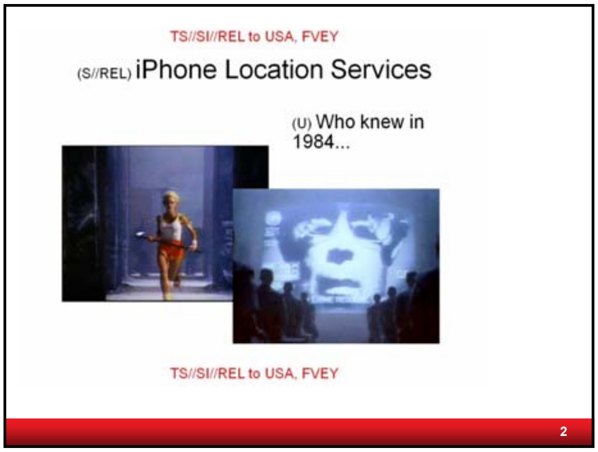
KU LEUVEN

Post-Snowden Cryptography

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

June 2016



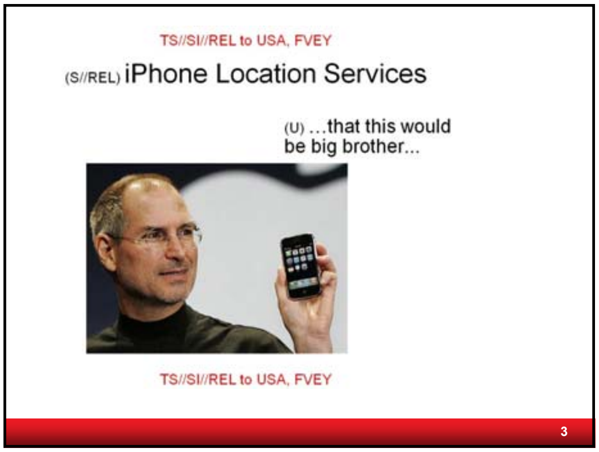
TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...

TS//SI//REL to USA, FVEY

2



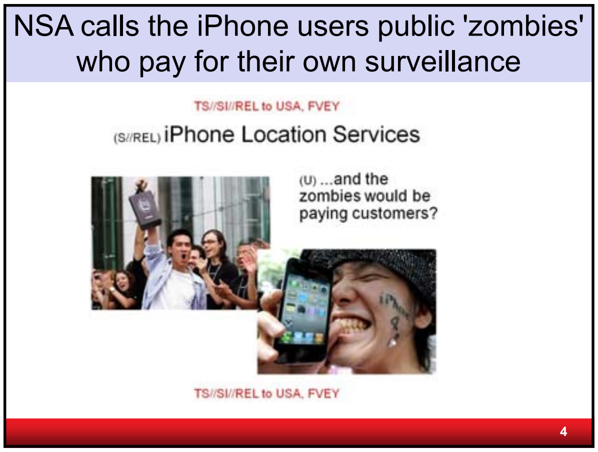
TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) ...that this would be big brother...

TS//SI//REL to USA, FVEY

3



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

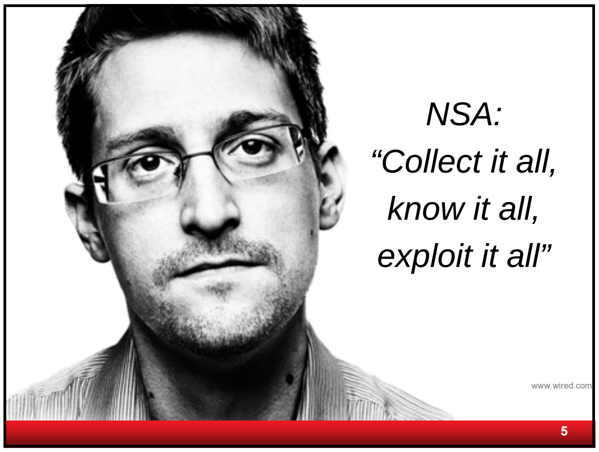
TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

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

TS//SI//REL to USA, FVEY

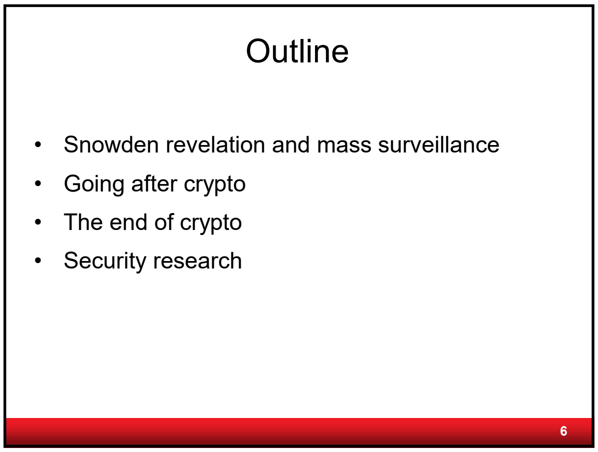
4



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

www.wired.com

5



Outline

- Snowden revelation and mass surveillance
- Going after crypto
- The end of crypto
- Security research

6

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

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

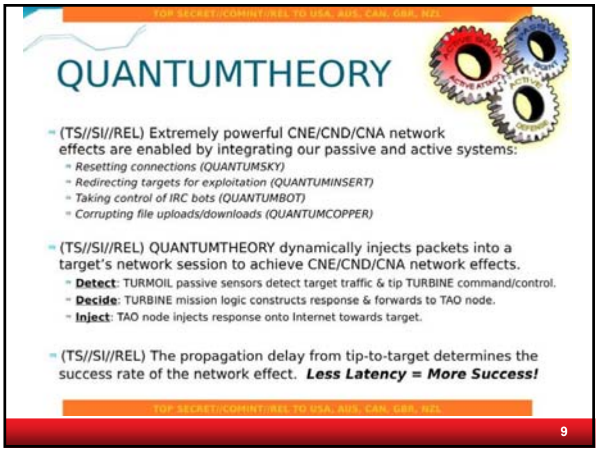
Snowden revelations (2)

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

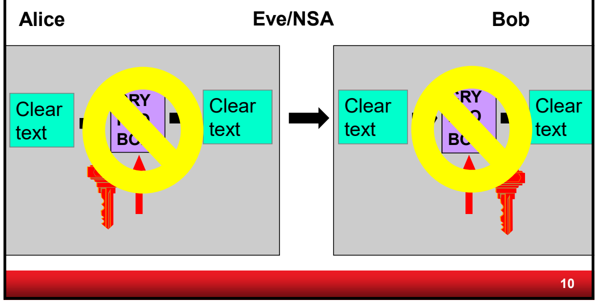
QUANTUMTHEORY

ACTIVE SIGINT
ACTIVE ATTACK
PASSIVE SIGINT
ACTIVE DEFENSE

- (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!***

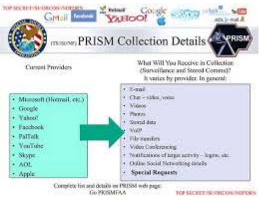
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

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



Where do you find plaintext? SSO: Special Source Operations

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



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

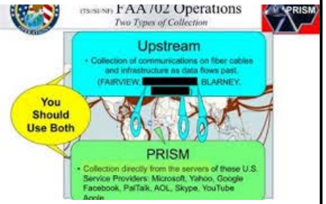
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page: Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) FAA702 Operations
Two Types of Collection

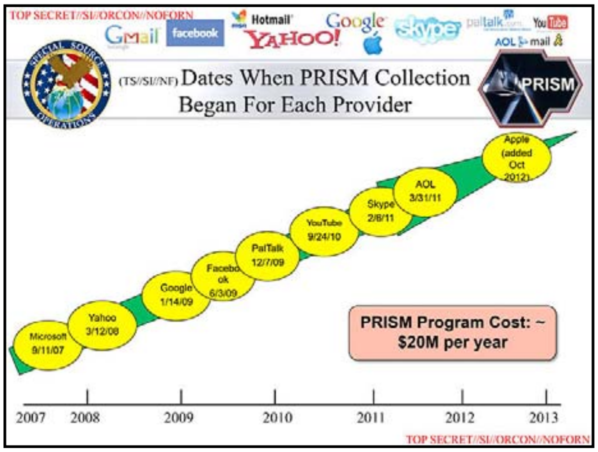
Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, [redacted] BLARNEY, [redacted]

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

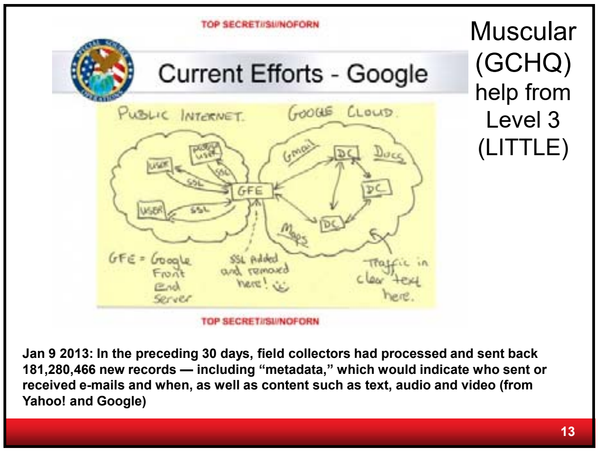


TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN



TOP SECRET//SI//NOFORN

Current Efforts - Google

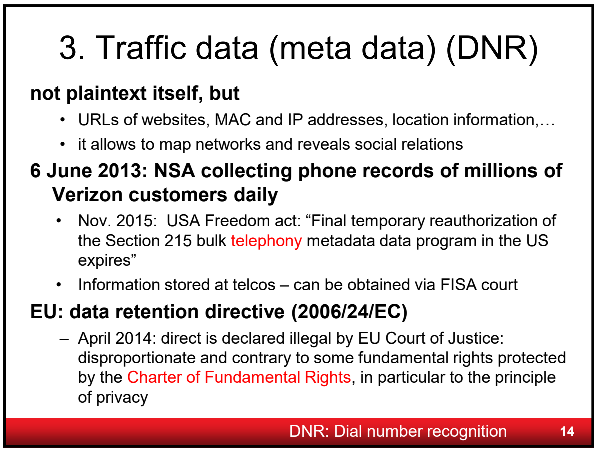
PUBLIC INTERNET
GOOGLE CLOUD
USER
PUBLIC USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

TOP SECRET//SI//NOFORN

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



3. Traffic data (meta data) (DNR)

not plaintext itself, but

- URLs of websites, MAC and IP addresses, location information,…
- it allows to map networks and reveals social relations

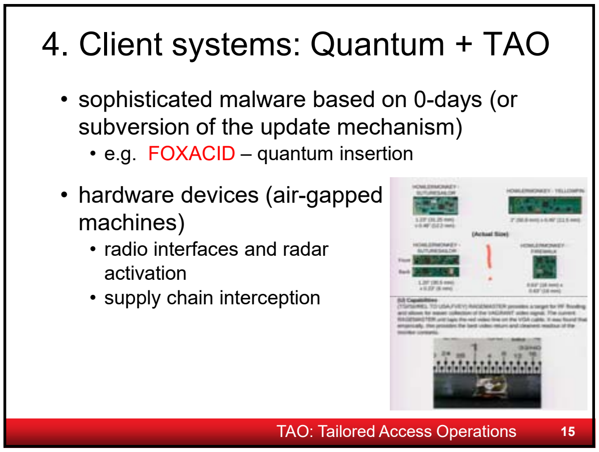
6 June 2013: NSA collecting phone records of millions of Verizon customers daily

- Nov. 2015: USA Freedom act: "Final temporary reauthorization of the Section 215 bulk telephony metadata data program in the US expires"
- Information stored at telcos – can be obtained via FISA court

EU: data retention directive (2006/24/EC)

- April 2014: direct is declared illegal by EU Court of Justice: disproportionate and contrary to some fundamental rights protected by the Charter of Fundamental Rights, in particular to the principle of privacy

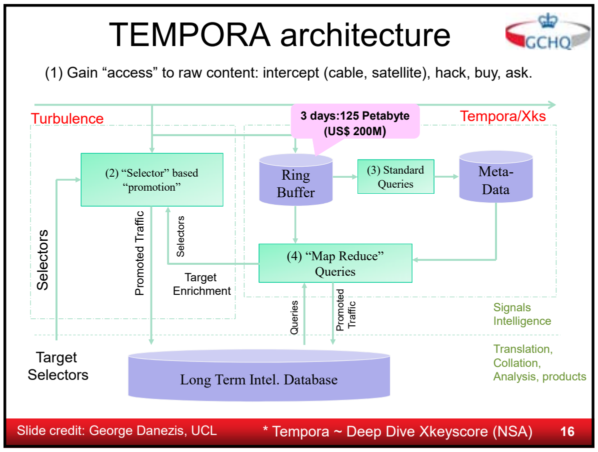
DNR: Dial number recognition 14



4. Client systems: Quantum + TAO

- sophisticated malware based on 0-days (or subversion of the update mechanism)
  - e.g. FOXACID – quantum insertion
- hardware devices (air-gapped machines)
  - radio interfaces and radar activation
  - supply chain interception

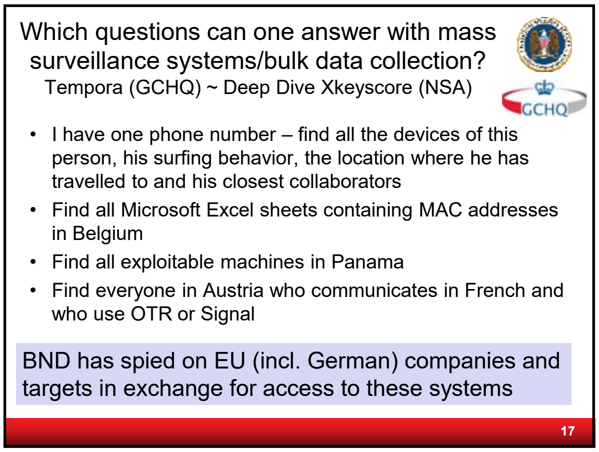
TAO: Tailored Access Operations 15



TEMPORA architecture

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

Slide credit: George Danezis, UCL * Tempora ~ Deep Dive Xkeyscore (NSA) 16



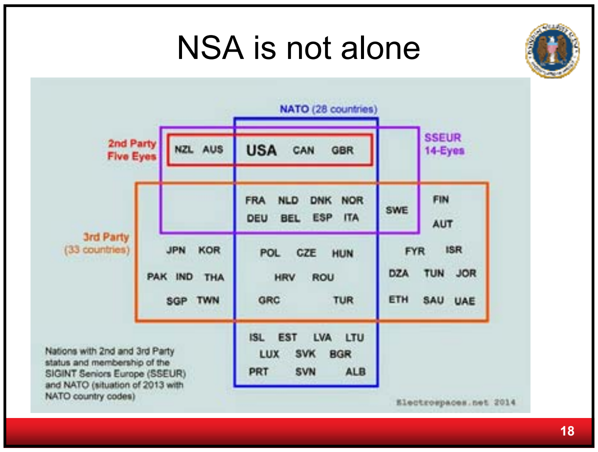
Which questions can one answer with mass surveillance systems/bulk data collection?

Tempora (GCHQ) ~ Deep Dive Xkeyscore (NSA)

- 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 Belgium
- Find all exploitable machines in Panama
- Find everyone in Austria who communicates in French and who use OTR or Signal

BND has spied on EU (incl. German) companies and targets in exchange for access to these systems

17

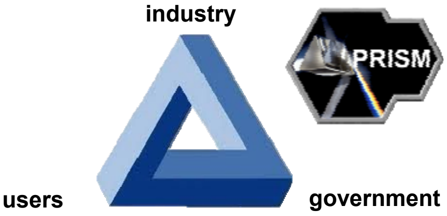


NSA is not alone

Nations with 2nd and 3rd Party status and membership of the SIGINT Seniors Europe (SSEUR) and NATO (situation of 2013 with NATO country codes)

18

If data is the new oil, data mining yields the rocket fuel



Mass Surveillance

panopticon
[Jeremy Bentham, 1791]

discrimination
fear
conformism - stifles dissent
oppression and abuse

Mass Surveillance

Economy of scale

Pervasive surveillance requires pervasive collection and active attacks

- implicates everyone - also innocent bystanders
- emphasis moving from COMSEC to COMPUSEC (from network security to systems security)
- undermines integrity of and trust in computing infrastructure

Human rights do not stop at your border

Outline

- Snowden revelation and mass surveillance
- Going after crypto
- The end of crypto
- Security research

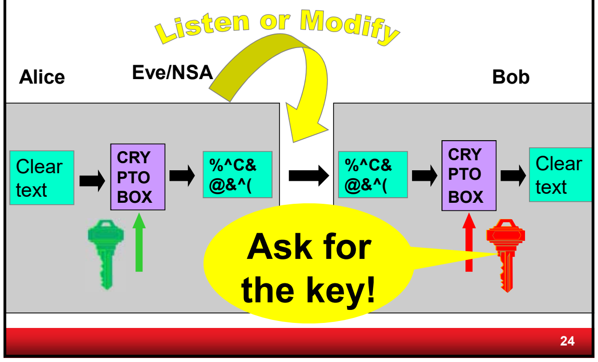
NSA foils much internet encryption

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]

If you can't get the plaintext

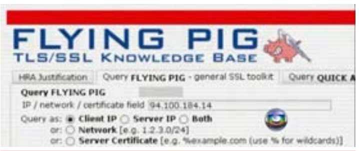


Asking for the key

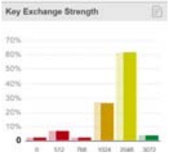
- (alleged) examples – through security letters?
  - Lavabit email encryption
  - CryptoSeal Privacy VPN
  - SSL/TLS servers of large companies?
  - Silent Circle email?
  - Truecrypt??

Find the Private Key (Somehow)

- Logjam: TLS fallback to 512-bit export control legacy systems
- 1024-bit RSA and Diffie-Hellman widely used default option not strong enough
- GCHQ Flying Pig program


FLYING PIG
TLS/SSL KNOWLEDGE BASE

Query FLYING PIG
IP / network / certificate field 94.100.184.14
Query as: ● Client IP ○ Server IP ○ Both
or: ○ Network [e.g. 1.2.3.0/24]
or: ○ Server Certificate [e.g. %example.com (use % for wildcards)]



[Adrian+] Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, CCS 2015

Source: SSL Pulse

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

12M SSL/TLS servers
fake SSL certificates or SSL person-in-the-middle as commercial product or government attack

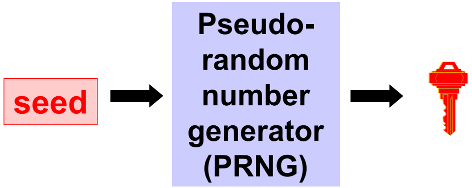
- 650 CA certs trustable by common systems
- Comodo, Diginotar, Turktrust, ANSSI, China Internet Network Information Center (CNNIC), Symantec
- Flame: rogue certificate by cryptanalysis

Let's Encrypt live since November 2015
https://letsencrypt.org/isrg/

[Holz+] TLS in the Wild, NDSS 2016
[Stevens] Counter-cryptanalysis, Crypto'13

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

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

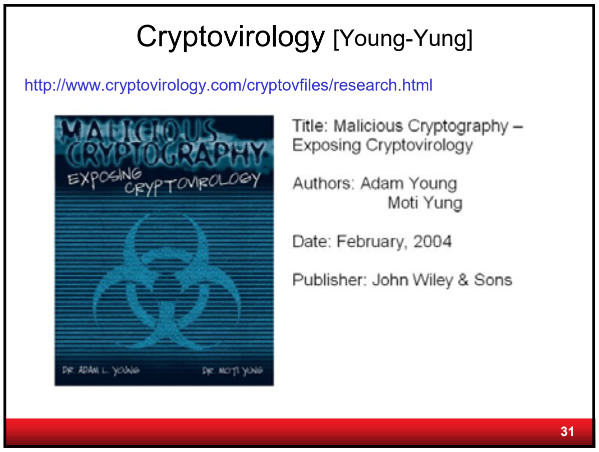
- Two "suspicious" parameters P and Q
- Many warnings and critical comments
  - before publication [Gjøsteen05], [Schoenmakers-Sidorenko06]
  - after publication [Ferguson-Shumov07]

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.

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."
- 16 Sept. 2013: NIST **"strongly recommends" against the use of Dual_EC_DRBG**, as specified in SP 800-90A (2012)
- Nov. 2013: RSA's BSAFE library chooses DUAL_EC as default
- Dec. 2015: Juniper announces Dual_EC problems for Netscreen
  - 08: 6.2.r01 uses Dual_EC in a way it can be exploited
  - 12: someone changed the backdoor (6.2.r015)

[Checkoway+] On the Practical Exploitability of Dual EC in TLS Implementations, Usenix Security 2014
[Checkoway+] A Systematic Analysis of the Juniper Dual EC Incident, Cryptology ePrint Archive, Report 2016/376



Cryptovirology [Young-Yung]

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

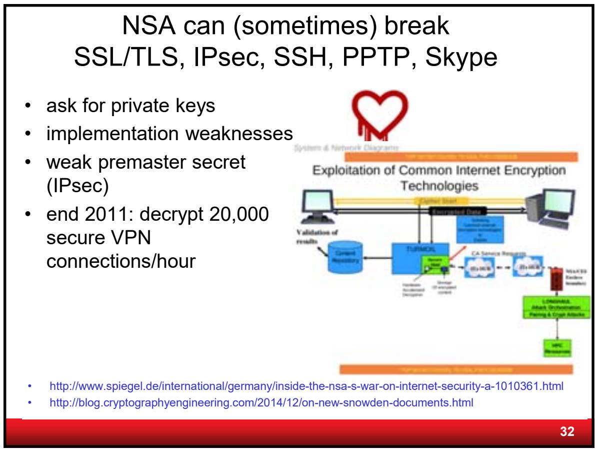
Title: Malicious Cryptography – Exposing Cryptovirology

Authors: Adam Young
Moti Yung

Date: February, 2004

Publisher: John Wiley & Sons

31



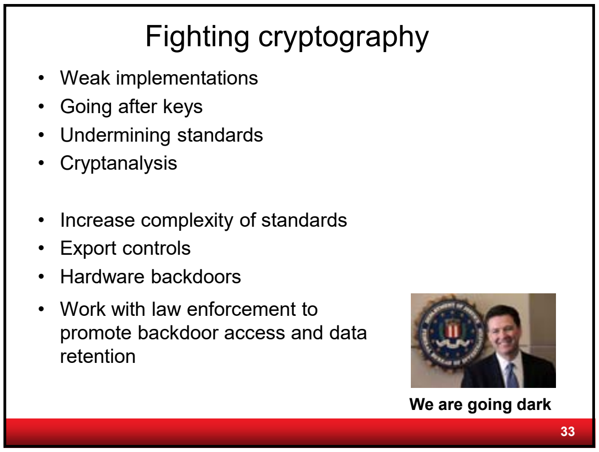
NSA can (sometimes) break SSL/TLS, IPsec, SSH, PPTP, Skype

- ask for private keys
- implementation weaknesses
- weak premaster secret (IPsec)
- end 2011: decrypt 20,000 secure VPN connections/hour

System & Network Diagrams
Exploitation of Common Internet Encryption Technologies
Validation of results
Content Repository
TURMOIL
CA Service Requests
LONGHAUL Attack Orchestration Pairing & Crypt Attacks
HPC Resources

- 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

32



Fighting cryptography

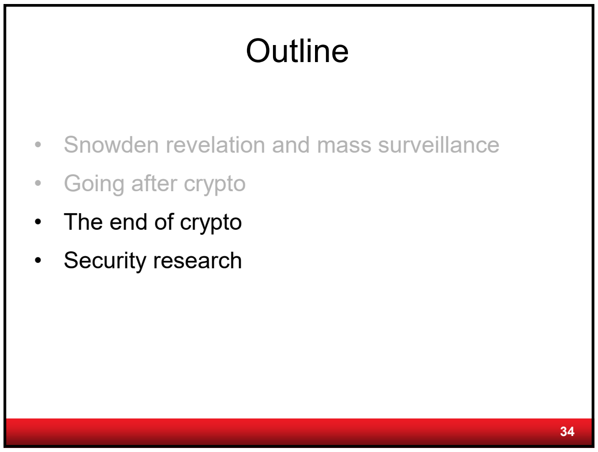
- Weak implementations
- Going after keys
- Undermining standards
- Cryptanalysis

- Increase complexity of standards
- Export controls
- Hardware backdoors

- Work with law enforcement to promote backdoor access and data retention

We are going dark

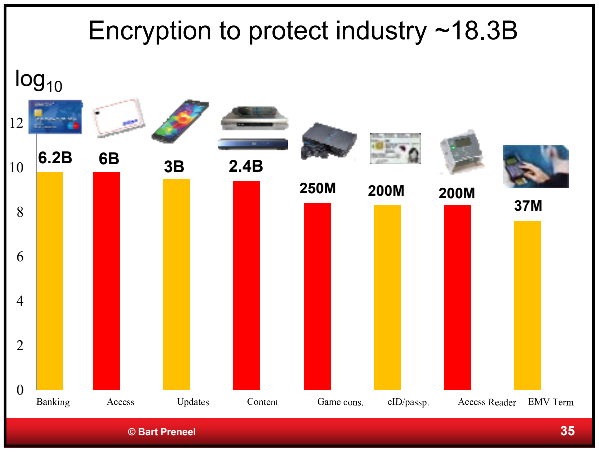
33



Outline

- Snowden revelation and mass surveillance
- Going after crypto
- The end of crypto
- Security research

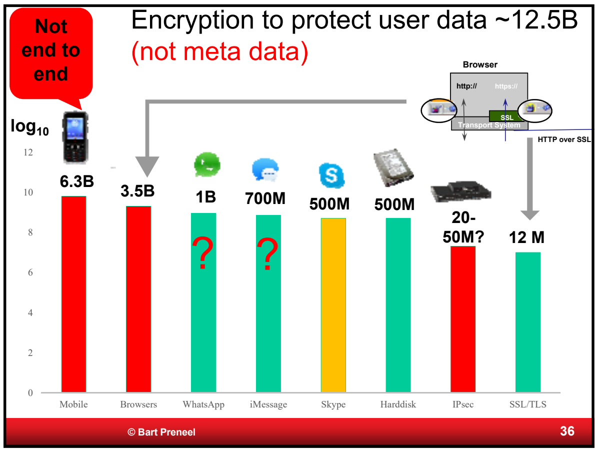
34



Encryption to protect industry ~18.3B

© Bart Preneel

35



Encryption to protect user data ~12.5B (not meta data)

© Bart Preneel

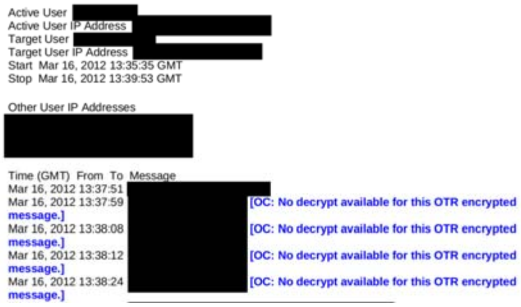
36

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
  - access cards
- confidentiality
  - government/military secrets
  - DRM/content protection
  - telco: not end-to-end or with a backdoor
  - hard disk encryption: backdoored?
  - most data in the cloud is not encrypted
- Metadata: only for the happy few (million)

[Narayan13] What Happened to the Crypto Dream? IEEE Security & Privacy

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]
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 [OC: No decrypt available for this OTR encrypted message.]

Cryptography that seems to work

difficulty decrypting certain types of traffic, including

- Truecrypt
- GPG
- Tor* ("Tor stinks") – likely that a lot of progress is being made
- ZRTP from implementations such as RedPhone (but downgrade problem)

commonalities

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

Outline

- Snowden revelation and mass surveillance
- Going after crypto
- The end of crypto
- Security research

COMSEC - Communication Security

Secure channels: still a challenge

- authenticated encryption studied in CAESAR http://competitions.cr.yp.to/caesar.html
- downgrade attacks
- forward secrecy
- denial of service

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

Or start from scratch: SCION [Perrig+]

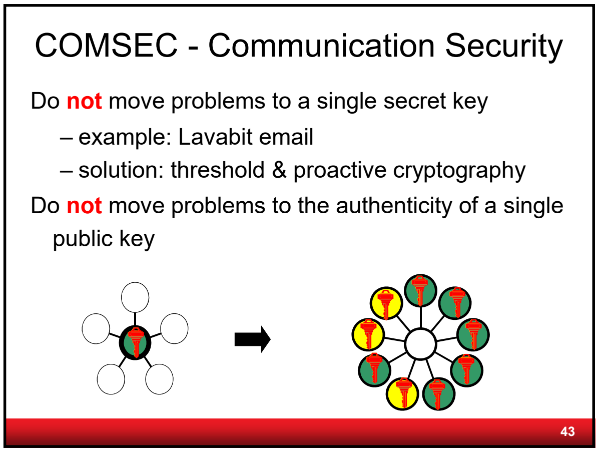
Limited fraction (a few %) of traffic is protected. A very small fraction of traffic is protected end-to-end with a high security level

COMSEC - Communication Security **meta data**

Hiding communicating identities

- few solutions – 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



COMSEC - Communication Security

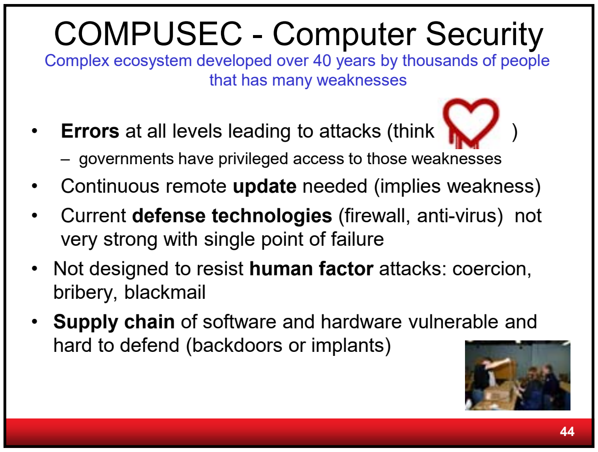
Do **not** move problems to a single secret key

- example: Lavabit email
- solution: threshold & proactive cryptography

Do **not** move problems to the authenticity of a single public key

➡

43

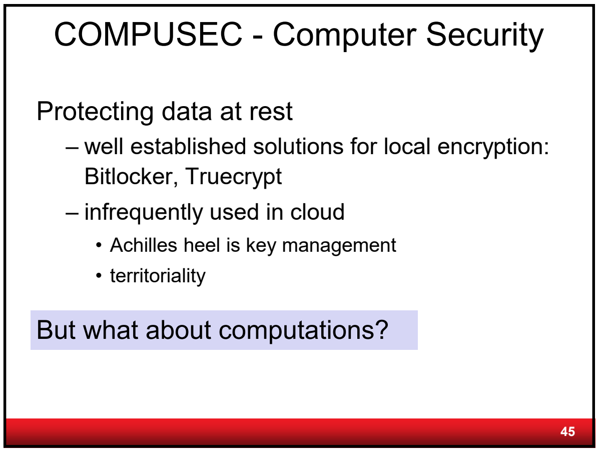


COMPUSEC - Computer Security

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 (implies weakness)
- Current **defense technologies** (firewall, anti-virus) not very strong with single point of failure
- Not designed to resist **human factor** attacks: coercion, bribery, blackmail
- **Supply chain** of software and hardware vulnerable and hard to defend (backdoors or implants)

44



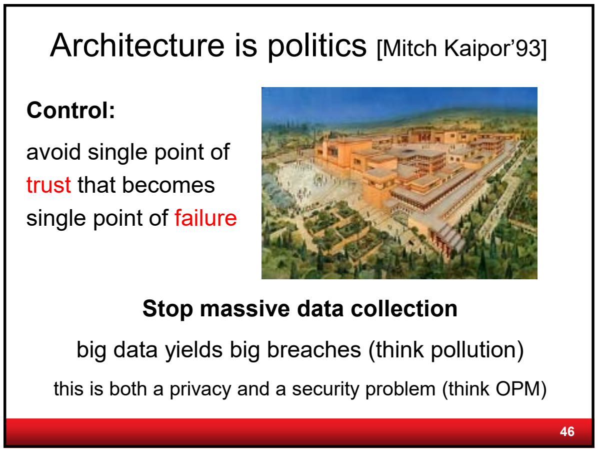
COMPUSEC - Computer Security

Protecting data at rest

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

But what about computations?

45



Architecture is politics [Mitch Kaipor'93]

Control:

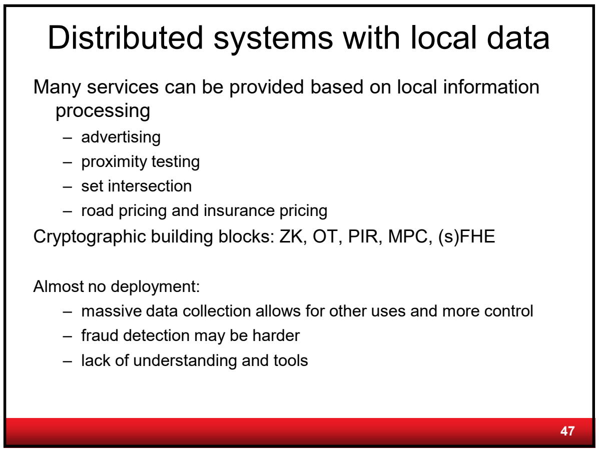
avoid single point of trust that becomes single point of failure

Stop massive data collection

big data yields big breaches (think pollution)

this is both a privacy and a security problem (think OPM)

46



Distributed systems with local data

Many services can be provided based on local information processing

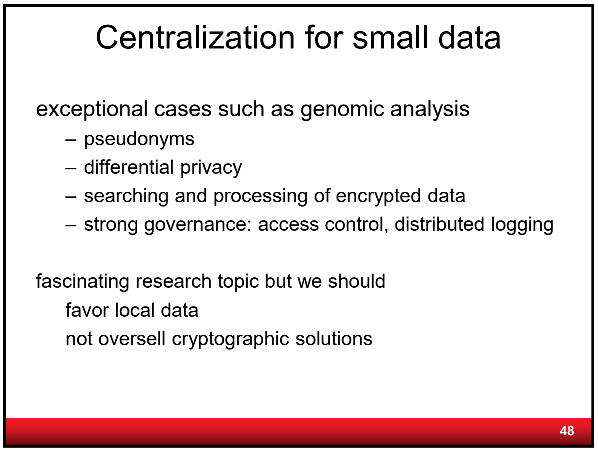
- advertising
- proximity testing
- set intersection
- road pricing and insurance pricing

Cryptographic building blocks: ZK, OT, PIR, MPC, (s)FHE

Almost no deployment:

- massive data collection allows for other uses and more control
- fraud detection may be harder
- lack of understanding and tools

47



Centralization for small data

exceptional cases such as genomic analysis

- pseudonyms
- differential privacy
- searching and processing of encrypted data
- strong governance: access control, distributed logging

fascinating research topic but we should

favor local data

not oversell cryptographic solutions

48

Transparency Open/Free Software and Hardware

Effective governance

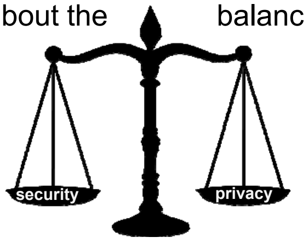
Increased transparency for service providers, privacy for the normal users

Crypto Life Cycle

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

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

What about the balance?



- privacy is a security property: not 0-sum
- privacy is multi-dimensional, e.g. both individual and collective
- intelligence agencies have used technology to tilt the balance
- law enforcement agencies may loose out on some fronts
- can we design better solutions?

http://www.juliansanchez.com/2011/02/04/the-trouble-with-balance-metaphors/

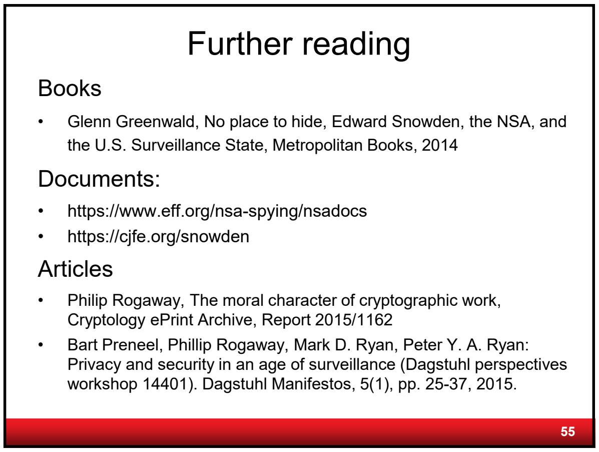
Conclusions

- New threat models
- Shift from network security to system security
- Rethink architectures: distributed
- Help build open technologies and contribute to review by open communities

It's all about choices

Thank you for your attention

"Optimism is a moral duty" [Immanuel Kant]



Further reading

Books

- Glenn Greenwald, No place to hide, Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014

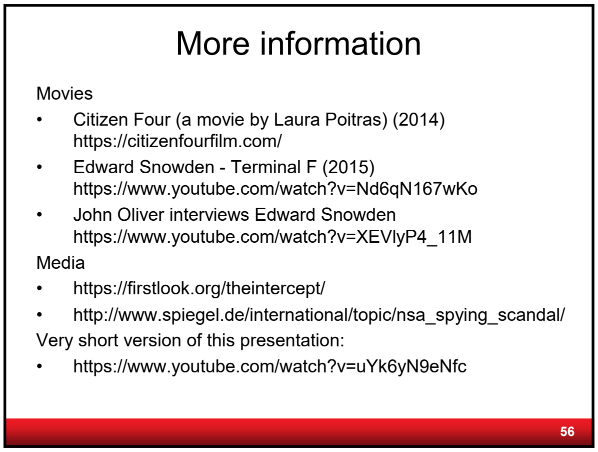
Documents:

- https://www.eff.org/nsa-spying/nsadocs
- https://cjfe.org/snowden

Articles

- Philip Rogaway, The moral character of cryptographic work, Cryptology ePrint Archive, Report 2015/1162
- Bart Preneel, Phillip Rogaway, Mark D. Ryan, Peter Y. A. Ryan: Privacy and security in an age of surveillance (Dagstuhl perspectives workshop 14401). Dagstuhl Manifestos, 5(1), pp. 25-37, 2015.

55



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
- John Oliver interviews Edward Snowden
  https://www.youtube.com/watch?v=XEVlyP4_11M

Media

- https://firstlook.org/theintercept/
- http://www.spiegel.de/international/topic/nsa_spying_scandal/

Very short version of this presentation:

- https://www.youtube.com/watch?v=uYk6yN9eNfc

56