



KU LEUVEN

Crypto Under Siege: New Threat Models

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



CONNECT. INNOVATE. CREATE

© KU Leuven COSIC, Bart Preneel

1

Outline

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

2

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

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...



TS//SI//REL to USA, FVEY

4

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

NSA calls the iPhone users public 'zombies' who pay for their own surveillance

TS//SI//REL to USA, FVEY

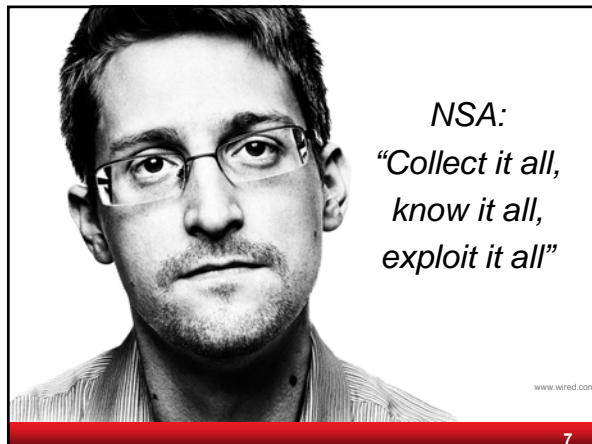
(S//REL) iPhone Location Services

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



TS//SI//REL to USA, FVEY

6



7

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 and implementations with backdoors (Bullrun) and also the credibility of NIST

* Impact of security letters reduced by Freedom Act (2 June 2015)

8

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

9

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)

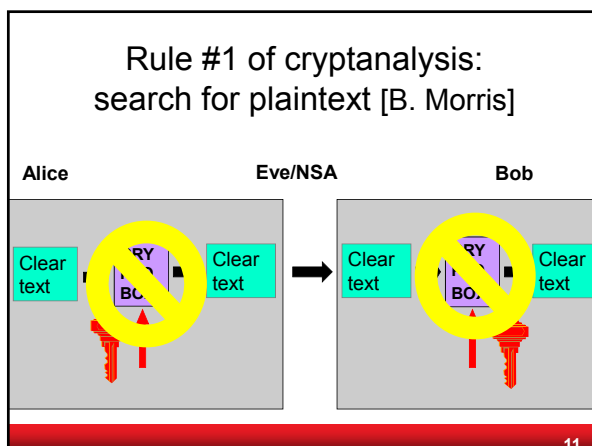
(TS//SI//REL) QUANTUMTHEORY dynamically injects packets into a target's network session to achieve CNE/CND/CNA network effects.

- **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, NED

10



11


Where do you find plaintext? SSO: Special Source Operations

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

Tempora

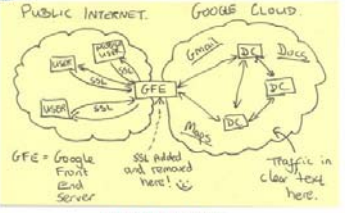
12

TOP SECRET//SI//NOFORN



Current Efforts - Google

Muscular (GCHQ) help from Level 3 (LITTLE)



TOP SECRET//SI//NOFORN

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

3. Traffic 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




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




14

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)

15

4. Client systems

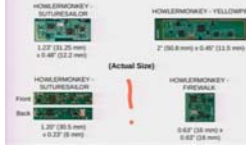
- hack the client devices
 - use unpatched weaknesses (disclosed by vendors or by update mechanism?)
 - sophisticated malware
- get plaintext
 - webcam pictures of users
 - mobile phones: turned into remote microphones or steal keys from SIM cards (Gemalto)

16

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**: installing spyware with a "quantum insert" that infects spyware at the packet level

17

(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.

18

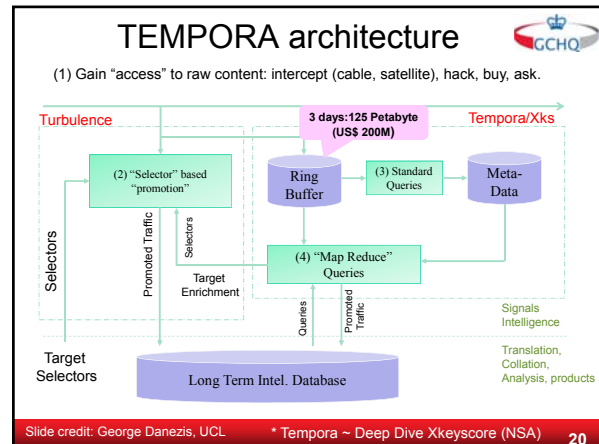
...and more

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]

19



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

Targeted surveillance based on mass surveillance

21

Surveillance spillover



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

23

Outline

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

24

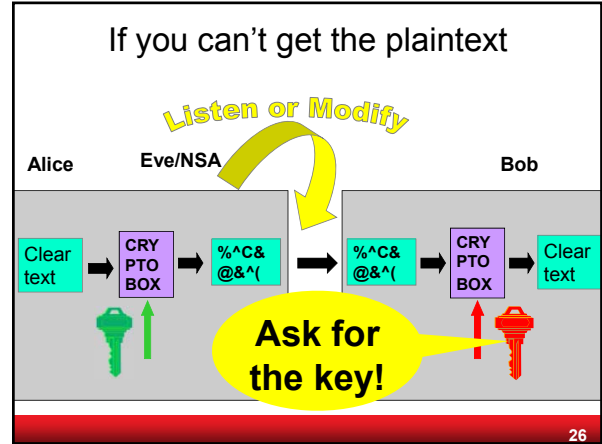
NSA foils much internet encryption

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]

25



Asking for the key

- (alleged) examples – through security letters?
 - Lavabit email encryption
 - CryptoSeal Privacy VPN
 - Silent Circle email
 - 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

27

Find the Private Key (Somehow)

[Adrian+15, LOGJAM, Imperfect forward secrecy]

- fallback to 512-bit export control legacy systems – cryptanalysed in real-time for Meet-In-The-Middle
- 1024-bit RSA and Diffie-Hellman widely used default option not strong enough
- GCHQ:



28

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

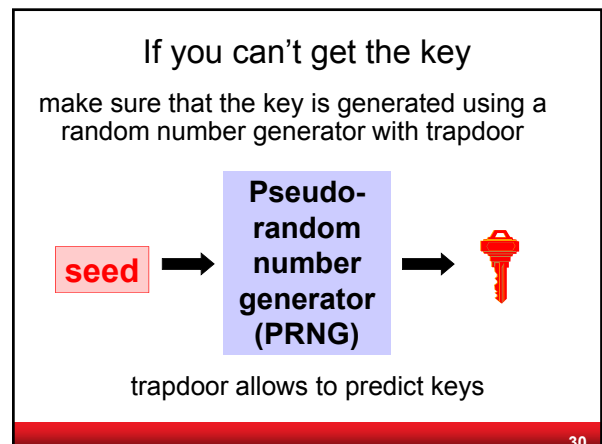
10.8M SSL/TLS servers
fake SSL certificates or SSL person-in-the-middle as commercial product or government attack

- 650 CA certs trustable by Windows or Firefox
- Comodo, Diginotar, Turktrust, ANSSI, China Internet Network Information Center (CNNIC), Symantec
- Debian OpenSSL bug (2006-2008): keys not revoked
- Flame: rogue certificate by cryptanalysis [Stevens, Counter-cryptanalysis, Crypto'13]



life since November 2015
<https://letsencrypt.org/isrg/>

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.

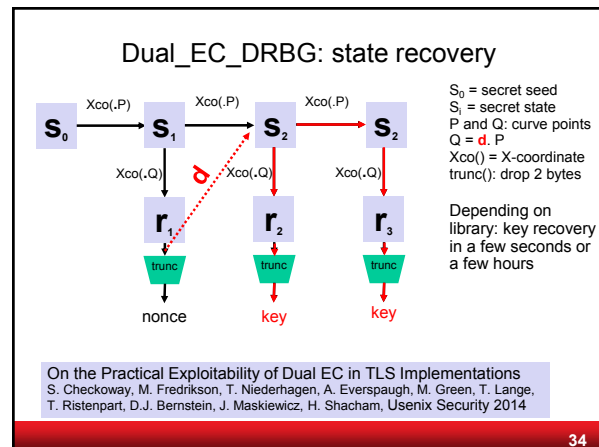
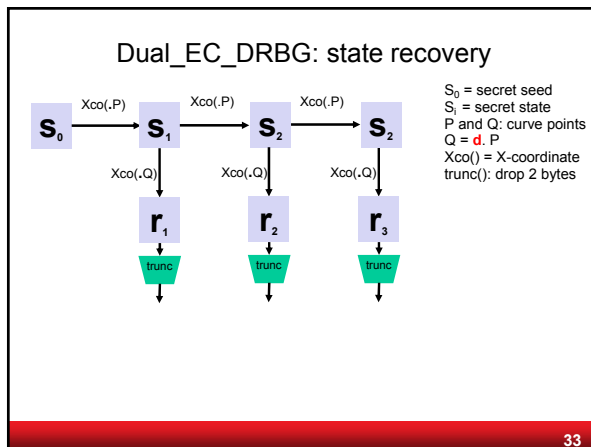
31

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?

32



Juniper Networks routers use Dual_EC_DRBG

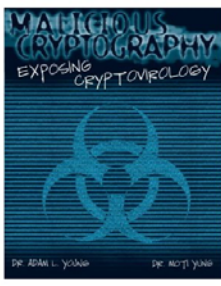
- Juniper in ScreenOS
 - used Dual_EC_DRBG with their own Q
 - processed output with ANSI X9.31 (3-DES)
- 2 security advisories on December 18, 2015
 - backdoor password for any user: “<<< %s(un=%s) = %u”
 - **someone managed to change the value of Q** (around August 2012)
 - a “bug” bypasses the ANSI X9.31 processing

NSA backdoor may have been used by someone else

35

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

36

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>

37

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

38

Outline

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

39

Symmetric Key Deployments ~19B

Not end to end

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

© Bart Preneel

40

Public Key Deployments ~10B

Category	Deployment
Updates	3B
EMV	2.7B
Browsers	2B
WhatsApp	900M
Pay TV	600M
Skype	500M
eID/pass, EMV Ter	200M
37M	37M
10M	10M
8M	8M
1M	1M
DNSSEC	500

Missing: SSH © Bart Preneel

41

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 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:08 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:12 [redacted] [OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:24 [redacted] [OC: No decrypt available for this OTR encrypted message.]
    
```

42

Cryptography that seems to work

difficulty decrypting certain types of traffic, including

- Truecrypt
- PGP/GPG
- Tor* ("Tor stinks")
- ZRTP from implementations such as Signal

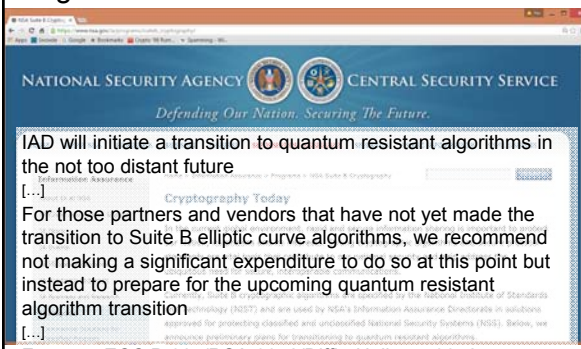
commonalities

- RSA (≥ 2048), Diffie-Hellman (≥ 2048), ECDH and AES
- open source
- end-to-end
- limited user base

* some Tor traffic can be deanonymized

43

August 19 2015: do not switch to Suite B



NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE
Defending Our Nation. Securing The Future.

IAD will initiate a transition to quantum resistant algorithms in the not too distant future

For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition

For now: ECC P-384/RSA-3072/Diffie-Hellman 3072


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.yt.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,...

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

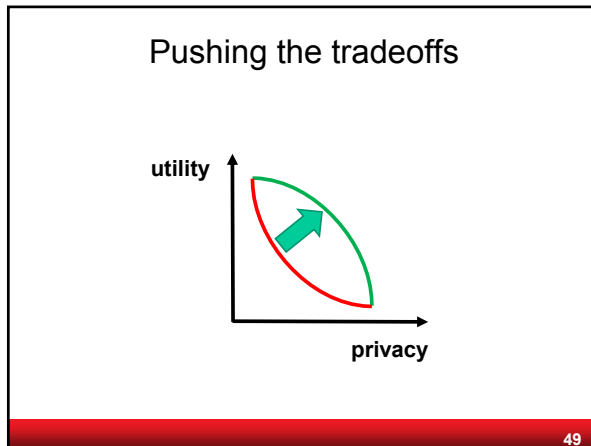
47

Architecture is politics [Mitch Kaipor'93]

Avoid single point of **trust** that becomes single point of **failure**



48

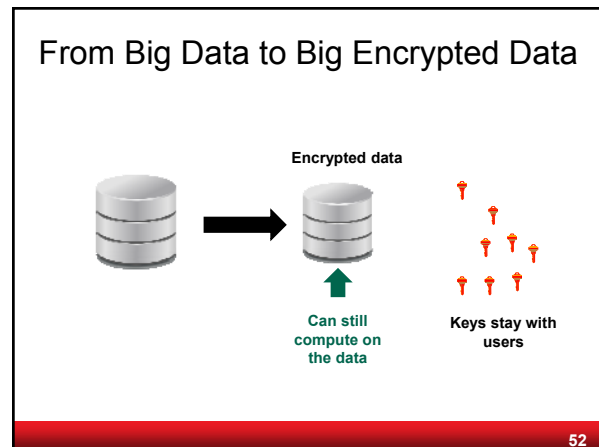
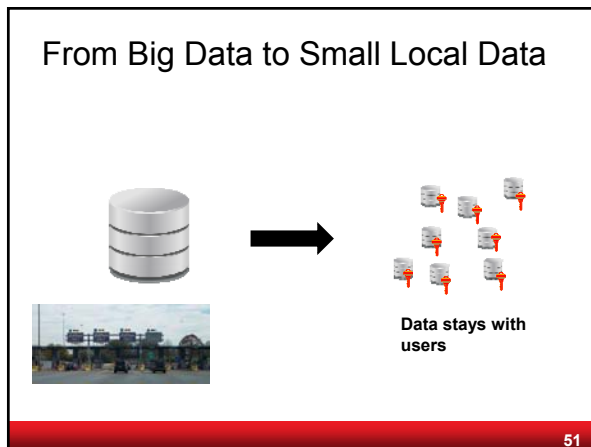


COMPUSEC - Computer Security

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?

50



Open (Source) Solutions

Effective governance

Transparency for service providers

53

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

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

55

Thank You for Your Attention



Industrial policy



to protect sovereignty and human rights

56

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>

57