

KU LEUVEN

Post-Snowden Cryptography (New Threat Models)

Bart Preneel
imec-COSIC KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
March 2017

© KU Leuven COSIC, Bart Preneel

1

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Going after crypto
- Impact on systems research and policy

2

National Security Agency

cryptologic intelligence agency of the USA DoD

- collection and analysis of foreign communications and foreign signals intelligence
- protecting government communications and information systems



THE PUZZLE PALACE

3

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...



TS//SI//REL to USA, FVEY

4

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) ...that this would be big brother...



TS//SI//REL to USA, FVEY

5

NSA calls the iPhone users public 'zombies' who pay for their own surveillance

TS//SI//REL to USA, FVEY


(S//REL) iPhone Location Services

(U) ...and the zombies would be paying customers?



TS//SI//REL to USA, FVEY

6




NSA:
"Collect it all,
know it all,
exploit it all"

www.wired.com

7

Snowden revelations



most capabilities could have been extrapolated from open sources

But still...

massive scale and impact (pervasive)

level of sophistication both organizational and technical


- redundancy: at least 3 methods to get to Google's data
- many other countries collaborated (beyond five eyes)
- industry collaboration through bribery, security letters*, ...
 - including industrial espionage

undermining cryptographic standards with backdoors (Bullrun) ... and also the credibility of NIST

* Impact of security letters reduced by Freedom Act (2 June 2015)

8

Snowden revelations (2)



Most spectacular: **active defense**

- networks
 - Quantum insertion: answer before the legitimate website
 - inject malware in devices
- devices
 - malware based on backdoors and 0-days (FoxAcid)
 - supply chain subversion


Translation in human terms: **complete control** of networks and systems, including bridging the air gaps

No longer deniable
Oversight weak

9

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

QUANTUMTHEORY

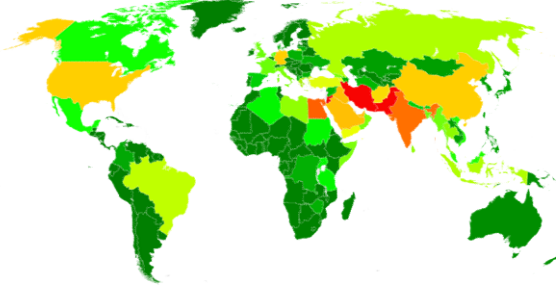



- (TS//SI//REL) Extremely powerful CNE/CND/CNA network effects are enabled by integrating our passive and active systems:
 - Resetting connections (QUANTUMSKY)
 - Redirecting targets for exploitation (QUANTUMINSERT)
 - Taking control of IRC bots (QUANTUMBOT)
 - Corrupting file uploads/downloads (QUANTUMCOPPER)
- (TS//SI//REL) QUANTUMTHEORY dynamically injects packets into a target's network session to achieve CNE/CND/CNA network effects.
 - **Detect:** TURMOIL passive sensors detect target traffic & tip TURBINE command/control.
 - **Decide:** TURBINE mission logic constructs response & forwards to TAO node.
 - **Inject:** TAO node injects response onto Internet towards target.
- (TS//SI//REL) The propagation delay from tip-to-target determines the success rate of the network effect. **Less Latency = More Success!**

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

10

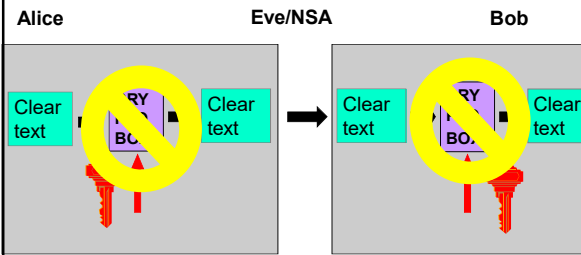
NSA surveillance by country

11

Rule #1 of cryptanalysis: search for plaintext [B. Morris]

Alice Eve/NSA Bob



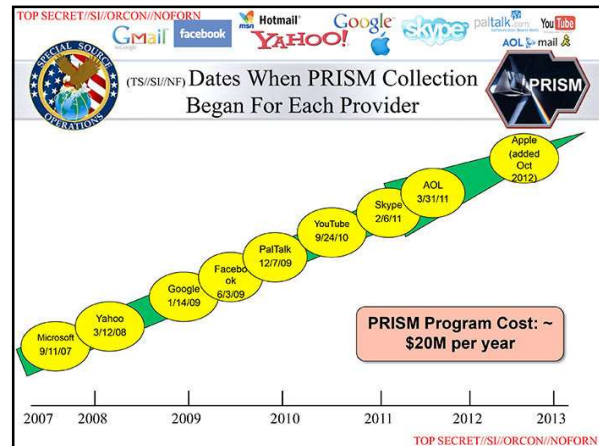
12

Where do you find plaintext? SSO: Special Source Operations

1. PRISM (server) 2. Upstream (fiber)

Tempora

13



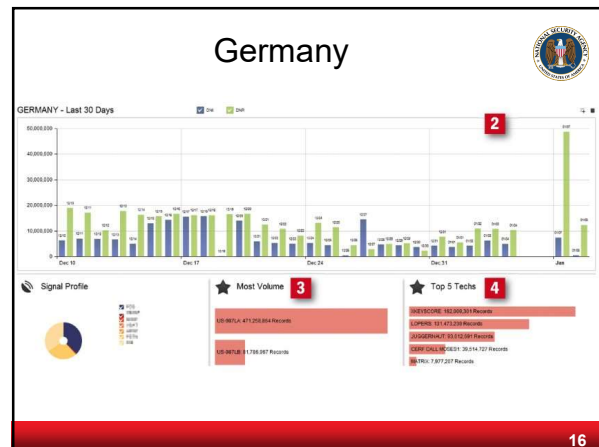
TOP SECRET//SI//NOFORN

Current Efforts - Google

Muscular (GCHQ) help from Level 3 (LITTLE)

Jan 9 2013: In the preceding 30 days, field collectors had processed and sent back 181,280,466 new records — including “metadata,” which would indicate who sent or received e-mails and when, as well as content such as text, audio and video (from Yahoo! and Google)

15



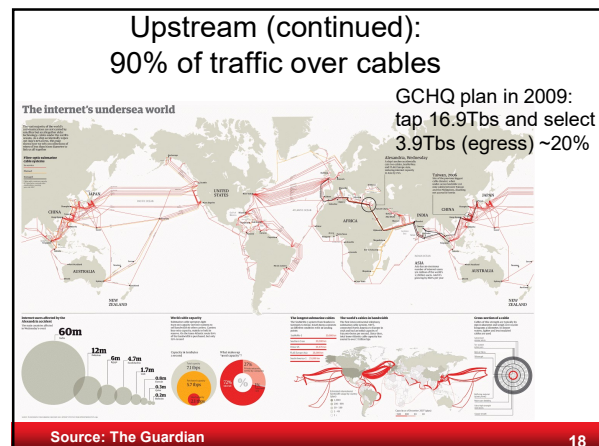
Recording all phone calls in the Bahamas and country X metadata in Mexico, Kenya, the Philippines

https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

MYSTIC

Illustration by Josh Begley

17



NSA has solved Skype messaging problem

May 2011: Microsoft buys Skype for B\$ 8.5
Feb. 2011: Skype-in and Skype-out interception (FISC court)
Jun. 2011: Skype peer to peer interception

TOP SECRET//COMINT//NOFORN

(TS//SI//NF) User's Guide For PRISM Skype Collection

h. Why do I receive multiple copies of Skype chat sessions?

h.i. You might get chats in segments and then get the whole chat in a third collect. This is how Skype works. Depending upon what your target is doing, a copy of his chat history can be sent in-bulk (which can span multiple chat sessions). If you target, for example, has 3 separate chat sessions with another individual on his laptop, then logs-into his Skype account on his desktop, the chat-history of those 3 separate chat sessions will be transmitted from this laptop to his desktop so that both his computers have a log of the whole conversation.

3. Traffic data (meta data) (DNR)

- traffic data is not plaintext itself, but it is very informative
 - it may contain URLs of websites
 - it allows to map networks
 - location information reveals social relations

6 June 2013: NSA collecting phone records of millions of Verizon customers daily

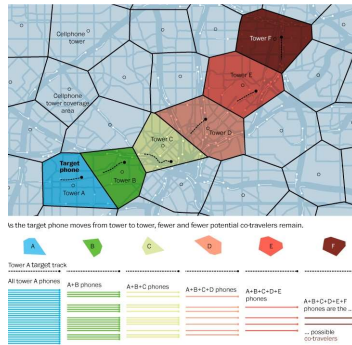
EU: data retention directive (2006/24/EC)

- declared illegal by EU Court of Justice in April 2014: disproportionate and contrary to some fundamental rights protected by the Charter of Fundamental Rights, in particular to the principle of privacy

<http://radiobruelleslibera.wordpress.com/2014/04/08/the-annulment-of-the-data-retention-directive-and-the-messy-consequences-on-national-legislations/>

3. Traffic data (DNR) – phone location

- NSA collects about 5B records a day on cell phone location
- Co-traveler



3. The meta data debate



It's *only* meta data



We kill people based on meta data



... but that's not what we do with *this* metadata

Former National Security Agency (NSA) and Central Intelligence Agency (CIA) Director Michael Hayden (Reuters/Larry Downing)

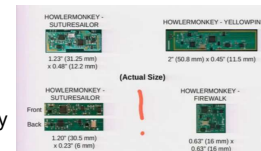
4. Client systems

- hack the client devices
 - use unpatched weaknesses (disclosed by vendors or by update mechanism?)
 - sophisticated malware
- get plaintext
 - webcam pictures of users
 - mobile phones: turned into remote microphones or steal keys from SIM cards (Gemalto)

4. Client systems: Quantum and TAO

TAO: Tailored Access Operations


- many technologies
- large number on bridging air gaps
- number of targets is limited by cost/effort



Examples:

- use radio interfaces and radar activation
- supply chain interception
- **FOXACID**: A system for installing spyware with a "quantum insert" that infects spyware at the packet level

(U) Capabilities
(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that empirically, this provides the best video return and cleanest readout of the monitor contents.



(U) Concept of Operation
(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

25

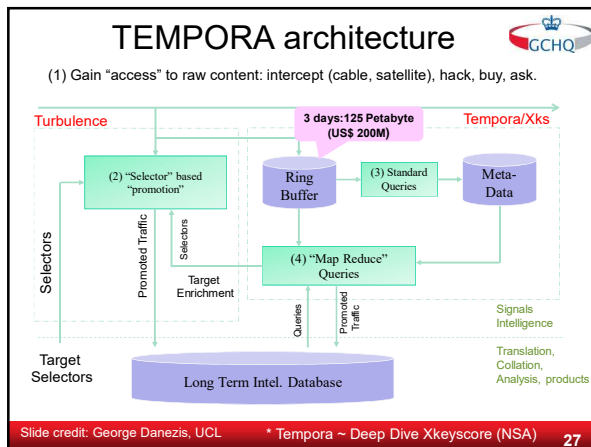
...and more

Spying on




Fourth order spying (hack South Korea implant to spy on North Korea) ...and even fifth order [01/15]
 BND helps NSA spying on EU politicians and companies [04/15]
 Hacking anti-virus companies [06/15]
 GCHQ spying on human rights groups [06/15]

26

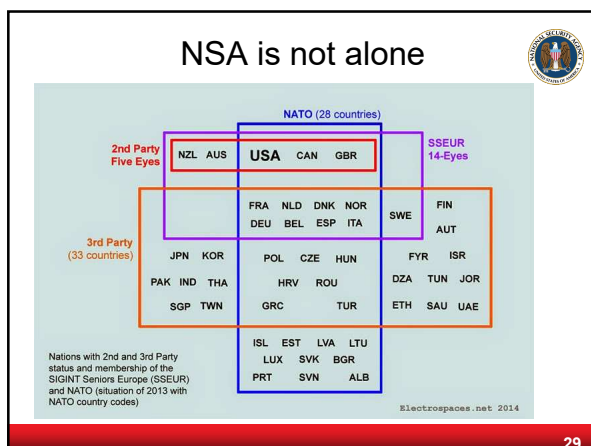


Which questions can one answer with these systems?



- I have one phone number – find all the devices of this person, his surfing behavior, the location where he has travelled to and his closest collaborators
- Find all Microsoft Excel sheets containing MAC addresses in Belgium
- Find all exploitable machines in Panama
- Find everyone in France who communicates in German and who uses Signal


28



Surveillance spillout





لا إله إلا الله
محمد رسول الله




If data is the new oil, data mining yields the rocket fuel

industry



users




government

31

Mass Surveillance

panopticon
[Jeremy Bentham, 1791]

discrimination
fear
conformism - stifles dissent
oppression and abuse



32

Lessons learned

Economy of scale

Never underestimate a motivated, well-funded and competent attacker

Pervasive surveillance requires pervasive collection and **active attacks** (also on **innocent** bystanders)

Active attacks undermines integrity of and trust in computing infrastructure

Emphasis moving from COMSEC to COMPUSEC (from network security to systems security)

Need for combination of industrial policy and non-proliferation treaties


33

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Going after crypto
- Impact on systems research and policy

34

NSA foils much internet encryption



NYT 6 September 2013

The National Security Agency is winning its long-running secret war on **encryption**, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age

[Bullrun]

35

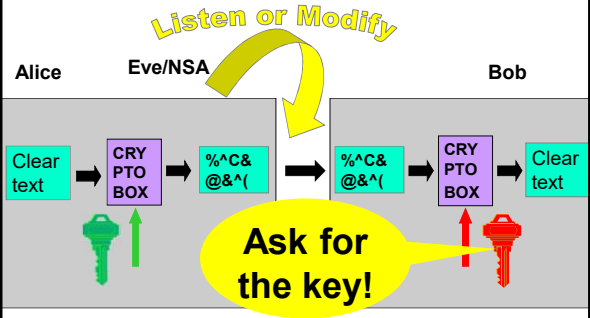
If you can't get the plaintext

Listen or Modify

Alice

Eve/NSA

Bob



Clear text → CRY PTO BOX → %^C& @&^(→ %^C& @&^(→ CRY PTO BOX → Clear text

Ask for the key!

36

Asking for the key

- national security letters?
 - exist since the 1980s
 - come with gag orders; a handful revealed
 - 300.000 issued since 2001
- Lavabit email encryption
- Yahoo <https://www.wired.com/2016/06/yahoo-publishes-national-security-letters-fbi-drops-gag-orders/>
- Silent Circle email?
- CryptoSeal Privacy VPN
- SSL/TLS servers of large companies?
- Truecrypt??

37

TLS and forward secrecy

Hack the server or ask for it with a security letter
Solution: replace RSA by Diffie-Hellman (D-H) for perfect forward secrecy

- long term private key is only used for signing
- ephemeral D-H keys for confidentiality

D-H downgrade attack [Adrian+15, CCS]

- downgrade to 512-bit export control (legacy)
- cryptanalyze ephemeral D-H keys in real time
- even 1024-bit keys (widely used default option) not strong enough

Same attack applies to large fraction of IPsec servers

[Adrian+] Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, CCS 2015

38

SSL/TLS keys: GCHQ Flying Pig

39

If you can't get the private key, substitute the public key

12M SSL/TLS servers
fake SSL certificates or SSL person-in-the-middle as commercial product or government attack

- 650 CA certs trustable by common systems
- Comodo, Diginotar, Turktrust, ANSSI, China Internet Network Information Center (CNNIC), Symantec
- Flame: rogue certificate by cryptanalysis

[Holz+] TLS in the Wild, NDSS 2016
[Stevens] Counter-cryptanalysis, Crypto'13

40

If you can't get the key

make sure that the key is generated using a random number generator with trapdoor

trapdoor allows to predict keys

41

Dual_EC_DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- ANSI and ISO standard
- 1 of the 4 PRNGs in NIST SP 800-90A
 - draft Dec. 2005; published 2006; revised 2012
- Two "suspicious" parameters P and Q
- Many warnings and critical comments
 - before publication [Gjosteen05], [Schoenmakers-Sidorenko06]
 - after publication [Ferguson-Shumov07]

Appendix: The security of Dual_EC_DRBG requires that the points P and Q be properly generated. To avoid using potentially weak points, the points specified in Appendix A.1 should be used.

42

Dual_EC_DRBG

- 10 Sept. 2013, NYT: "internal memos leaked by a former NSA contractor suggest that [...] the Dual EC DRBG standard [...] contains a **backdoor** for the NSA."
- 9 Sept. 2013: NIST "**strongly recommends**" against the use of Dual_EC_DRBG, as specified in SP 800-90A (2012)

Why was the slowest and least secure of the 4 PRNGs chosen as the default algorithm in BSAFE?

43

Dual_EC_DRBG: state recovery

S_0 = secret seed
 S_i = secret state
 P and Q : curve points
 $Q = d \cdot P$
 $Xco()$ = X-coordinate
 $trunc()$: drop 2 bytes

44

Dual_EC_DRBG: state recovery

S_0 = secret seed
 S_i = secret state
 P and Q : curve points
 $Q = d \cdot P$
 $Xco()$ = X-coordinate
 $trunc()$: drop 2 bytes

Depending on library: key recovery in a few seconds or a few hours

On the Practical Exploitability of Dual EC in TLS Implementations
S. Checkoway, M. Fredrikson, T. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D.J. Bernstein, J. Maskiewicz, H. Shacham, Usenix Security 2014

45

Dual_EC_DRBG in Juniper

Juniper Security Advisory (17/12/2015), CVE-2015-7755/7756
ScreenOS 6.2.r015-r018 and 6.3.r017-r020
"discovered unauthorized code in the ScreenOS software that powers Netscreen firewalls"

Two backdoors

- bypass authentication in the SSH and Telnet daemons
- passive eavesdropper can decrypt VPN traffic

(1) Was inserted on 25 April 2014, 6.3.r017
password was discovered within 6 hours after release of CVE

```
<<< %s(un='%s') = %u
```

46

Dual_EC_DRBG in Juniper (2)

(2) Passive eavesdropper can decrypt VPN traffic

From the Juniper knowledge base (Oct 2013)

ScreenOS does make use of the Dual_EC_DRBG standard, but is designed to not use Dual_EC_DRBG as its primary random number generator. ScreenOS uses it in a way that should not be vulnerable to the possible issue that has been brought to light. Instead of using the NIST recommended curve points it uses self-generated basis points and then takes the output as an input to FIPS/ANSI X.9.31 PRNG, which is the random number generator used in ScreenOS cryptographic operations.

47

Dual_EC_DRBG in Juniper (3)

(2) Passive eavesdropper can decrypt VPN traffic

Changes introduced on 20 October 2008 (6.2.r01)

- Add **Dual_EC_DRBG** but with a different **Q**
- Add **global** variables to RNG code
- Output is supposed to be input to a second RNG based on ANSI X9.31, but due to a subtle bug a "for loop" is never executed and there is no post-processing with ANSI X9.31
- RNG produces **32 bytes** rather than 20
- Nonce** for IKE (IPsec) is increased from 20 to 32 bytes
- Nonces are **pre-generated**

48

Dual_EC_DRBG in Juniper (4)

(2) Passive eavesdropper can decrypt VPN traffic

Changes introduced on 12 September 2012 (6.2.r015)

- Q point in Dual_EC_DRBG code is replaced by another point Q'
- Juniper calls this as an "unauthorized patch"

17 December 2015: Juniper patch

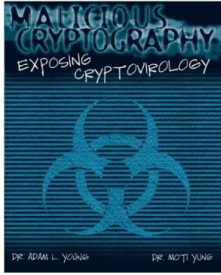
- Remove SSH/Telnet backdoor
- Restore Q

That's it folks

49

Cryptovirology [Young-Yung]

<http://www.cryptovirology.com/cryptovfiles/research.html>



Title: Malicious Cryptography – Exposing Cryptovirology

Authors: Adam Young
Moti Yung

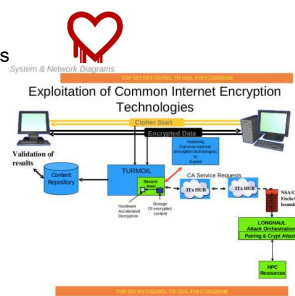
Date: February, 2004

Publisher: John Wiley & Sons

50

NSA can (sometimes) break SSL/TLS, IPsec, SSH, PPTP, Skype

- ask for private keys
- implementation weaknesses
- weak premaster secret (IPsec)
- end 2011: decrypt 20,000 secure VPN connections/hour



<http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html>

<http://blog.cryptographyengineering.com/2014/12/on-new-snowden-documents.html>

51

Fighting cryptography

- Weak implementations
- Going after keys
- Undermining standards
- Cryptanalysis

- Increase complexity of standards
- Export controls
- Hardware backdoors
- Work with law enforcement to promote backdoor access and data retention

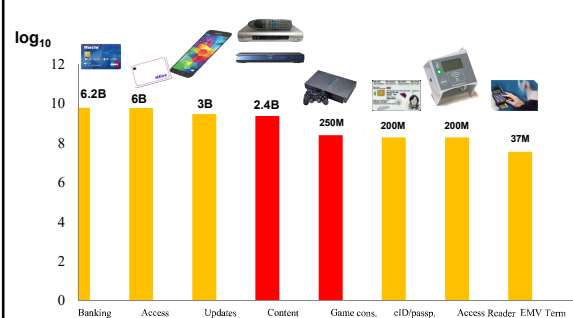
52

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Going after crypto
- Impact on systems research and policy

53

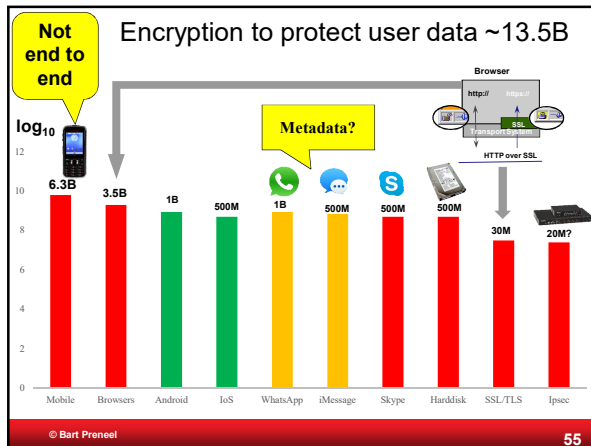
Encryption to protect industry ~18.3B



Category	Value
Banking	6.2B
Access	6B
Updates	3B
Content	2.4B
Game cons.	250M
eID/passp.	200M
Access Reader	200M
EMV Term	37M

© Bart Preneel

54



- ### Deployment of cryptography
- most crypto in volume and market serves for data and entity authentication
 - code updates
 - payments: credit/debit/ATM/POS and SSL/TLS
 - confidentiality
 - government/military secrets
 - DRM/content protection
 - ehealth (growing market)
 - telco: not end-to-end or with a backdoor
 - hard disk encryption: backdoored?
 - most data in the cloud is not encrypted
- 56

Cryptography that seems to work

```

Active User [redacted]
Active User IP Address [redacted]
Target User [redacted]
Target User IP Address [redacted]
Start Mar 16, 2012 13:38:35 GMT
Stop Mar 16, 2012 13:39:53 GMT

Other User IP Addresses
[redacted]

Time (GMT) From To Message
Mar 16, 2012 13:37:51 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:37:59 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:08 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:12 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:24 [redacted] [OC: No decrypt available for this OTR encrypted message.]
    
```

Snowden did not have access to cryptanalytic know-how and documents of NSA (only SIGINT)

57

- ### Cryptography that seems to work
- difficulty decrypting certain types of traffic, including
- Truecrypt
 - PGP/GPG
 - Tor* ("Tor stinks")
 - ZRTP from implementations such as RedPhone
- commonalities
- RSA (≥ 2048), Diffie-Hellman (≥ 2048), ECDH and AES
 - open source
 - end-to-end
 - limited user base
- * some Tor traffic can be deanonymized
- 58

Policy debate

Should we fight this at the technical level?
Or should we argue about liberty, agency, chilling effects and self-censorship, government abuse

59

- ### COMSEC - Communication Security
- Protecting data in transit: (authenticated) encryption**
- effective when done right (encryption works)
 - ok (but complex) standards: TLS, IPsec, S/MIME
 - weak legacy systems: GSM, Bluetooth
 - not end-to-end: WLAN, 3G
 - lack of transparency: Skype
 - weak implementations: Dual EC DRBG
 - weak governance and key management: DigiNotar
 - insecure routing and domain name services
 - backdoors likely
- Limited fraction (a few %) of traffic is protected.
A very small fraction of traffic is protected end-to-end with a high security level
- 60

COMSEC - Communication Security

Secure channels

- authenticated encryption studied in CAESAR
<http://competitions.cr.yp.to/caesar.html>


Forward secrecy: Diffie-Hellman versus RSA

Denial of service

Simplify internet protocols with security by default:
DNS, BGP, TCP, IP, http, SMTP,...

61

COMSEC - Communication Security meta data



Hiding communicating identities

- few solutions – need more
- largest one is TOR with a few million users
- well managed but known limitations
 - e.g. security limited if user and destination are in same country

Location privacy: problematic

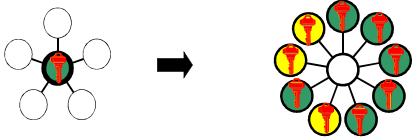
62

COMSEC - Communication Security

Do **not** move problems to a single secret key

- example: Lavabit email
- solution: threshold cryptography; proactive cryptography


Do **not** move problems to the authenticity of a single public key




63

COMPUSEC - Computer Security

Complex ecosystem developed over 40 years by thousands of people that has many weaknesses

- **Errors** at all levels leading to attacks (think )
 - governments have privileged access to those weaknesses
- Continuous remote **update** needed (implies weakness)
- Current **defense technologies** (firewall, anti-virus) not very strong with single point of failure
- Not designed to resist **human factor** attacks: coercion, bribery, blackmail
- **Supply chain** of software and hardware vulnerable and hard to defend (backdoors or implants)



64

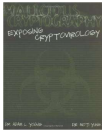

COMPUSEC - Computer Security

Protecting data at rest

- well established solutions for local encryption: Bitlocker, Truecrypt
- infrequently used in cloud
 - Achilles heel is key management
 - Territoriality
- what if computations are needed?

65

Reconsider every stage

Crypto design	Kleptography	
Hardware/software design	Hardware backdoors	
Hardware production	Software backdoors	
Firmware/sw impl.	Adding/modifying hardware backdoors	
Device assembly	Configuration errors	
Device shipping	Backdoor insertion	
Device configuration		
Device update		

66

Architecture is politics [Mitch Kaipor'93]

Control:

avoid single point of
trust that becomes
single point of **failure**



Stop massive data collection

big data yields big breaches (think pollution)
this is both a privacy and a security problem (think OPM)

67

Governance and Architectures

Back to principles: minimum disclosure

- stop collecting massive amounts of data
 - local secure computation
- if we do collect data: encrypt with key outside control of host
 - with crypto still useful operations

Bring "cryptomagic" to use without overselling

- zero-knowledge, oblivious transfer, functional encryption
- road pricing, smart metering, health care

68

Distributed solutions work

Root keys of some
CAs



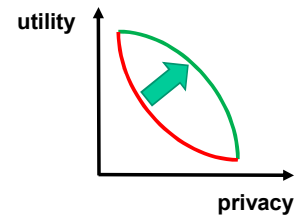
Skype (pre -2011)

Cryptocurrencies



69

Pushing the tradeoffs



70

From Big Data to Small Local Data



Data stays with
users

71

Distributed systems with local data

Many services can be provided based on local information
processing

- advertising
- proximity testing
- set intersection
- road pricing and insurance pricing

Cryptographic building blocks: ZK, OT, PIR, MPC, (s)FHE

Almost no deployment:

- massive data collection allows for other uses and more control
- fraud detection may be harder
- lack of understanding and tools

72

From Big Data to (Small) Encrypted Data

Encrypted data

Can still compute on the data

Keys stay with users

73

Centralization for small data

- exceptional cases such as genomic analysis
 - pseudonyms
 - differential privacy
 - searching and processing of encrypted data
 - strong governance: access control, distributed logging

fascinating research topic but we should favor local data
not oversell cryptographic solutions

74

Open (Source) Solutions

Effective governance

Transparency for service providers

EU-FOSSA EU Free and Open Source Software Auditing

75

KISS Principle

Keep It Simple Stupid

76

Conclusions (research)

- Rethink architectures: distributed
- Shift from network security to system security
- Increase robustness against powerful opponents who can subvert many subsystems during several lifecycle stages
- Open technologies and review by open communities
- Keep improving cryptographic algorithms, secure channels and meta-data protection

77

Conclusions (policy)

- Pervasive surveillance needs **pervasive collection** and **active attacks** with massive collateral damage on our ICT infrastructure
- Back to targeted surveillance under the rule of law
 - avoid cyber-colonialism [Desmedt]
 - need industrial policy with innovative technology that can guarantee economic sovereignty
 - need to give law enforcement sufficient options

78

More information

Movies

- Citizen Four (a movie by Laura Poitras) (2014) <https://citizenfourfilm.com/>
- Edward Snowden - Terminal F (2015) <https://www.youtube.com/watch?v=Nd6qN167wKo>
- John Oliver interviews Edward Snowden https://www.youtube.com/watch?v=XEVlyP4_11M

Documents:

- <https://www.eff.org/nsa-spying/nsadocs>
- <https://cjfe.org/snowden>

Media

- <https://firstlook.org/theintercept/>
- http://www.spiegel.de/international/topic/nsa_spying_scandal/

Books

- Glenn Greenwald, No place to hide, Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014

Very short version of this presentation:

- <https://www.youtube.com/watch?v=uYk6yN9eNfc>

79

Thank You for Your Attention



Industrial policy



to protect sovereignty and human rights

80

Further reading

Books

Glenn Greenwald, No place to hide, Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014

Documents

<https://www.eff.org/nsa-spying/nsadocs>
<https://cjfe.org/snowden>

Articles

Philip Rogaway, The moral character of cryptographic work, Cryptology ePrint Archive, Report 2015/1162
Bart Preneel, Phillip Rogaway, Mark D. Ryan, Peter Y. A. Ryan: Privacy and security in an age of surveillance (Dagstuhl perspectives workshop 14401). Dagstuhl Manifestos, 5(1), pp. 25-37, 2015.

81

More information

Movies

Citizen Four (a movie by Laura Poitras) (2014) <https://citizenfourfilm.com/>
Edward Snowden - Terminal F (2015) <https://www.youtube.com/watch?v=Nd6qN167wKo>
John Oliver interviews Edward Snowden https://www.youtube.com/watch?v=XEVlyP4_11M
Snowden (a movie by Oliver Stone) (2016)
Zero Days (a documentary by Alex Gibney) (2016)

Media

<https://firstlook.org/theintercept/>
http://www.spiegel.de/international/topic/nsa_spying_scandal/
Very short version of this presentation:
<https://www.youtube.com/watch?v=uYk6yN9eNfc>

82