# Cryptography and Information Security in the Post-Snowden era

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




## Outline

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



## 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





## Snowden revelations

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



## 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



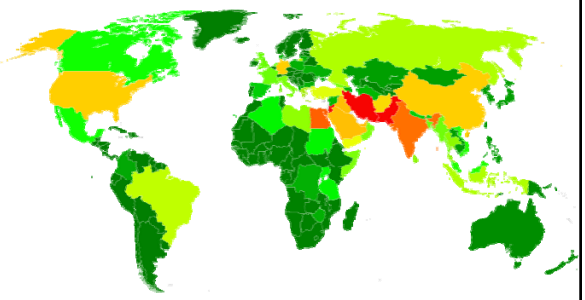
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## 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

## NSA surveillance by country



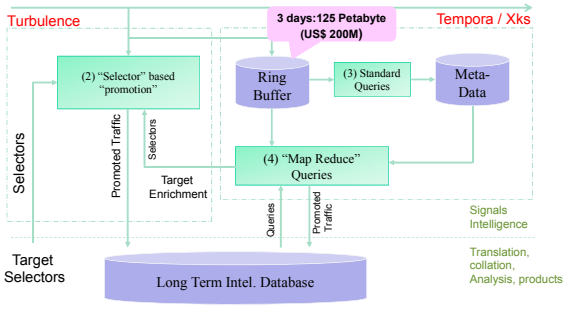
7

## Germany


8

## TEMPORA architecture (GCHQ)

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




Slide credit: George Danezis, UCL

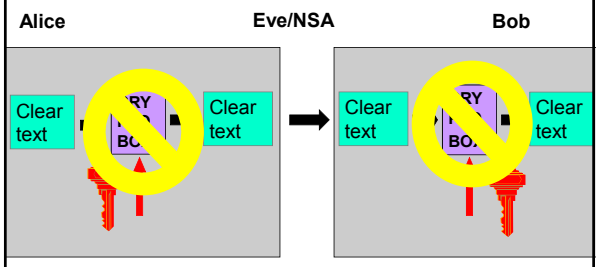
9

## 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

10

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



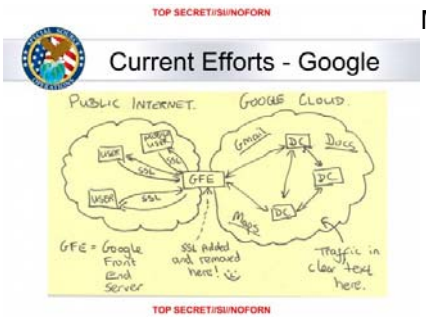

11

## Where do you find plaintext?

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


Tempora

12

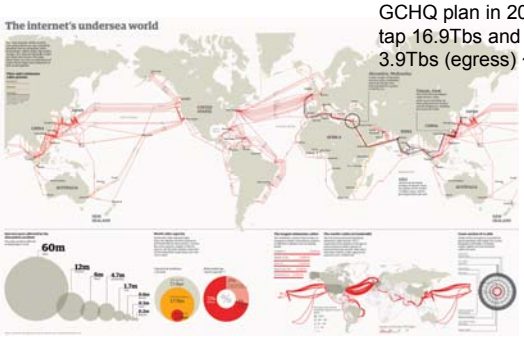



Muscular (GCHQ) help from Level 3 (LITTLE)

**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)**

13

## Upstream (continued): 90% of traffic over cables




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

Source: The Guardian

14

## 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**

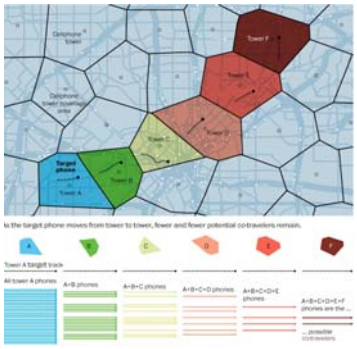
**EU: data retention directive (2006/24/EC)**
- declared illegal by EU Court of Justice in April 2014: disproportionate and contrary to some fundamental rights protected by the Charter of Fundamental Rights, in particular to the principle of privacy

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

15

## 3. Traffic data (DNR) – phone location

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



16

## 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)

17

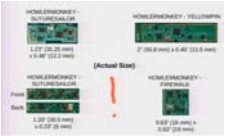
## 4. Client systems

- hack the client devices
  - use unpatched weaknesses (disclosed by vendors or by update mechanism?)
  - sophisticated malware
- get plaintext
  - e.g. webcam pictures of users
- it is well known that any mobile phone can be converted into a remote microphone

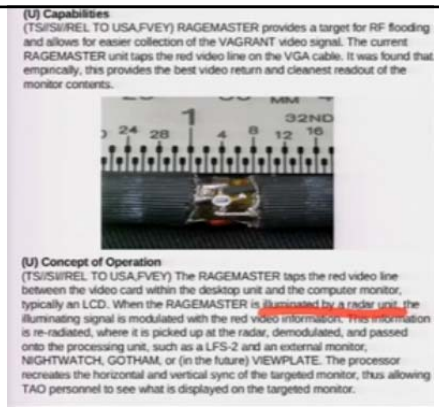
18

## 4. Client systems: 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



19



**(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.

20

## Lessons learned (1)

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)

21

## Lessons learned (2)

Economics of scale play a central role

It is not about the US or US/UK or even five eyes

- other nations have similar capabilities
- more are developing them
- organized crime and terrorists working on this too

Need for combination of industrial policy and non-proliferation treaties

22

## Outline

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

23

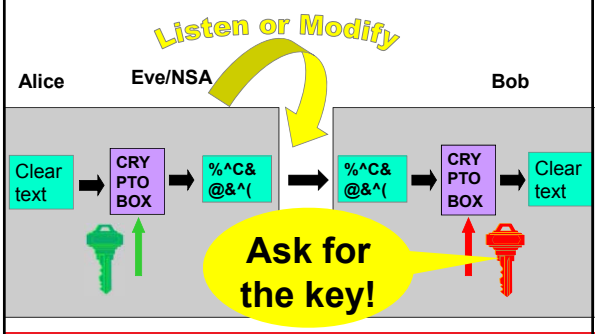
## NSA foils much internet encryption

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

24

## If you can't get the plaintext




25

## Asking for the key

- (alleged) examples
  - 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

26

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

fake SSL certificates or SSL person-in-the-middle

- Flame: rogue certificate by cryptanalysis*
- Comodo, Diginotar, Turktrust
- TLS data stored by GCHQ FLYING PIG (Google, Hotmail, Yahoo!)

* *Stevens*, Counter-cryptanalysis, *Crypto 2013*

27

## The CA Mess on the web

[Eckersley10] "An observatory for the SSLiverse"

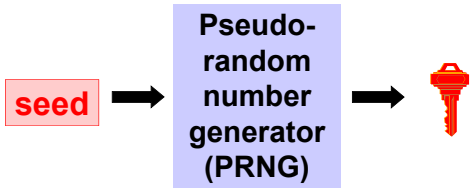
10.8M servers start SSL handshake
4.3M use valid certificate chains
650 CA certs trustable by Windows or Firefox
1.4M unique valid leaf certs
- 300K signed by one GoDaddy cert

80 distinct keys used in multiple CA certs
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)
- resulted in 28K vulnerable certs
- fortunately only 530 validate
- only 73 revoked

28

## 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

29

## 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.*

30

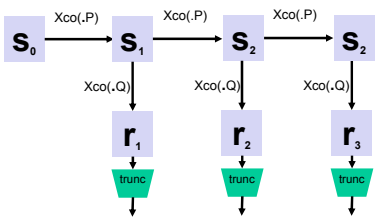
## Dual_EC_DRBG

- NSA **Bullrun program:** NSA has been actively working to "Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets."
- 10 Sept. 2013, NYT: "internal memos leaked by a former NSA contractor suggest that the NSA generated one of the random number generators used in a 2006 NIST standard — called the Dual EC DRBG standard — which contains a **backdoor** for the NSA."
- 9 Sept. 2013: NIST **"strongly recommends" against the use of Dual_EC_DRBG**, as specified in the January 2012 version of SP 800-90A.

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

31

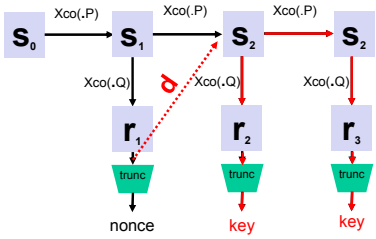
## Dual_EC_DRBG: state recovery




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

32

## Dual_EC_DRBG: state recovery




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

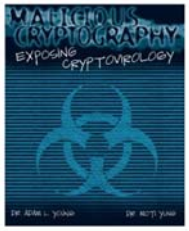
Depending on library: key recovery in a few seconds or a few hours

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

33

## Cryptovirology [Young-Yung]

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




Title: Malicious Cryptography – Exposing Cryptovirology

Authors: Adam Young
Moti Yung

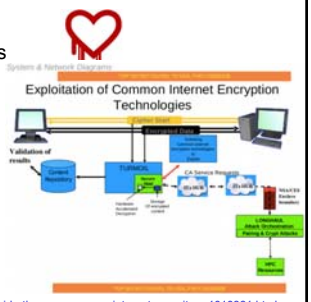
Date: February, 2004

Publisher: John Wiley & Sons

34

## 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

35

## Can NSA break AES with TUNDRA?

(TS//SI//REL) **TUNDRA** -- Electronic codebooks, such as the Advanced Encryption Standard, are both widely used and difficult to attack cryptanalytically. NSA has only a handful of in-house techniques. The TUNDRA project investigated a potentially new technique -- the Tau statistic -- to determine its usefulness in codebook analysis. This project was supported by [redacted] of R21.

TUNDRA = 2009 undergraduate student project

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

*"The EDGE"*

**National Information Assurance Research Laboratory (NIARL) Science, Technology, and Personnel Highlights**

36

## 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 13:35:35 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 | | | [OC: No decrypt available for this OTR encrypted message.] |
| 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 | | | |

Snowden had no access to cryptanalytic know-how and documents of NSA (only SIGINT)

37

## 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, Diffie-Hellman, ECDH and AES
- open source
- end-to-end
- limited user base

* some Tor traffic can be deanonymized

38

## Fighting cryptography

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

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

39

## Outline

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

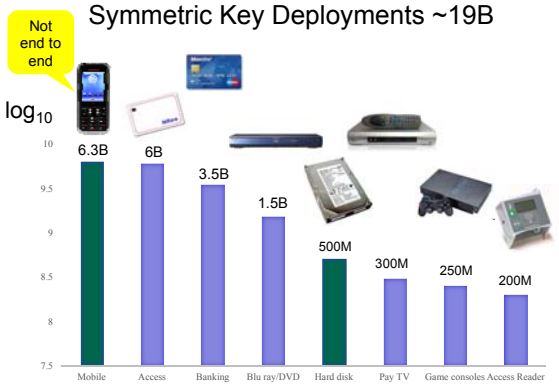
40

## 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

41

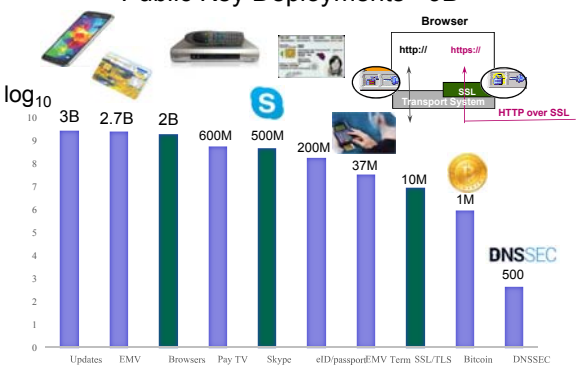
## Symmetric Key Deployments ~19B




Missing: IPsec, SSH © Bart Preneel

42

## Public Key Deployments ~9B




Missing: IPsec, SSH © Bart Preneel

43

## 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

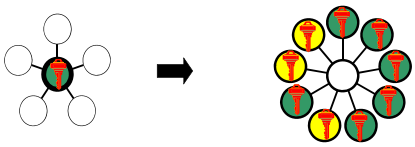
44

## 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



45

## COMSEC - Communication Security

Secure channels

- authenticated encryption studied in CAESAR http://competitions.cr.yp.to/caesar.html
- protection against replay, reordering, packet deletion
- hiding length of plaintext
- release of unverified plaintext [Asiacrypt'14]

Forward secrecy: Diffie-Hellman versus RSA

Denial of service

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

46

## 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

47

## 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?

48

## 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
  - entity that controls updates is in charge
- Current **defense technologies** (firewall, anti-virus) not very strong
  - cannot resist a motivated attacker
- Not designed to resist **human factor** attacks: coercion, bribery, blackmail
- **Supply chain** of software and hardware vulnerable and hard to defend
  - **backdoors** are hard to detect

49

## COMPUSEC - Computer Security

- Simplify to reduce attack surface
- Secure local computation
  - with minimal trusted computing base
  - with threshold security
  - MPC, (F)HE, .. in practice
  - hardware support: TPM, SMART, Sancus, SGX,…
- Secure and open standards and implementations
- Community driven open audit

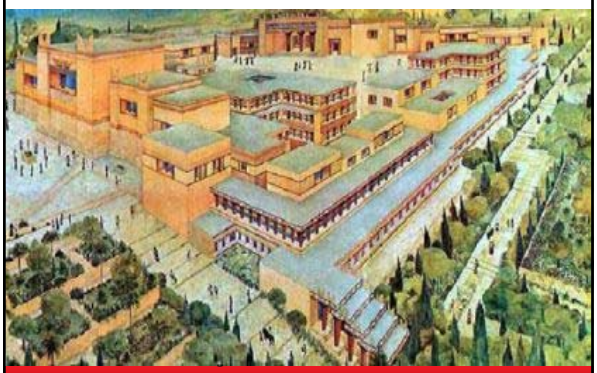
50

## Reconsider every stage

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

51

## Architecture is politics [Mitch Kaipor'93]



52

## 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

53

## Conclusions (research)

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

54

## 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

55