Post-Snowden Cryptography
or who holds your keys?
Bart Preneel
COSIC KU Leuven and iMinds, Belgium
Bart.Prneel(at)esat.kuleuven.be
February 2014

© KU Leuven COSIC, Bart Preneel

Crypto Wars History 101
• hardware export (and import) controls
  – weak or very weak encryption in mobile phones
    (A5/1 and A5/2)
• research: attempts to suppress
  – US in late 1970s: examples: RSA, Davida
  – EU around 1988: example: RIPE
• software export controls (1987-1993)
  – mostly restricted to 40-bit keys (RC4/DES = IBM
    CDMF)
  – even hooks/APIs disallowed
  – avoid: using print books (e.g. PGP)

Cracking DES (56-bit key)
controversy in 1977: $20-200 million
M. Wiener’s design (1993):
$1 million machine: 3 hours
(today < 1 second)
EFF Deep Crack (July 1998)
250,000 $ machine: 50 hours…
DES was withdrawn by NIST
in 2004

Wassenaar Arrangement
(1995-present)
the first global multilateral arrangement on export
controls for conventional weapons and sensitive
dual-use goods and technologies
signed in 1995, operational Sept. 1996
33 members now expanded to 41
relaxed in 1998:
  – symmetric key: 56 bits, public key: 512 RSA/112 ECC
  – mass market: 64 bits (but…)
no cryptanalytic hardware
personal use exemption

Sept. 2000: announcement about lifting some
restrictions
Oct. 2000: Rijndael selected as AES
Dec. 2000: 64-bit limit relaxed for mass market
software and hardware
details: http://www.cryptolaw.org/
Legal intercept

Overlooked for GSM
Has been added to various communication systems
- VOIP
- 3G/LTE

Digital Millennium Copyright Act (1998)
goal: implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty (and for other purposes)
cryptanalytic research may not be allowed
- example: Dmitry Sklyarov

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

Mission from Cold War, repurposed after 9/11
Collect it all, know it all, exploit it all (or: in God we trust, all others we monitor)
- even air to ground link from laptop to ground in airplanes and chat in second life

Information about NSA/GCHQ

- 1982
- 1987
- 2002
- 2010
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 surveillance by country

The Netherlands and France

Spain and Italy
NSA analyzes massive data

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
- SS0 (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

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)

Is upstream surprising?

- 7 April 2006
- whistleblower Marc Klein, ex-AT&T Technician reports about NSA room 641A at 611 Folsom Street in San Francisco
  - includes splitter + data mining

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)
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?)

With help of foreign agencies?

- in 1 day: 444,743 e-mail address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers
  - 250 M email addresses per year
  - 500,000 buddy lists and inboxes per day
  - 180 M per year

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)

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 (Egostical/Giraffe)
    - 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?)
  - anyone remembers _NSAKEY from 1999?
- get plaintext

- it is well known that any mobile phone can be converted into a remote microphone
4. Client systems: TAO

- Targeted 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

4. Client systems: TAO (2)

ANDYGRAM: A telephone tripwire that mimics a cellphone tower.
ANGRYNEIGHBOR: taps your PS/2 or USB keyboard and transmits to the radio antenna station.
COTTONMOUTH: A modified USB plug for intercepting communications, installing trojans etc.
WATERWITCH: A handheld "finishing tool" for finding the exact location of nearby handsets.
SURLYSPAWN: Monitors keystrokes when a target computer isn't connected to the Internet.
FOXACID: A system for installing spyware with a "quantum insert" that infects spyware at the packet level.
IRONCHEF: Infects networks by installing itself in a computer's input-output BIOS.
JETPLLOW: A firmware implant that provides a permanent backdoor through a Cisco firewall.

4. Client systems: TAO (3)

HEADWATER: Does the same for China's Huawei routers.
RAGEMASTER: Taps the line between a desktop computer's video card and its monitor.
HOWLERMONKEY: A radio transceiver for extracting data from systems or making them remote-controllable.
  - 50 units fetches $200,000 USD
MONKEYCALENDAR: Attack software that sends a mobile phone's location by covert text message.
DIETYBOUNCE: Installs a secret payload in a Dell computer by reflashing the motherboard BIOS when the machine is turned on.
SOMBERKNAVE: A Windows XP implant to connect computers to NSA headquarters, from where they can be remotely controlled.

4. Client systems: TAO (4)

ANGRYMONK: Inserts itself into the firmware of hard drives made by Western Digital, Seagate, Maxtor and Samsung.
SWAP: Reflashes the BIOS of multiprocessor systems running Windows, Solaris, Linux or FreeBSD.
SPARROW II: A tool for detecting and mapping wireless networks via drone.
TOTEHOSTLY: An implant that allows full remote control of Window Mobile phones.
DROPOUTJEEP: "A software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted."

TOTS/SCREEN TO USA/FVEY: The CTX4000 is a portable sensitive area (SPA) radar unit. It can be used in a target system to recover all sensitive information. Primary uses include VAGRANT and DROPMIRE collection.
Further comments

Quantum:
- great firewall of China works in the same way
- similar methods used in Syria

[Feb.’14]: GCHQ runs DDOS attacks on chatrooms run by anonymous

If you can’t get the plaintext

If you can’t get the plaintext

Asking for the key

• (alleged) examples
  - Lavabit email encryption
  - CryptoSeal Privacy VPN
  - SSL/TLS servers of large companies

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
- NSA – GCHQ FLYING PIG (Google, Hotmail, Yahoo!)

* Stevens, Counter-cryptanalysis, Crypto 2013

---

The CA Mess on the web

- Ekeckley10 “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 addr. 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

---

If you can’t get or replace the key

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

\[ \text{seed} \rightarrow \text{Pseudo-random number generator (PRNG)} \rightarrow \text{trapdoor allows to predict keys} \]

---

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: problem if one fails to choose P and Q at random but one chooses Q = dP 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."

---

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?
More PRNG flaws

- 1996: Netscape SSL [Goldberg-Wagner]
- 2008: Debian SSL [Bellu]
- 2012: wireless routers [Heninger+], PGP/SSL [Lenstra+]
- 15 Aug. 2013: Android Java and OpenSSL PRNG flaw led to theft of bitcoins

AC’13 Factoring RSA keys from certified smart cards:
184 keys from Taiwan Citizen Digital Certificate cards
card + OS: EAL 4+; FIPS 140-2 Level 2

The Cryptocalypse?

2013 breakthrough for
DLOG in group of
special form

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

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

Integer factorization: RSA (n = p.q)
Discrete LOGarithm: Diffie-Hellman, DSA: y = g^x
Elliptic Curve Discrete LOGarithm, ECDSA: Q = x.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) — polynomial (weak)
L(1/2) — 1981 Factoring and DLOG
L(1) — best ECC DLOG solvers
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]
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

2001: 7-bit quantum computer factors 15
2007: two new 7-bit quantum computers
2012: 143 has been factored in April
2012: 10 to 15 years for a large quantum computer

And what about NSA?

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

Quantum Computing: An IBM Perspective
Steffen, M.; DiVincenzo, D. P.; Chow, J. M.; Theis, T. N.; Ketchen, M. B.
Quantum physics provides an intriguing basis for achieving computational power to address certain categories of mathematical problems that are completely intractable with machine computation as we know it today. We present a brief overview of the current theoretical and experimental works in the emerging field of quantum computing. 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.

Cryptographic breakthrough? (speculation)
Indications: James Clapper referred to it when presenting the budget
1) ECC - in general or for some curves; NSA has influenced curve selection
2) general factoring/DLOG - 10 year ahead
3) RC4 – effective attack
4) AES – solve the equations?
5) Random number generation flaws

Good crypto works but NSA finds a way around it

COMSEC - Communication Security
Protecting data in transit: encryption
– effective when done right
– good (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

meta data

- hiding communicating identities
  - few solutions
  - 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

---

COMPUSEC - Computer Security

Encrypting stored data

- well established solutions for local encryption: Bitlocker, Truecrypt
- few solutions for the cloud
- infrequently used
- 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
  - foreign 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

---

How to Improve the State of the Art

Human factor: education of IT people combined with security & privacy by default

Legal: strong privacy and security legislation with technical enforcement and substantial fines

Technology factor: research
  - cryptology
  - privacy enhancing technologies such as anonymous networking
  - secure and open implementations in hardware and software
  - community driven open audit
  - rethink IT
    - security architectures: security and privacy “by design”
    - key building blocks need to be rebuilt from scratch

Economic dimension:
  - standardization
    - going for gold standards, not compromises
    - open process, not driven by a single country (ideally European) or by industry only
  - procurement: European backdoor-free security

---

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
Transparency and community review

---

Recommendations

Invest more in defense than in offense
Open technologies and review by open communities
Rethink architectures
Research on improved technologies and standards
Use procurement wisely

Advertisement: draft report of EU parliament
More questions
How could Snowden collect 1.7 million documents?
- [NYT, 8 Feb. 14] “web crawler” software designed to search, index and back up a website
Which information does he not have?
- mostly SIGINT
- little about crypto
- not databases themselves
Will new policy restrict NSA?
- does it make a difference to store meta data at a third party provider? (automated access anyway)
- 3 degrees away becomes 2 degrees away
- can dual mission of NSA be rebalanced?
Will there be another whistleblower in 30 years?
Will revelations hurt recruitment for NSA?

The end
Thank you for your attention