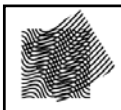


KU LEUVEN

Cryptography and Information Security in the Post-Snowden Era

Bart Preneel
COSIC KU Leuven and iMinds, Belgium
Bart.Preneel(at)esat.kuleuven.be
October 2014

iMinds
CONNECT.INNOVATE.CREATE

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Backdoors in crypto standard
- Impact on cryptology and information security research

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

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

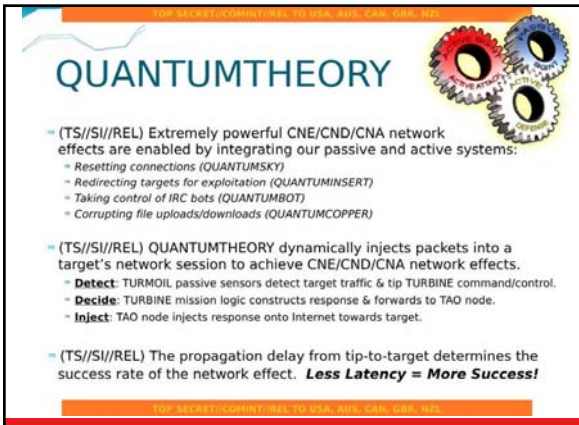
undermining cryptographic standards with backdoors (Bullrun) … and also the credibility of NIST

Snowden revelations (2)

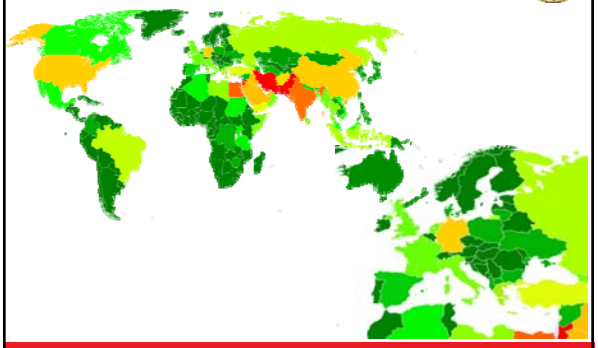
Most spectacular: **active defense**
- networks
  - Quantum insertion: answer before the legitimate website
  - FoxAcid: specific malware
- devices
  - malware
  - supply chain subversion

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

No longer deniable

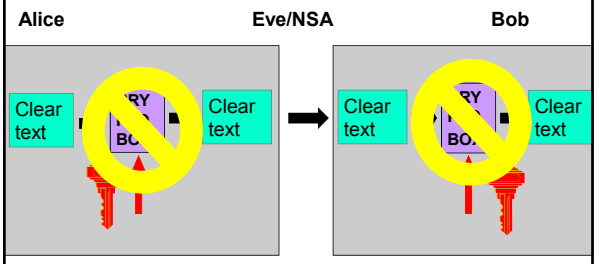


NSA surveillance by country



7

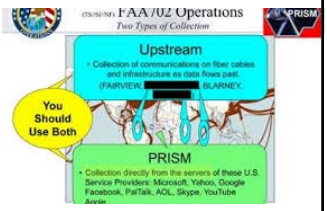
Rule #1 of cryptanalysis: search for plaintext [B. Morris]



8

Where do you find plaintext?

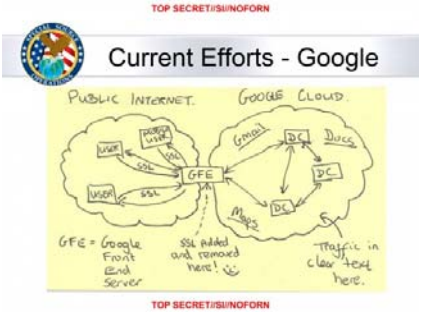
1. PRISM (server)
2. Upstream (fiber)



Tempora

9

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)

10

Upstream (continued)

- What if you want the upstream in other countries?
  - Echelon (European Parliament 2001)
    - submarines (underwater cables)
    - satellites
    - fiber
  - reroute traffic– who ever believed that internet routing was secure?
  - hack the telcos (Belgacom?)

11

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

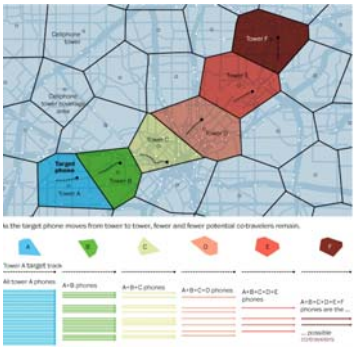
6 June 2013: NSA collecting phone records of millions of Verizon customers daily

EU: data retention directive (2006/24/EC)
– declared illegal by EU Constitutional Court in April 2014

12

3. Traffic data (DNR) – phone location

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



13

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)

14

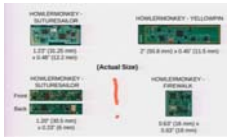
4. Client systems

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

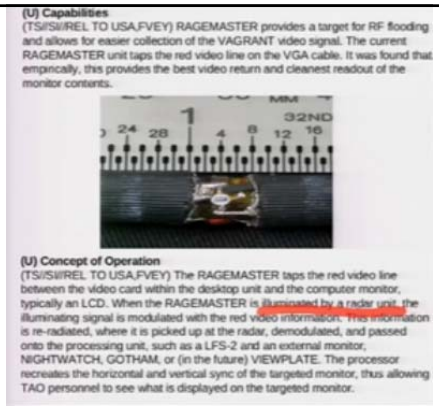
15

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



16



(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.

17

Lessons learned

Never underestimate a motivated, well-funded and competent attacker

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

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 will follow

Need for non-proliferation treaties

18

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Backdoors in crypto standard
- Impact on cryptology and information security research

19

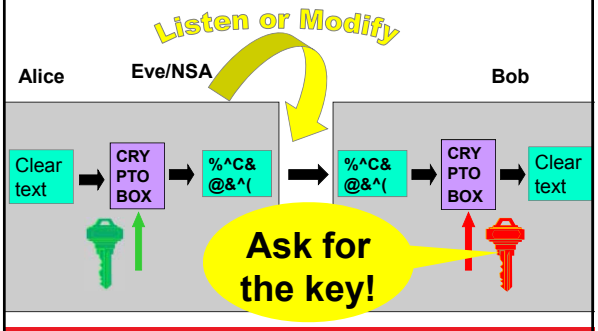
NSA foils much internet encryption

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

20

If you can't get the plaintext



21

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

22

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

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

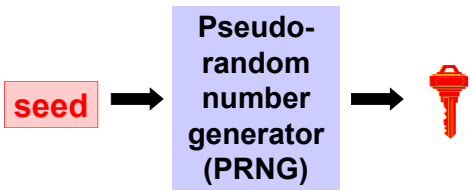
- Flame: rogue certificate by cryptanalysis*
- Comodo, Diginotar, Turktrust
- TLS data stored by GCHQ FLYING PIG (Google, Hotmail, Yahoo!)

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

23

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

24

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.

25

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?

26

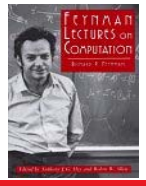
Cryptanalysis on Quantum Computers?

exponential parallelism

n coupled quantum bits ⇒ 2^n degrees of freedom !

Shor 1994: perfect for factoring

but: can a quantum computer be built?



27

If a large quantum computer can be built...

all schemes based on factoring (RSA) and DLOG will be insecure

same for elliptic curve cryptography

symmetric key sizes: x2

hash sizes: unchanged (for collisions)

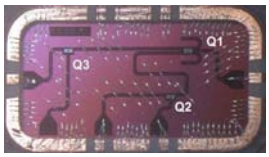
alternatives: postquantum crypto

- McEliece, NTRU,…
- so far it seems very hard to match performance of current systems while keeping the security level against conventional attacks

28

2001: 7-bit quantum computer factors 15
2007: two new 7-bit quantum computers
2012: 143 has been factored

2012: 10 to 15 years for a large quantum computer



Quantum Computing: An IBM Perspective

Steffen, M.; DiVincenzo, D. P.; Chow, J. M.; Theis, T. N.; Ketchen, M. B.

The implementation of a functioning quantum computer poses tremendous scientific and technological challenges, but current rates of progress suggest that these challenges will be substantively addressed over the next ten years. We provide a sketch of a quantum computing system based on superconducting circuits, which are the current focus of our research. A realistic vision emerges concerning the form of a future scalable fault-tolerant quantum computer.

News in January 2014: NSA has spent 85 M$ on building a quantum computer

29

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

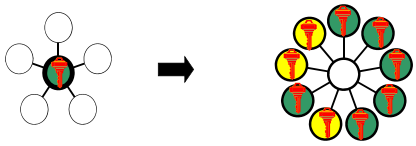
Limited fraction(a few %) of traffic is protected.
A very small fraction of traffic is protected end-to-end with a high security level

30

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



31

COMSEC - Communication Security

Secure channels

Authenticated encryption studied in CAESAR
http://competitions.cr.yp.to/caesar.html

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

32

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

33

COMPUSEC - Computer Security

Protecting data at rest
- well established solutions for local encryption: Bitlocker, Truecrypt
- infrequently used in cloud
- Achilles heel is key management

34

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

35

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 implementations
- Community driven open audit

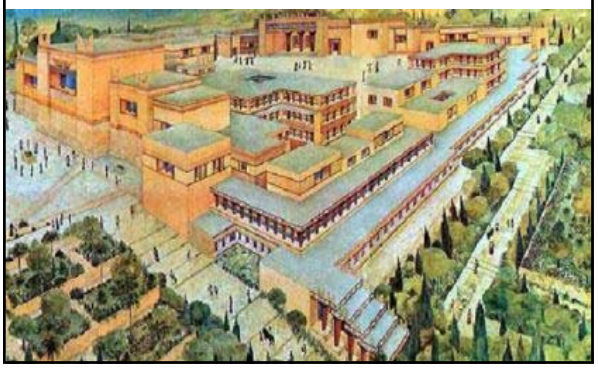
36

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

37

Architecture is politics [Mitch Kaipor'93]



Governance and architectures

Governments: want access for themselves but preclude this for others
- seems elusive with current state of the art

Industry: conflicting requirements
1. government requirements for access and backdoors
2. DRM for content and software
3. privacy of consumer

Individual: cannot manage complex tradeoffs

Need to rethink centralized architectures with massive storage of raw data
- avoid single point of trust that becomes single point of failure
- data minimization through infrastructure

39

Governance and Architectures

Back to principles: minimum disclosure
- stop collecting massive amounts of data
- 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

40

IACR Copenhagen Declaration May 2014

The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards. Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.

41

Conclusions

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

42