happen if German Chancellor Angela Merkel finds out that Hollande is going behind her back to meet with the German opposition.) Earlier reporting reveals that following talks last week in Berlin with Merkel, Hollande complained that nothing of substance was achieved; it was purely for show. Hollande had found the chancellor fixated on the Fiscal Pact and above all on Greece, on which he claimed she had given up and was unwilling to budge. This made Hollande very worried for Greece and the Greek people, who might react by voting for an extremist party. After meeting Merkel, the French president contacted SPD Chairman Sigmar Gabriel and invited him to Paris so that they could talk.

Foreign Satellite, Unconventional French, German governmental Z-G/OO/503643-12, 211549Z; Z-G/OO/503541-12, 161711Z

Methods

For most of the five initial, and for all five additional reports, NSA's source of the intercepted communications is "**Unconventional**". It's not clear what that means, but phone calls between the president and his ministers will in most cases be handled by a local switch and therefore don't go through the intercontinental submarine fiber-optic cables, where they could pass NSA's conventional filter systems for telephone and internet traffic.

For intercepting this kind of foreign government phone calls, NSA would have to have access to the public telephone exchange(s) of Paris or the private branch exchanges (PBX) of the presidential palace and important government departments.

This would indeed require unconventional methods, like those conducted by the joint NSA-CIA units of the Special Collection Service (SCS) who operate from US embassies, or NSA's hacking division TAO.

Update:
According to a book by James Bamford, NSA had an Office of Unconventional Programs in the late 1990s, which in another book was presented as NSA's own equivalent of the SCS units. It is not known whether this office still exists or has evolved into another division.
A 2010 presentation (.pdf) says that RAMPART-A is "NSA's unconventional special access program". This is about cable tapping in cooperation with Third Party partner agencies, but seems not the means to get access to local government phone calls.

CONCLUSION

What will be the future ? How to resist?

Conclusion: Forensics

- Cryptography will no longer be the unique solution
  - When you encrypt you send noise! Then you are visible!
- Criminals will probably use steganography especially for network communications in the very near future
  - Unsuspected contents cannot be targeted!
  - For investigators, no longer evidence available

Conclusion: The Future

- Justice must adapt the penal procedure code
  - Investigators must have at least the same power and tools as criminals
- The control over cryptology is necessary but it cannot remain a matter of strategic hegemony
  - Must be respectful of citizens' freedom and privacy
  - Control the controllers!
- The solution could be to switch from hegemony to interdependency between democratic countries
  - Develop your own standards
  - Cooperate and share information

THANKS FOR YOUR ATTENTION!

आपका ध्यान के लिए धन्यवाद

നിങ്ങൾ ശ്രദ്ധയ്ക്ക് നന്ദി