Post-Snowden Cryptography (New Threat Models)

Bart Preneel
imec-COSIC KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
February 2018

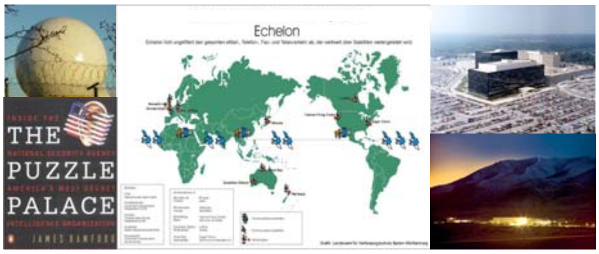
Outline

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

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



TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...

TS//SI//REL to USA, FVEY

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

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

TS//SI//REL to USA, FVEY

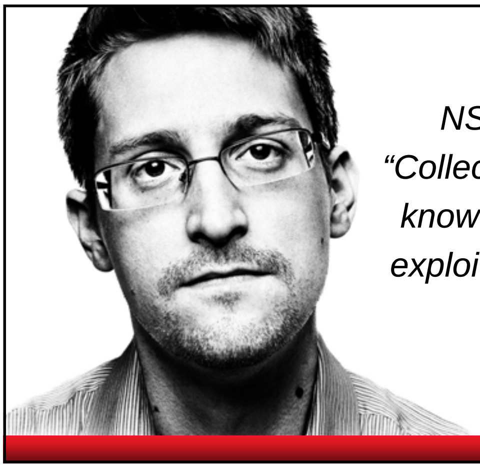
NSA calls the iPhone users public 'zombies' who pay for their own surveillance

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



NSA:

“Collect it all,

know it all,

exploit it all”

www.wired.com

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)

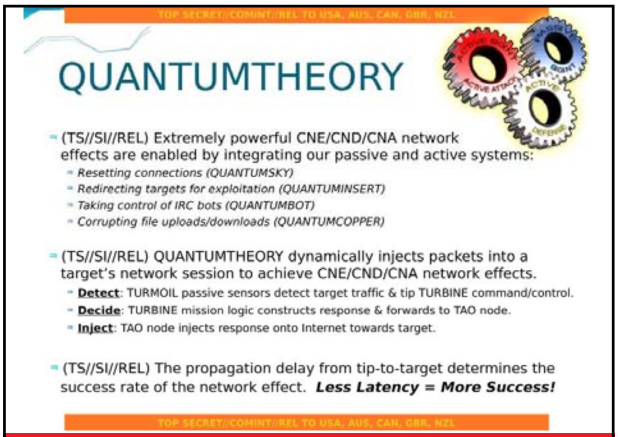
Most spectacular: **active defense**

- 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

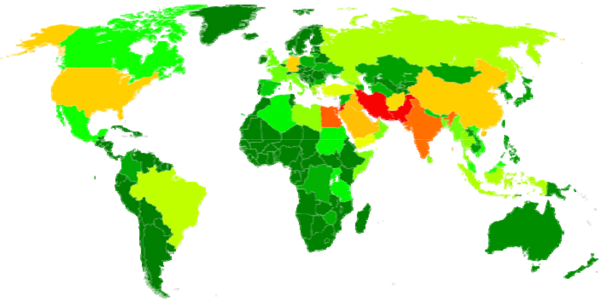
QUANTUMTHEORY

ACTIVE SIGINT
PASSIVE
SIGINT
ACTIVE ATTACK
ACTIVE
DEFENSE

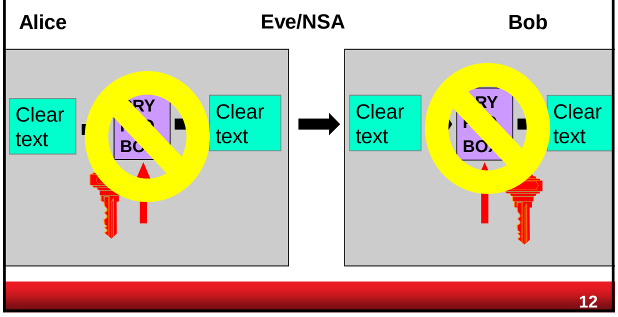
- (TS//SI//REL) Extremely powerful CNE/CND/CNA network effects are enabled by integrating our passive and active systems:
  - *Resetting connections (QUANTUMSKY)*
  - *Redirecting targets for exploitation (QUANTUMINSERT)*
  - *Taking control of IRC bots (QUANTUMBOT)*
  - *Corrupting file uploads/downloads (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

NSA surveillance by country



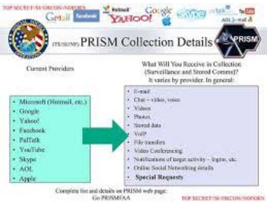
Rule #1 of cryptanalysis: search for plaintext [B. Morris]



Where do you find plaintext?
SSO: Special Source Operations

1. PRISM (server)

2. Upstream (fiber)



TOP SECRET//SI//ORCON//NOFORN

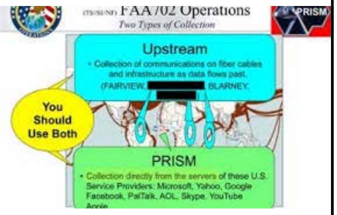
(TS//SI//NF) PRISM Collection Details

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,

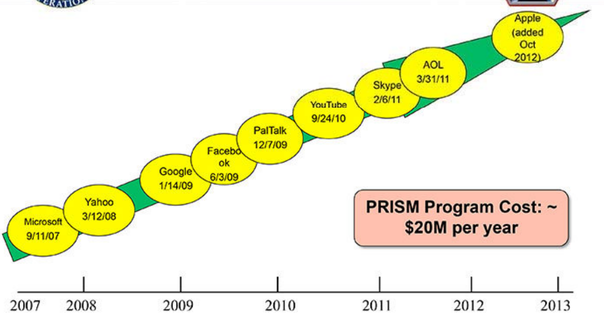
You Should Use Both

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

Tempora

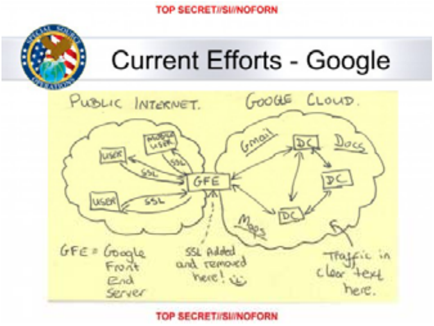
TOP SECRET//SI//ORCON//NOFORN

(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

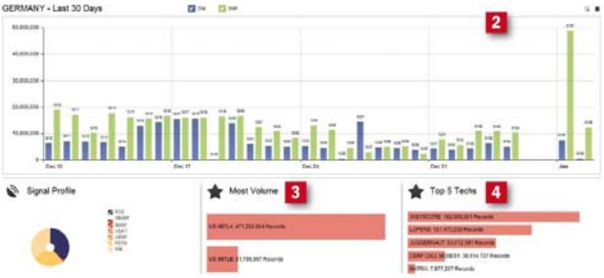
PUBLIC INTERNET.
GOOGLE CLOUD.
USER
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

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)

Germany



Recording all phone calls in the Bahamas and country X metadata in Mexico, Kenya, the Philippines

https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

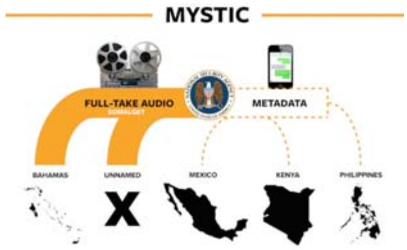
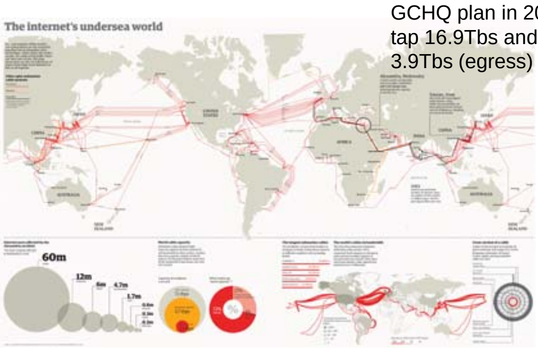


Illustration by Josh Begley

Upstream (continued): 90% of traffic over cables

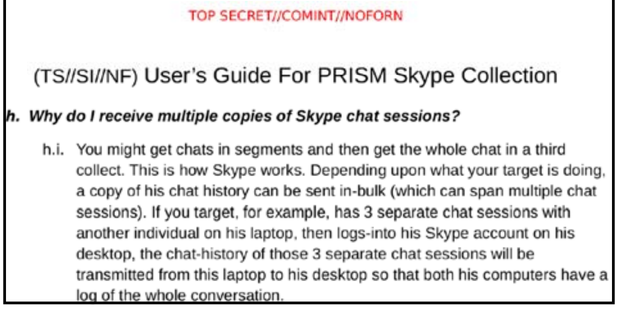
GCHQ plan in 2009: tap 16.9Tbs and select 3.9Tbs (egress) ~20%



Source: The Guardian

NSA has solved Skype messaging problem

May 2011: Microsoft buys Skype for B$ 8.5
Feb. 2011: Skype-in and Skype-out interception (FISC court)
Jun. 2011: Skype peer to peer interception



TOP SECRET//COMINT//NOFORN

(TS//SI//NF) User's Guide For PRISM Skype Collection

h. Why do I receive multiple copies of Skype chat sessions?

h.i. You might get chats in segments and then get the whole chat in a third collect. This is how Skype works. Depending upon what your target is doing, a copy of his chat history can be sent in-bulk (which can span multiple chat sessions). If you target, for example, has 3 separate chat sessions with another individual on his laptop, then logs-into his Skype account on his desktop, the chat-history of those 3 separate chat sessions will be transmitted from this laptop to his desktop so that both his computers have a log of the whole conversation.

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

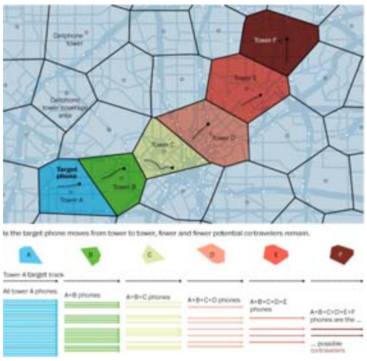
EU: data retention directive (2006/24/EC)

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

http://radiobruxelleslibera.wordpress.com/2014/04/08/the-annulment-of-the-data-retention-directive-and-the-messy-consequences-on-national-legislations/

3. Traffic data (DNR) – phone location

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


Cellphone tower
Cellphone tower coverage area
Tower F
Tower E
Tower D
Tower C
Target phone
Tower B
Tower A
As the target phone moves from tower to tower, fewer and fewer potential co-travelers remain.
A
B
C
D
E
F
Tower A target track
All tower A phones
A+B phones
A+B+C phones
A+B+C+D phones
A+B+C+D+E phones
A+B+C+D+E+F phones are the ...
... possible co-travelers

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)

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)

4. Client systems: Quantum and TAO

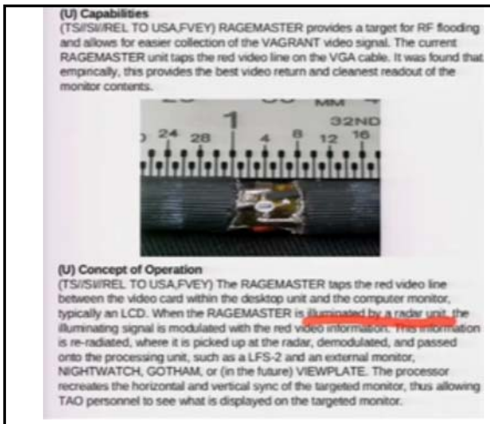
TAO: Tailored Access Operations

- many technologies
- large number on bridging air gaps
- number of targets is limited by cost/effort

HOWLERMONKEY - SUTURESAILOR
1.23" (31.25 mm) x 0.48" (12.2 mm)
HOWLERMONKEY - YELLOWPIN
2" (50.8 mm) x 0.45" (11.5 mm)
(Actual Size)
HOWLERMONKEY - SUTURESAILOR
Front
Back
1.20" (30.5 mm) x 0.23" (6 mm)
HOWLERMONKEY - FIREWALK
0.63" (16 mm) x 0.63" (16 mm)

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



(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.

MM
1
32ND
24
28
4
8
12
16

(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.

Supply chain interception

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Names and definitions of leaked CIA hacking tools

Posted Mar 9, 2017 by Devin Coldewey

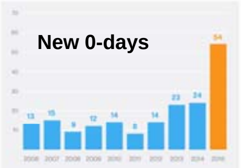
THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities

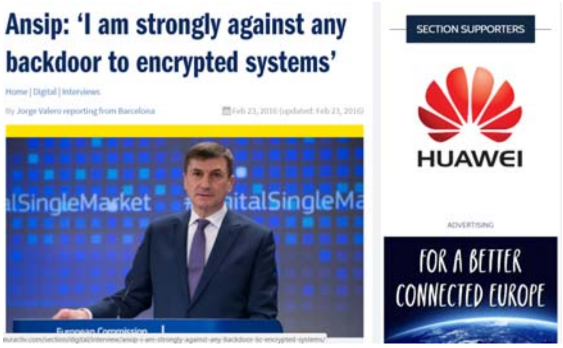
(Part of) government seems to prefer offense over defense

How many 0-days do the NSA, FBI and CIA have?
Are they revealed to vendors?
If so when?

0-days stolen by Shadow brokers from Equation Group resulting in Wannacry and Petya



New 0-days



Ansip: ‘I am strongly against any backdoor to encrypted systems’

Home | Digital | Interviews

By Jorge Valero reporting from Barcelona

Feb 23, 2016 (updated: Feb 23, 2016)

euractiv.com/section/digital/interview/ansip-i-am-strongly-against-any-backdoor-to-encrypted-systems/

EU COM(2017)608

towards an effective and genuine Security Union

encryption will not be "prohibited, limited or weakened"

"measures should not have an impact on a larger or indiscriminate number of people".

more collaboration

96 (or 19?) extra people for Europol

encourages the countries to collaborate in developing a toolbox with alternative investigation techniques

Key search machines? 0-days? Malware

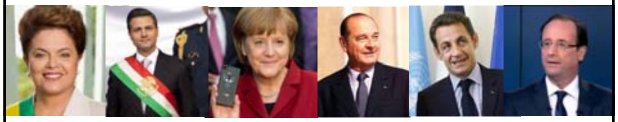
We need a Digital Geneva Convention

Microsoft President Brad Smith:

"Nation states are hacking civilians in peace time"

…and more

Spying on



Fourth order spying (hack South Korea implant to spy on North Korea) …and even fifth order [01/15]

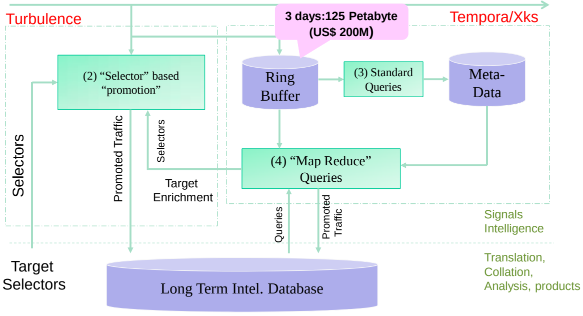
BND helps NSA spying on EU politicians and companies [04/15]

Hacking anti-virus companies [06/15]

GCHQ spying on human rights groups [06/15]

TEMPORA architecture

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



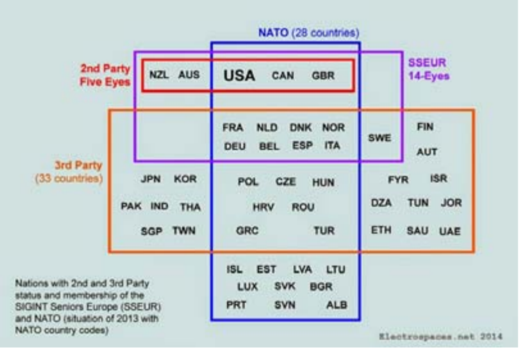
Slide credit: George Danezis, UCL

* Tempora ~ Deep Dive Xkeyscore (NSA)

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 Belgium
- Find all exploitable machines in Panama
- Find everyone in France who communicates in German and who uses Signal

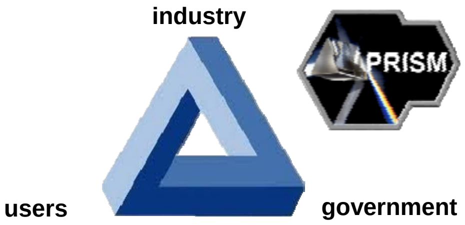
NSA is not alone



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

Surveillance spillout

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

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

Outline

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

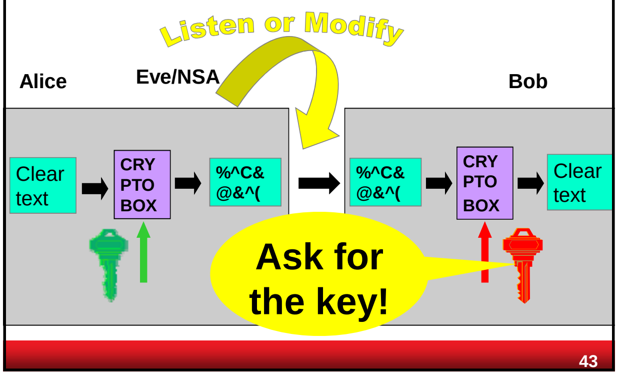
NSA foils much internet encryption

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

- national security letters?
  - exist since the 1980s
  - come with gag orders; a handful revealed
  - 300.000 issued since 2001

  - Lavabit email encryption
  - Yahoo https://www.wired.com/2016/06/yahoo-publishes-national-security-letters-fbi-drops-gag-orders/
  - Silent Circle email?
  - CryptoSeal Privacy VPN
  - SSL/TLS servers of large companies?
  - Truecrypt??

TLS and forward secrecy

Hack the server or ask for it with a security letter

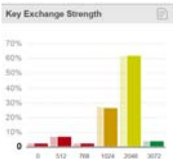
Solution: replace RSA by Diffie-Hellman (D-H) for perfect forward secrecy

- long term private key is only used for signing
- ephemeral D-H keys for confidentiality

D-H downgrade attack [Adrian+15, CCS]

- downgrade to 512-bit export control (legacy)
- cryptanalyze ephemeral D-H keys in real time
- even 1024-bit keys (widely used default option) not strong enough

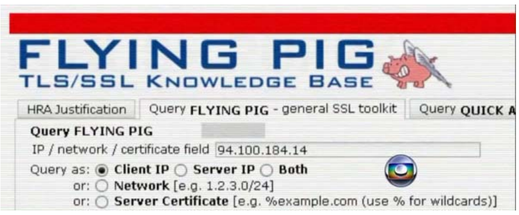
Same attack applies to large fraction of IPsec servers



Source: SSL Pulse

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

SSL/TLS keys: GCHQ Flying Pig


FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query FLYING PIG - general SSL toolkit | Query QUICK A

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)]

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

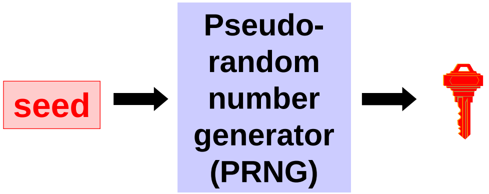
- 650 CA certs trustable by common systems
- Comodo, Diginotar, Turktrust, ANSSI, China Internet Network Information Center (CNNIC), Symantec
- Flame: rogue certificate by cryptanalysis

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

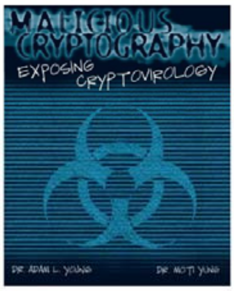
- 1 of the 4 PRNGs in NIST SP 800-90A
  - draft Dec. 2005; published 2006; revised 2012
- Many warnings and critical comments
- Implemented by major players
- Deployed in Juniper ScreenOS 6.2.r015-r018 and 6.3.r017-r020
  - first not a threat but activated by combination of bugs
  - backdoor was replaced by someone

On the Practical Exploitability of Dual EC in TLS Implementations
S. Checkoway, M. Fredrikson, T. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D.J. Bernstein, J. Maskiewicz, H. Shacham, Usenix Security 2014

A Systematic Analysis of the Juniper Dual EC Incident
S. Checkoway, J. Maskiewicz, C. Garman, J.Fried, S. Cohney, M. Green, N. Heninger, R.-P. Weinmann, E. Rescorla, H. Shacham, CCS 2016

Cryptovirology [Young-Yung]

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



Title: Malicious Cryptography – Exposing Cryptovirology

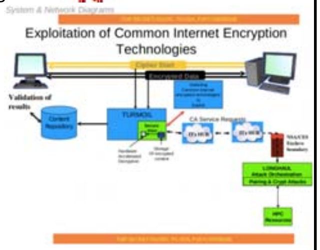
Authors: Adam Young
Moti Yung

Date: February, 2004

Publisher: John Wiley & Sons

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

Fighting cryptography

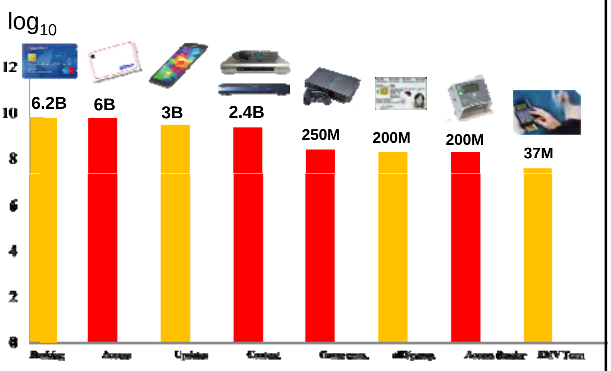
- Weak implementations
- Going after keys
- Undermining standards
- Cryptanalysis

- Increase complexity of standards
- Export controls
- Hardware backdoors
- Work with law enforcement to promote backdoor access and data retention

Outline

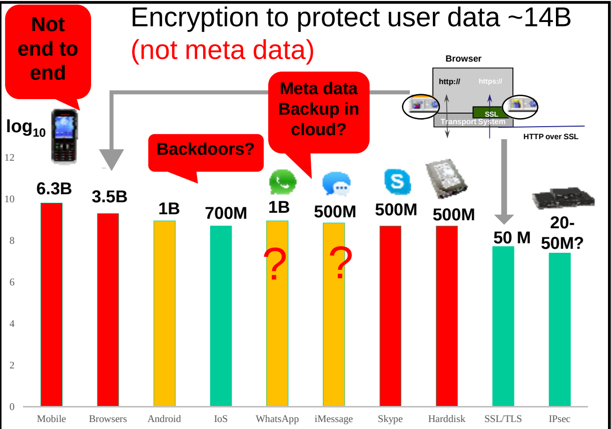
- Snowden revelation: the essentials
- Snowden revelations: some details
- Going after crypto
- Impact on systems research and policy

Encryption to protect industry ~18.3B



© Bart Preneel

Encryption to protect user data ~14B (not meta data)



© Bart Preneel

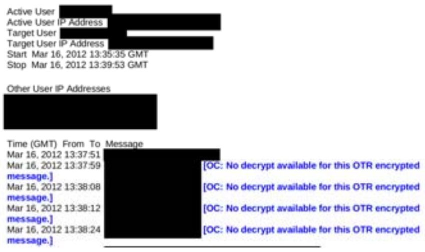
55

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
- confidentiality
  - government/military secrets
  - DRM/content protection
  - ehealth (growing market)
  - telco: not end-to-end or with a backdoor
  - hard disk encryption: backdoored?
  - most data in the cloud is not encrypted

56

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.]

Snowden did not have access to cryptanalytic know-how and documents of NSA (only SIGINT)

57

Cryptography that seems to work

difficulty decrypting certain types of traffic, including

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

commonalities

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

* some Tor traffic can be deanonymized

58

Policy debate

Should we fight this at the technical level?

Or should we argue about liberty, agency, chilling effects and self-censorship, government abuse

59

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

60

COMSEC - Communication Security

Secure channels

- authenticated encryption studied in CAESAR
  http://competitions.cr.yp.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,…

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

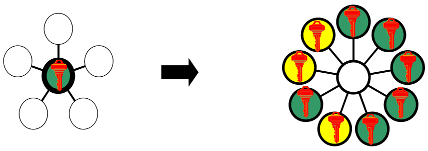
Location privacy: problematic

COMSEC - Communication Security

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

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

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



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)

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?

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

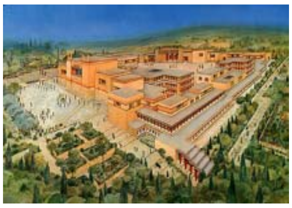
Backdoor insertion

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Architecture is politics [Mitch Kaipor'93]

Control:

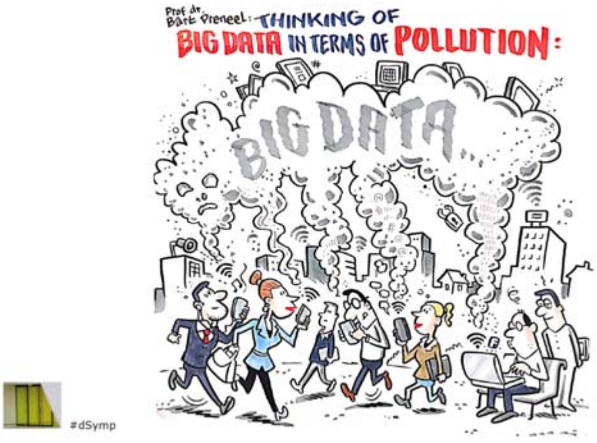
avoid single point of trust that becomes single point of failure



Stop massive data collection

big data yields big breaches (think pollution)

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


Prof. dr. Bart Preneel: THINKING OF BIG DATA IN TERMS OF POLLUTION:
BIG DATA
#dSymp

Governance and Architectures

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

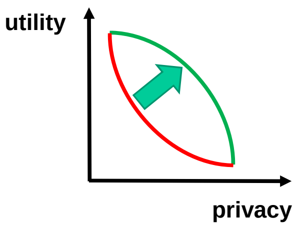
Distributed solutions work

Root keys of some CAs

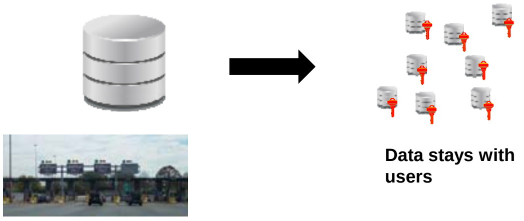
Skype (pre -2011)

Cryptocurrencies

Pushing the tradeoffs



From Big Data to Small Local Data



Distributed systems with local data

Many services can be provided based on local information processing

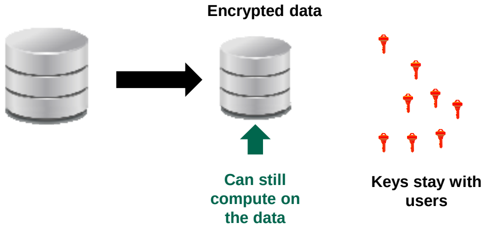
- advertising
- proximity testing
- set intersection
- road pricing and insurance pricing

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

From Big Data to (Small) Encrypted Data



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

Open (Source) Solutions

Effective governance

Transparency for service providers

EU-FOSSA EU Free and Open Source Software Auditing

KISS Principle

Keep It Simple Stupid

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

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

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

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

Very short version of this presentation:

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

Thank You for Your Attention

Industrial policy

to protect sovereignty and human rights

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.

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

Snowden (a movie by Oliver Stone) (2016)

Zero Days (a documentary by Alex Gibney) (2016)

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

The CA Mess on the web

[Eckersley10] “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 adr. 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

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-Shumow07]

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.

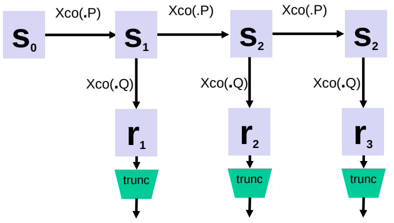
Dual_EC_DRBG

- 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."

- 9 Sept. 2013: NIST **“strongly recommends" against the use of Dual_EC_DRBG**, as specified in SP 800-90A (2012)

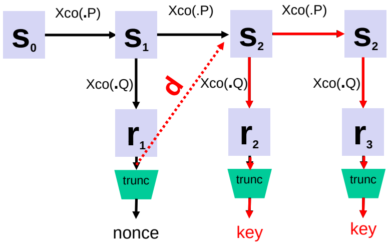
Why was the slowest and least secure of the 4 PRNGs chosen as the default algorithm in BSAFE?

Dual_EC_DRBG: state recovery



S_0 = secret seed
S_i = secret state
P and Q: curve points
Q = **d**. P
Xco() = X-coordinate
trunc(): drop 2 bytes

Dual_EC_DRBG: state recovery



S_0 = secret seed
S_i = secret state
P and Q: curve points
Q = **d**. P
Xco() = X-coordinate
trunc(): drop 2 bytes

Depending on library: key recovery in a few seconds or a few hours

On the Practical Exploitability of Dual EC in TLS Implementations
S. Checkoway, M. Fredrikson, T. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D.J. Bernstein, J. Maskiewicz, H. Shacham, Usenix Security 2014

Dual_EC_DRBG in Juniper

Juniper Security Advisory (17/12/2015), CVE-2015-7755/7756
ScreenOS 6.2.r015-r018 and 6.3.r017-r020
“discovered unauthorized code in the ScreenOS software that powers Netscreen firewalls”

Two backdoors
1. bypass authentication in the SSH and Telnet daemons
2. passive eavesdropper can decrypt VPN traffic

(1) Was inserted on 25 April 2014, 6.3.r017
password was discovered within 6 hours after release of CVE

```
<<< %s(un='%s') = %u
```

Dual_EC_DRBG in Juniper (2)

(2) Passive eavesdropper can decrypt VPN traffic

From the Juniper knowledge base (Oct 2013)

ScreenOS does make use of the Dual_EC_DRBG standard, but is designed to not use Dual_EC_DRBG as its primary random number generator. ScreenOS uses it in a way that should not be vulnerable to the possible issue that has been brought to light. Instead of using the NIST recommended curve points it uses self-generated basis points and then takes the output as an input to FIPS/ANSI X.9.31 PRNG, which is the random number generator used in ScreenOS cryptographic operations.

Dual_EC_DRBG in Juniper (3)

(2) Passive eavesdropper can decrypt VPN traffic

Changes introduced on 20 October 2008 (6.2.r01)

- Add Dual_EC_DRBG but with a different Q
- Add global variables to RNG code
- Output is supposed to be input to a second RNG based on ANSI X9.31, but due to a subtle bug a “for loop” is never executed and there is no post-processing with ANSI X9.31
- RNG produces 32 bytes rather than 20
- Nonce for IKE (IPsec) is increased from 20 to 32 bytes
- Nonces are pre-generated

Dual_EC_DRBG in Juniper (4)

(2) Passive eavesdropper can decrypt VPN traffic

Changes introduced on 12 September 2012 (6.2.r015)

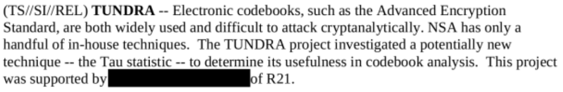
- Q point in Dual_EC_DRBG code is replaced by another point Q’
- Juniper calls this as an “unauthorized patch”

17 December 2015: Juniper patch

- Remove SSH/Telnet backdoor
- Restore Q

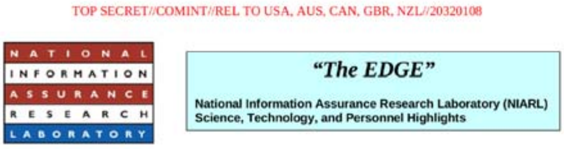
That’s it folks

Can NSA break AES with TUNDRA?



(TS//SI//REL) **TUNDRA** -- Electronic codebooks, such as the Advanced Encryption Standard, are both widely used and difficult to attack cryptanalytically. NSA has only a handful of in-house techniques. The TUNDRA project investigated a potentially new technique -- the Tau statistic -- to determine its usefulness in codebook analysis. This project was supported by [redacted] of R21.

TUNDRA = 2009 undergraduate student project



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

“The EDGE”

National Information Assurance Research Laboratory (NIARL) Science, Technology, and Personnel Highlights

What is privacy?

Context dependent

Conflicts are inherent

Legal approach: trust and consent

Irish privacy commissioner here

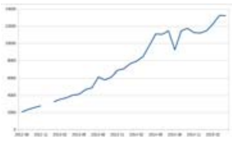
The State of Encryption

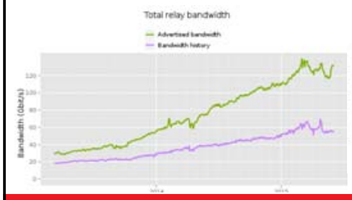
http://www.dailydot.com/politics/encryption-since-snowden-trending-uo/

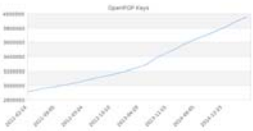
Tails: 13K boots per day (x2)

OpenPGP: 4M public keys (x1.2)

Tor: 7000 relays (x2), 130 Gbps advertised bandwidth (x4)

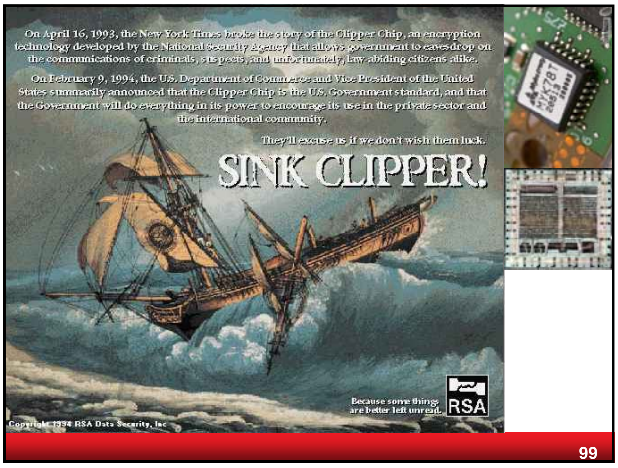






We are going dark

“[I]n our country, do we want to allow a means of communication between people which we cannot read?”



On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

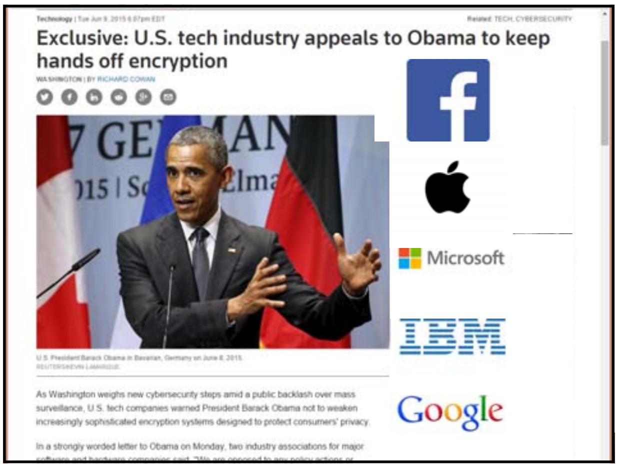
They'll excuse us if we don't wish them luck.

SINK CLIPPER!

Because some things are better left unread.

RSA

Copyright 1994 RSA Data Security, Inc



Technology | Tue Jun 9, 2015 6:07pm EDT

Related: TECH, CYBERSECURITY

Exclusive: U.S. tech industry appeals to Obama to keep hands off encryption

WASHINGTON | BY RICHARD COWAN

U.S. President Barack Obama in Bavarian, Germany on June 8, 2015.
REUTERS/KEVIN LAMARQUE

As Washington weighs new cybersecurity steps amid a public backlash over mass surveillance, U.S. tech companies warned President Barack Obama not to weaken increasingly sophisticated encryption systems designed to protect consumers' privacy.

In a strongly worded letter to Obama on Monday, two industry associations for major software and hardware companies said, "We are opposed to any policy actions or

US government

Exceptional access: four feasible technical solutions have been analyzed

- Physical backdoor to device: special port that exports encrypted output
- Backdoor through automatic update
- Secret sharing technique: backdoor key split
- Forced backup in the cloud

All are feasible but have drawbacks

US academics: “Keys under Doormats”

Exceptional access has many problems

- Add complexity to an ecosystem that is already very complex
  - technologies
  - developers (> 100K app developers)
- Backdoor will be target for bad actors (criminals, terrorists, nation states)
- Incompatible with technologies such as perfect forward secrecy and authenticated encryption
- Jurisdiction: many nations will require exceptional access

Policy decisions

- US: no measures for exceptional access
- NL: no backdoors
- UK:
  - online surveillance bill (aka Snooper's Charter) currently in parliament
  - GCHQ's MIKEY-SAKKE protocol (even standardized by ETSI)
- France: code de la sécurité intérieure approved in May'15

- All 4 countries (and many others) keep hacking
- NSA
  - biggest buyer of 0-days
  - has released more than 91% of them (but it does not say when)

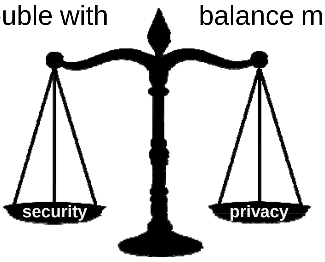
At least some golden keys known … and backdoors abused

vodafone

gemalto
security to be free

Juniper
NETWORKS

The trouble with balance metaphors



- 0-sum while privacy is a security property; loss of privacy may not result in more security
- only way to make a sound decision is unidimensional while privacy is multi-dimensional
- assumes a lot of analytic background work that hasn't actually been done—and conceals the fact that it still needs to be

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