Cryptography in the Post-Snowden Era

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

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
Cryptography in the post-Snowden era
Bart Preneel

August 2014

NSA analyzes massive data

**Boundless informant** (8 June 2013)
- big data analysis and data visualization for surveillance overview
- summarizes data records from 504 separate DNR and DNI collection sources
- scale: millions of items per day and per country
  - DNI: Digital Network Intelligence – content
  - DNR: Dial Number Recognition – meta data

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

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

Where do you find plaintext?

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

NSA surveillance by country

**Xkeyscore** (July 2013):
- 700 servers at approximately 150 sites
  - F6 (Special Collection Service) – CIA/NSA clandestine operations including espionage on foreign diplomats and leaders
  - FORNSAT (foreign satellite collection): intercepts from satellites
  - SSO (Special Source Operations) – cooperation with telcos
  - Overhead: US spy planes, drones and satellites
  - TAO (Tailored Access Operations) – hacking and cyberwarfare
  - FISA – approved by the Foreign Intelligence Surveillance Court
  - Third party – foreign partners of the NSA such as the (signals) intelligence agencies of other nations
  - Also Windows error reporting
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

3. Traffic data (DNR) – phone location
- NSA collects about 5B records a day on cell phone location
- Co-traveler

3. Traffic data (DNR) - defense
- TOR: tool for anonymous browsing and services
  - not designed to resist global attacker

- NSA’s attempts
  - denial of service
  - compromise end systems e.g. via bug in browser package (EgotisticalGiraffe)
  - meet-in-the-middle via web site impersonations (Quantum)

- according to leaked documents from 2006: “We will never be able to de-anonymize all Tor users all the time” but “with manual analysis we can de-anonymize a very small fraction of Tor users”


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
Cryptography in the post-Snowden era
Bart Preneel

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

Lessons learned

Never underestimate a motivated, well-funded and competent attacker

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

It is not about the US or US/UK or even five nations
  - other nations have similar capabilities
  - more are developing them
  - organized crime and terrorists will follow

Need for non-proliferation treaties

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Impact on cryptology
- Impact on cryptology research

If you can’t get the plaintext

Outline

- Snowden revelation: the essentials
- Snowden revelations: some details
- Impact on cryptology
- Impact on cryptology research

Ask 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
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
- Info on TLS collected in FLYING PIG (GCHQ)

* Stevens, Counter-cryptanalysis, Crypto 2013

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

If you can't get or replace the key
make sure that the key is generated using a
random number generator with trapdoor

Pseudo-random number generator (PRNG)

trapdoor allows to predict keys

Dual_EC_DRBG or Dual Elliptic Curve Deterministic Random Bit Generator

- 1 of the 4 PRNGs in NIST SP 800-90A
- draft Dec. 2005; published 2006; revised 2012
- warnings
  - Dec 05: output not perfectly random [Gjøsteen]
  - Mar 06: security proof; but weak if one fails to choose P and Q at random, e.g. Q = d.P for a known d [Brown]
  - May 06: flaw [Schoenmakers-Sidorenko]
  - Aug 07: backdoor [Ferguson-Shumov]

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.

Dual_EC_DRBG or Dual Elliptic Curve Deterministic Random Bit Generator

- 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."

- 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."

If you can't get or replace the key
make sure that the key is generated using a
random number generator with trapdoor

Pseudo-random number generator (PRNG)

trapdoor allows to predict keys

Dual_EC_DRBG or Dual Elliptic Curve Deterministic Random Bit Generator

- 9 Sept. 2013: NIST “strongly recommends” against the use of dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A.
- in light of community security concerns SP 800-90A reissued as draft standard, and re-opening SP800-90B/C for public comment

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

On 7 Feb 2001 Bleichenbacher of Bell Labs found an attack on the PRNG building block of DSA (FIPS 186). Coincidence?

If you can't get plaintext or key: cryptanalysis

Can NSA break
- RSA-512: easily
- RSA-768: definitely
- RSA-1024: likely
- RSA-1536: perhaps
- RSA-2048: who knows
Cryptography in the post-Snowden era
Bart Preneel

August 2014

Widely used public-key systems rely on 3 problems from algebraic number theory

Integer factorization: RSA \( (n = p \cdot q) \)
Discrete LOGarithm: Diffie-Hellman, DSA: \( y = g^x \)
Elliptic Curve Discrete LOGarithm, ECDSA: \( Q = x \cdot P \)

RSA-1024 ~ DLOG-1024 ~ ECC-146
RSA-2048 ~ DLOG-2048 ~ ECC-206
RSA-4096 ~ DLOG-4096 ~ ECC-282

Not so likely that NSA can break some specific ECC curves proposed by NIST

Public key crypto security

L(0): Factoring and DLOG
L(1): best ECC DLOG solvers
L(1/2): 1981 Factoring and DLOG
L(1/3): 1984 Factoring and (Non-ECC) DLOG stay here for 30 years
L(1/4): DLOG special numbers (Joux Feb'13)

with restriction on the groups (Barbulescu et al. in Jun'13)

Special form DLOG record: 9234 bits [Granger+’13]
Supersingular binary curves 59-bit security << 128 [Granger+’13]

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?

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
Cryptography in the post-Snowden era

Bart Preneel

August 2014

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

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

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
Use forward secrecy: Diffie-Hellman rather than public-key encryption (e.g. TLS)

COMSEC - Communication Security
Randomized encryption
– great success of theory
– but vulnerable to kleptography such as algorithm substitution attack [Paterson et al.'14]

Deterministic stateful encryption
– can avoid some of these problems
– security guarantees not much worse if carefully implemented

Similar observation for MAC algorithms and digital signatures; see e.g.: subliminal channels [Simmons] kleptography [Young-Yung]

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
Cryptography in the post-Snowden era

Bart Preneel

August 2014

COMPUSEC - Computer Security

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

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

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

Reconsider every stage

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

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
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

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.

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