Slide 1

KU LEUVEN

System Security after Snowden

Bart Preneel
COSIC KU Leuven and iMinds, Belgium
Bart.Preneel(at)esat.kuleuven.be
2 June 2015

iMinds
CONNECT.INNOVATE.CREATE

© KU Leuven COSIC, Bart Preneel

1

Slide 2

Outline

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

2

Slide 3

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

Slide 4

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...

TS//SI//REL to USA, FVEY

4

Slide 5

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

Slide 6

NSA calls the iPhone users public 'zombies' who pay for their own surveillance
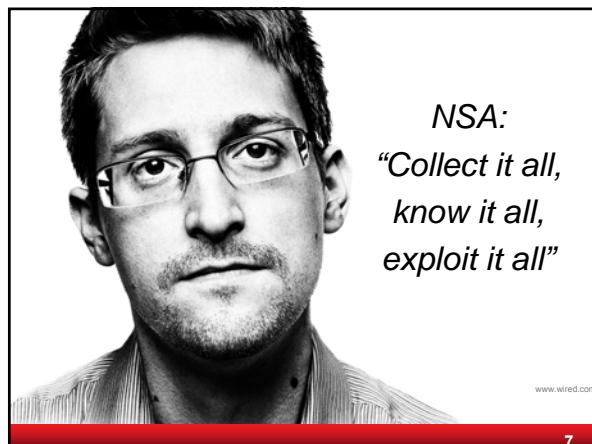
TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

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

TS//SI//REL to USA, FVEY

6

Slide 7

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

www.wired.com

Slide 8

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)

Slide 9

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
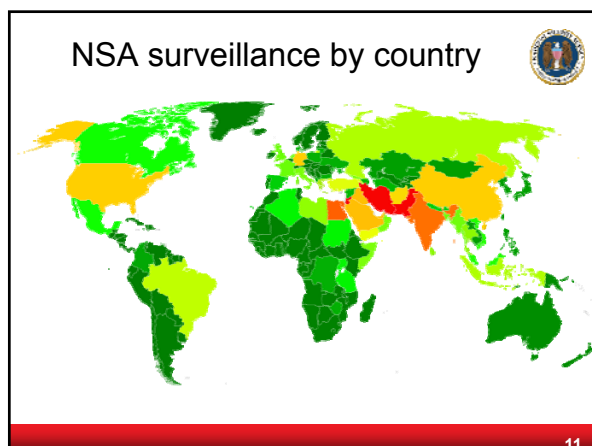
No longer deniable
Oversight weak

Slide 10

Slide 11

NSA surveillance by country

Slide 12

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

Alice   Eve/NSA   Bob

Clear text   Clear text   Clear text   Clear text

Where do you find plaintext?
SSO: Special Source Operations

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

Tempora

13

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year

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

Germany

16

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

17

Upstream (continued):
90% of traffic over cables

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

Source: The Guardian

18

3

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

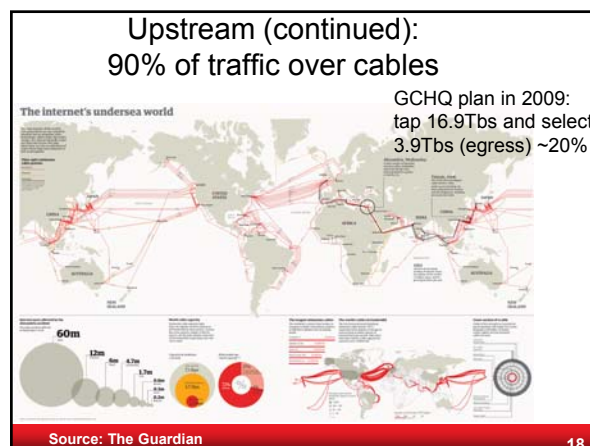**6 June 2013: NSA collecting phone records of millions of Verizon customers daily**

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/

19

3. Traffic data (DNR) – phone location

- NSA collects about 5B records a day on cell phone location
- Co-traveler
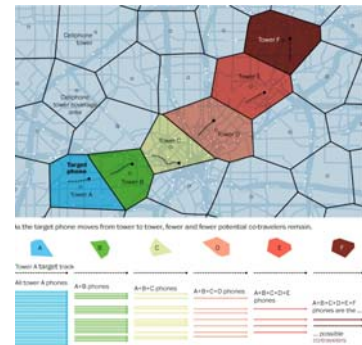
20

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)

21

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)

22

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

23

24

…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]

25

Another leaked document
https://search.edwardsnowden.com/

Roger Dingledine at NSA NOV 2007

Document Date: 2007-11-01   Release Date: 2013-10-04

This NSA memo summarises a talk given by Roger Dingledine of the Tor Project on 1 November 2007: see the Secret NSA documents show campaign against Tor encrypted network, 4 October 2013.

TOP SECRET // COMINT // REL TO USA, AUS, CAN, GBR, NZL Roger Dingledine at NSA NOV 2007 From PE Contents * 1 (U) Talk by Roger Dingledine at NSA, 11/01/2007 at R&E (Sponsored by NSA RT) o 1...

🏛 NSA   Encryption and Cryptanalysis

🌐 France (FRA/FR), Germany (DEU/DE), United States (USA/US)

◆ Top Secret   Brazil, United States, Nigeria, Netherlands, Seychelles

26

TEMPORA architecture

GCHQ

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

Slide credit: George Danezis, UCL   * Tempora ~ Deep Dive Xkeyscore (NSA)

27
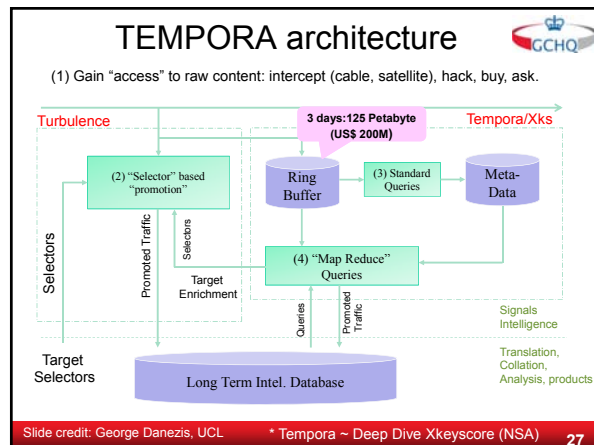
Which questions can one answer with these systems?

- 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 country X
- Find all exploitable machines in country X
- Find everyone in country X who communicates in German and who uses the encryption tool Z

28

Surveillance spillout

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

30

Outline

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

31

NSA foils much internet encryption

NYT 6 September 2013

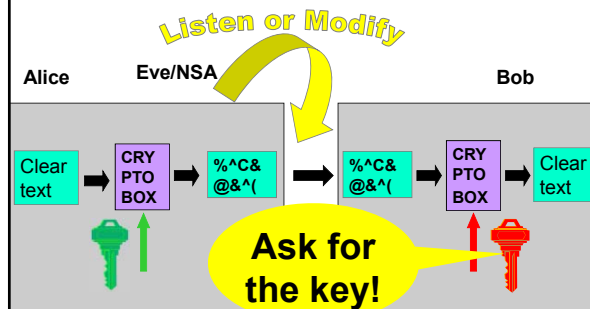The National Security Agency is winning its long-running secret war on **encryption**, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age

[Bullrun]

32

If you can't get the plaintext

Listen or Modify

Alice   **Eve/NSA**   **Bob**

Clear text → CRYPTO BOX → %^C& @&^(→ %^C& @&^(→ CRYPTO BOX → Clear text

Ask for the key!

33

Asking for the key

- (alleged) examples – through security letters?
  - Lavabit email encryption
  - CryptoSeal Privacy VPN
  - SSL/TLS servers of large companies
  - Truecrypt?

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

Ladar Levison, Owner and Operator, Lavabit LLC

34

Find the Private Key (Somehow)
[Adrian+15, Imperfect forward secrecy]

- Systems can be made to fall back to 512-bit export control legacy systems
- 1024-bit RSA and Diffie-Hellman widely used default option not strong enough

- GCHQ:

FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query FLYING PIG - general SSL toolkit | Query QUICK A
Query FLYING PIG
IP / network / certificate field 94.100.184.14
Query as: ● Client IP ○ Server IP ○ Both
or: ○ Network [e.g. 1.2.3.0/24]
or: ○ Server Certificate [e.g. %example.com (use % for wildcards)]

35

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

fake SSL certificates or SSL person-in-the-middle as commercial product or government attack

- Flame: rogue certificate by cryptanalysis
  - Stevens, Counter-cryptanalysis, Crypto 2013
- Comodo, Diginotar, Turktrust, ANSSI, China Internet Network Information Center (CNNIC)

Let's Encrypt will go life in September 2015
https://letsencrypt.org/isrg/

36

6

The CA Mess on the web
[Eckersley10] "An observatory for the SSLiverse"

10.8M servers start SSL handshake

4.3M use valid certificate chains

650 CA certs trustable by Windows or Firefox

several CAs sign the IP adr. 192.168.1.2 (reserved by RFC 1918)

2 leaf certs have 508-bit keys

Debian OpenSSL bug (2006-2008): keys not revoked

37

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)** ➡ 🔑
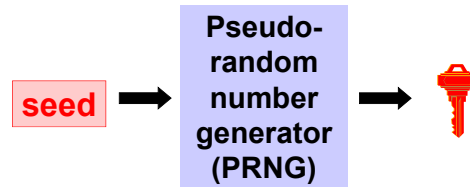
trapdoor allows to predict keys

38

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 [Gjøsteen05], [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.

39

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?

40

Cryptovirology [Young-Yung]

http://www.cryptovirology.com/cryptovfiles/research.html
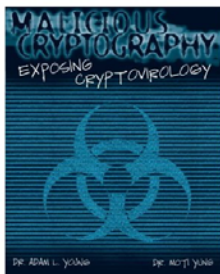
Title: Malicious Cryptography – Exposing Cryptovirology

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

Exploitation of Common Internet Encryption Technologies

- 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

7
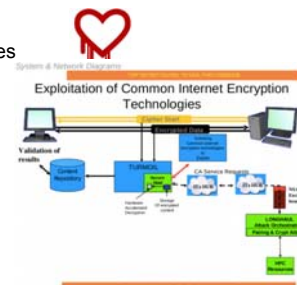
Fighting cryptography

- 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
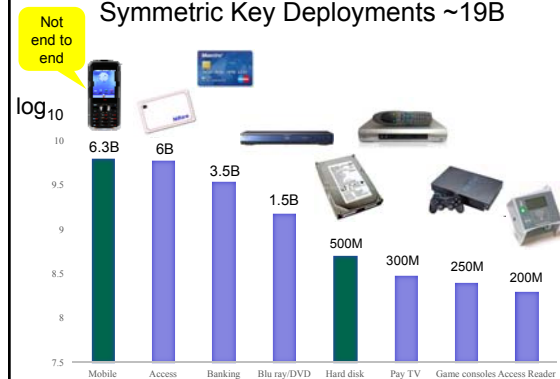- Impact on systems research and policy

44

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?
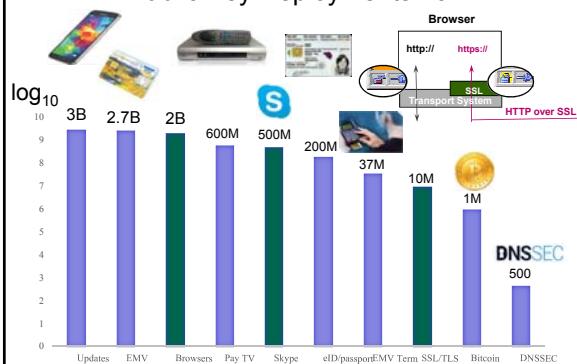 - most data in the cloud is not encrypted

45

Symmetric Key Deployments ~19B

Not end to end

$\log_{10}$

6.3B	Mobile
6B	Access
3.5B	Banking
1.5B	Blu ray/DVD
500M	Hard disk
300M	Pay TV
250M	Game consoles
200M	Access Reader

Missing: IPsec, SSH   © Bart Preneel

46

Public Key Deployments ~9B

$\log_{10}$

Browser

http://   https://

SSL
Transport System

HTTP over SSL

3B	Updates
2.7B	EMV
2B	Browsers
600M	Pay TV
500M	Skype
200M	eID/passport
37M	EMV Term
10M	SSL/TLS
1M	Bitcoin
500	DNSSEC

DNSSEC

Missing: IPsec, SSH   © Bart Preneel

47

Cryptography that seems to work

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

Other User IP Addresses

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

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 ($\geq$ 2048), Diffie-Hellman ($\geq$ 2048), ECDH and AES
- open source
- end-to-end
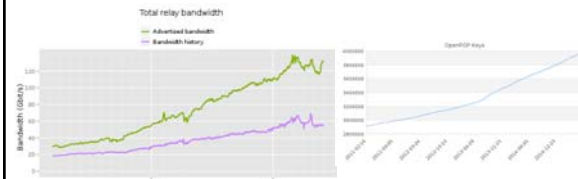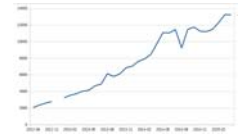- limited user base

* some Tor traffic can be deanonymized

49

The State of Encryption
http://www.dailydot.com/politics/encryption-since-snowden-trending-uo/

Tails: 13K boots per day (x2)

OpenPGP: 4M public keys (x1.2)

Tor: 7000 relays (x2), 130 Gbps
    advertised bandwidth (x4)

50

We are going dark

51

"[I]n our country, do we want to allow a means of communication between people which we cannot read?"

52

53

Exclusive: U.S. tech industry appeals to Obama to keep hands off encryption

As Washington weighs new cybersecurity steps amid a public backlash over mass surveillance, U.S. tech companies warned President Barack Obama not to weaken increasingly sophisticated encryption systems designed to protect consumers' privacy.
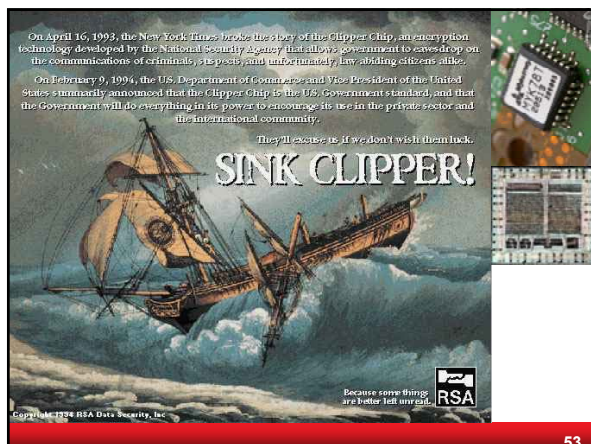
9

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

55

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,…

56

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

57

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)
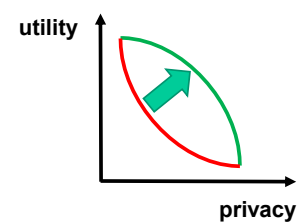
58

Architecture is politics [Mitch Kaipor'93]

Avoid single point of trust that
becomes single point of failure

59

Pushing the tradeoffs

utility

privacy

60

10

COMPUSEC - Computer Security

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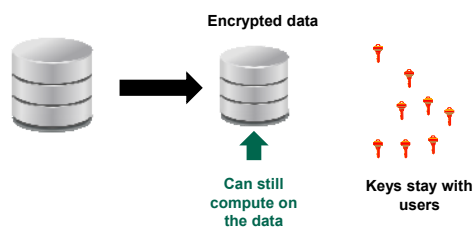 - • Territoriality
- – what if computations are needed?

61

From Big Data to Small Local Data

Data stays with users

62

From Big Data to Big Encrypted Data

Encrypted data

Can still compute on the data

Keys stay with users

63

Open (Source) Solutions

Effective governance

Transparency for service providers

64

KISS Principle

Keep It Simple Stupid

65

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

66

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 [Danezis]
  – need industrial policy with innovative technology that can guarantee economic sovereignty
  – need to give law enforcement sufficient options

67

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

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

Short version of this presentation:
- https://www.youtube.com/watch?v=uYk6yN9eNfc

68