Mass Surveillance

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

June 2017

1

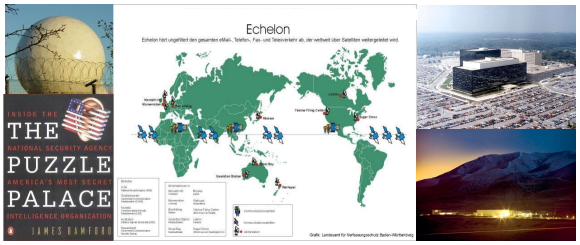
Outline

- 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



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

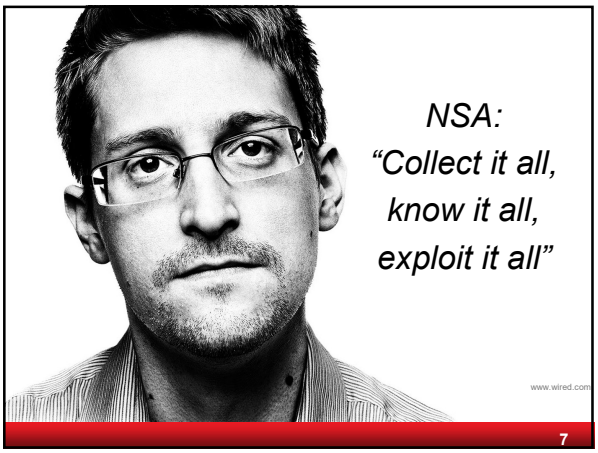
TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

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

TS//SI//REL to USA, FVEY

6



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**

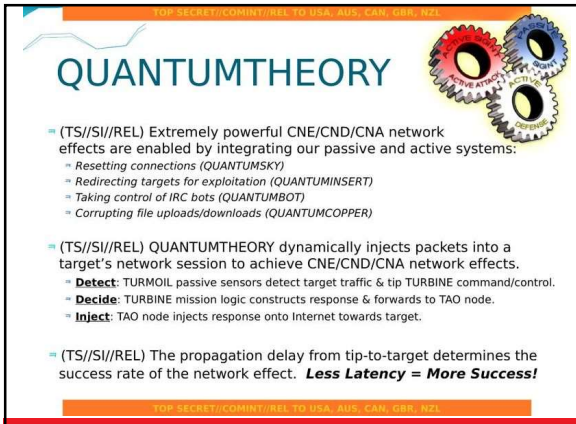
- networks
  - Quantum insertion: answer before the legitimate website
  - inject malware in devices
- devices
  - malware based on backdoors and 0-days (FoxAcid)
  - supply chain subversion

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

No longer deniable

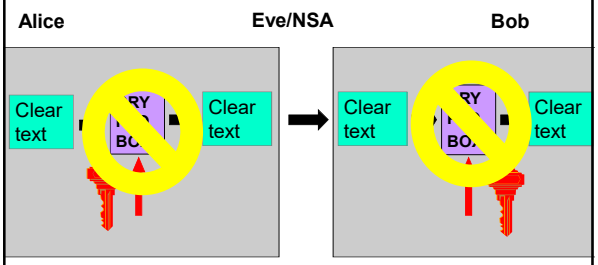
Oversight weak

9



10

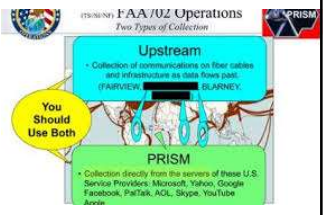
Rule #1 of cryptanalysis: search for plaintext [B. Morris]



11

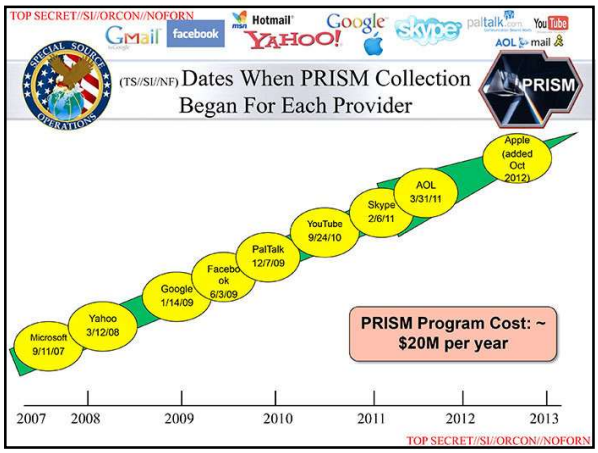
Where do you find plaintext? SSO: Special Source Operations

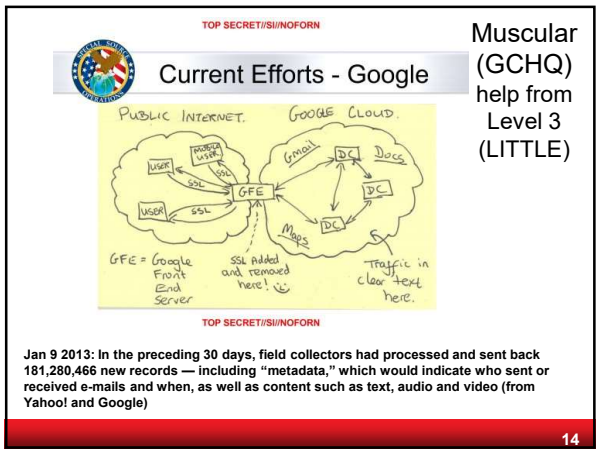
1. PRISM (server)
2. Upstream (fiber)



Tempora

12





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)

14

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

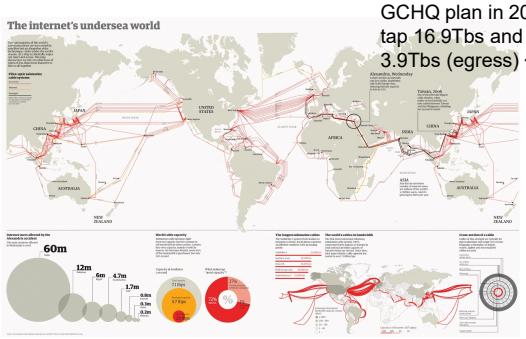
https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

Illustration by Josh Begley

15

Upstream (continued): 90% of traffic over cables

GCHQ plan in 2009: tap 16.9Tbs and select 3.9Tbs (egress) ~20%



Source: The Guardian

16

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)

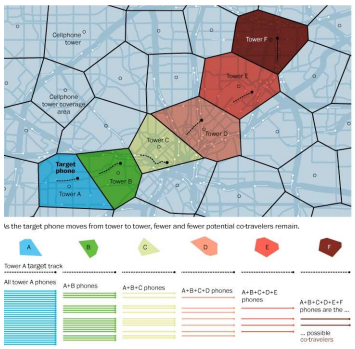
– declared illegal by EU Court of Justice in April 2014: disproportionate and contrary to some fundamental rights protected by the Charter of Fundamental Rights, in particular to the principle of privacy

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

18

3. Traffic data (DNR) – phone location

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



19

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)

20

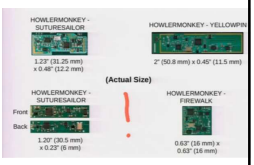
4. Client systems

- 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)

21

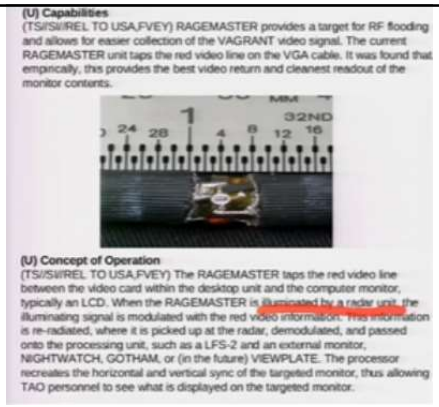
4. Client systems: Quantum and TAO

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

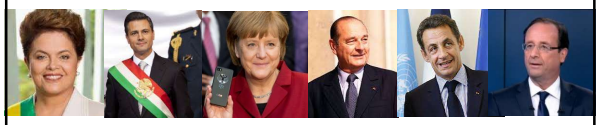
22



23

…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]

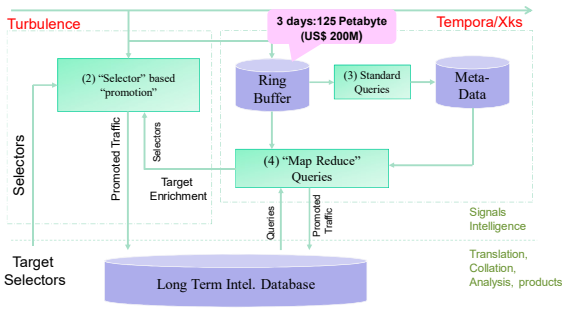
Hacking anti-virus companies [06/15]

GCHQ spying on human rights groups [06/15]

24

TEMPORA architecture

(1) Gain "access" to raw content: intercept (cable, satellite), hack, buy, ask.



Slide credit: George Danezis, UCL

* Tempora ~ Deep Dive Xkeyscore (NSA)

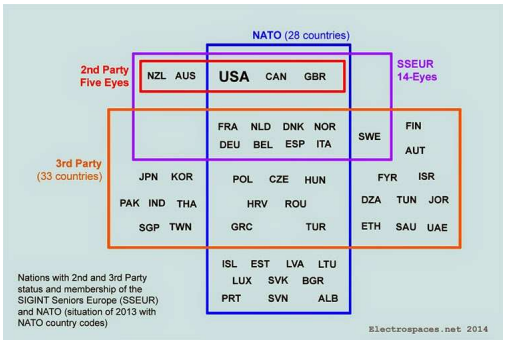
25

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

26

NSA is not alone

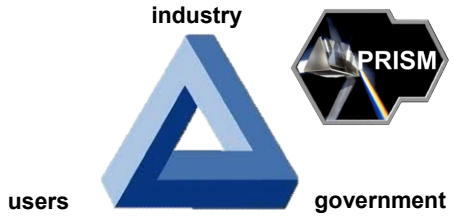


27

Surveillance spillout

29

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

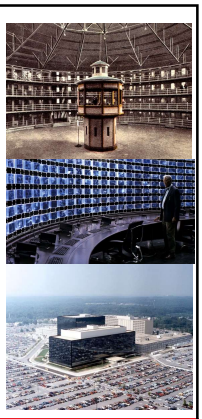


30

Mass Surveillance

panopticon
[Jeremy Bentham, 1791]

discrimination
fear
conformism - stifles dissent
oppression and abuse



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

31

Outline

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

32

NSA foils much internet encryption

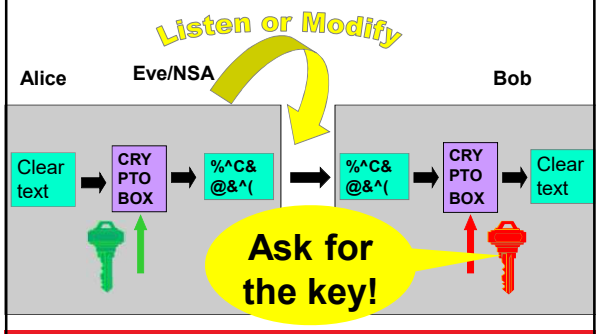
NYT 6 September 2013

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]

33

If you can't get the plaintext



34

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??

35

TLS and forward secrecy

Hack the server or ask for it with a security letter

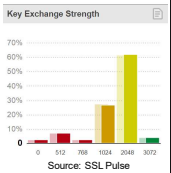
Solution: replace RSA by Diffie-Hellman (D-H) for perfect forward secrecy

- 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

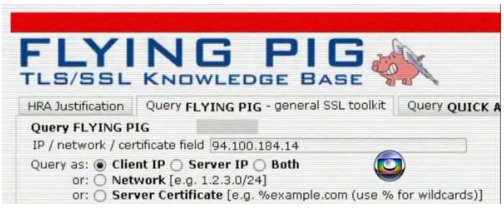
Same attack applies to large fraction of IPsec servers



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

36

SSL/TLS keys: GCHQ Flying Pig



37

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

Let's Encrypt live since November 2015
https://letsencrypt.org/isrg/

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

38

If you can't get the key

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

seed → **Pseudo-random number generator (PRNG)** → 

trapdoor allows to predict keys

39

Dual_EC_DRBG

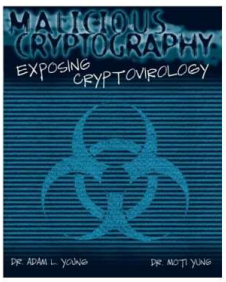
Dual Elliptic Curve Deterministic Random Bit Generator

- 1 of the 4 PRNGs in NIST SP 800-90A
  - draft Dec. 2005; published 2006; revised 2012
- Many warnings and critical comments
- Implemented by major players
- Deployed in Juniper ScreenOS 6.2.r015-r018 and 6.3.r017-r020
  - first not a threat but activated by combination of bugs
  - backdoor was replaced by someone

40

Cryptovirology [Young-Yung]

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



Title: Malicious Cryptography – Exposing Cryptovirology

Authors: Adam Young
Moti Yung

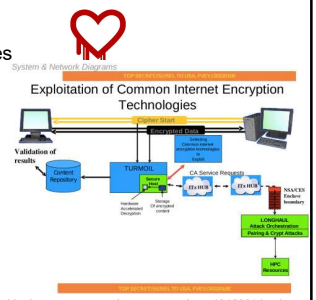
Date: February, 2004

Publisher: John Wiley & Sons

41

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

42

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

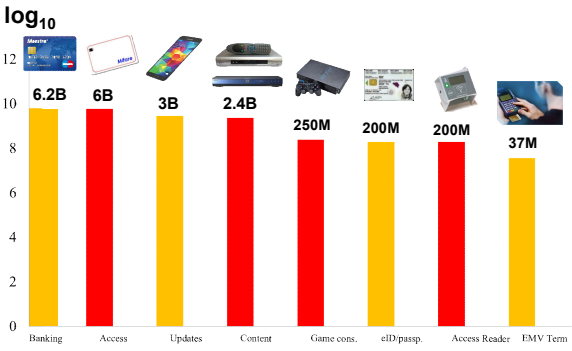
43

Outline

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

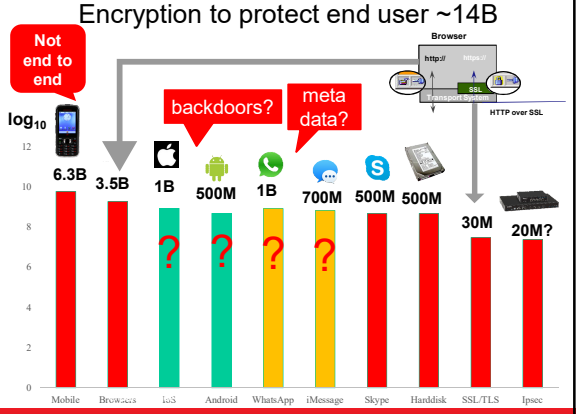
44

Encryption to protect industry ~18.3B



45

Encryption to protect end user ~14B



46

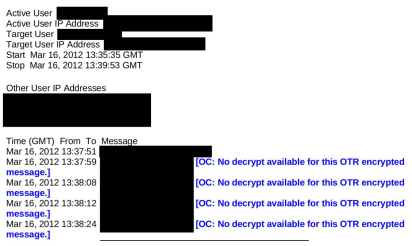
Deployment of cryptography

- 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

47

Cryptography that seems to work



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

48

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

49

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)

50

Governance and Architectures

Back to principles: minimum disclosure

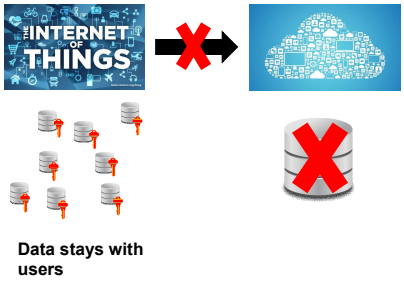
- stop collecting massive amounts of data
  - local secure computation
- if we do collect data: encrypt with key outside control of host
  - with crypto still useful operations

Bring "cryptomagic" to use without overselling

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

51

From Big Data to Small Local Data



Data stays with users

52

Distributed solutions work

Root keys of some CAs

Skype (pre -2011)

Cryptocurrencies

53

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

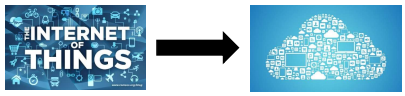
Cryptographic building blocks: ZK, OT, PIR, MPC, (s)FHE

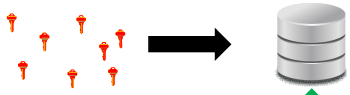
Almost no deployment:

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

54

From Big Data to Encrypted Data





Local encryption with low multiplication depth

Encrypted data
Can still compute on the data with somewhat Fully Homomorphic Encryption

55

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

56

Open (Source) Solutions

Effective governance

Transparency for service providers

EU-FOSSA EU Free and Open Source Software Auditing

57

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

58

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

59

Thank You for Your Attention

Industrial policy

to protect sovereignty and human rights

60

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.

61

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

62