KU LEUVEN

Revisiting Threat Models for Cryptography

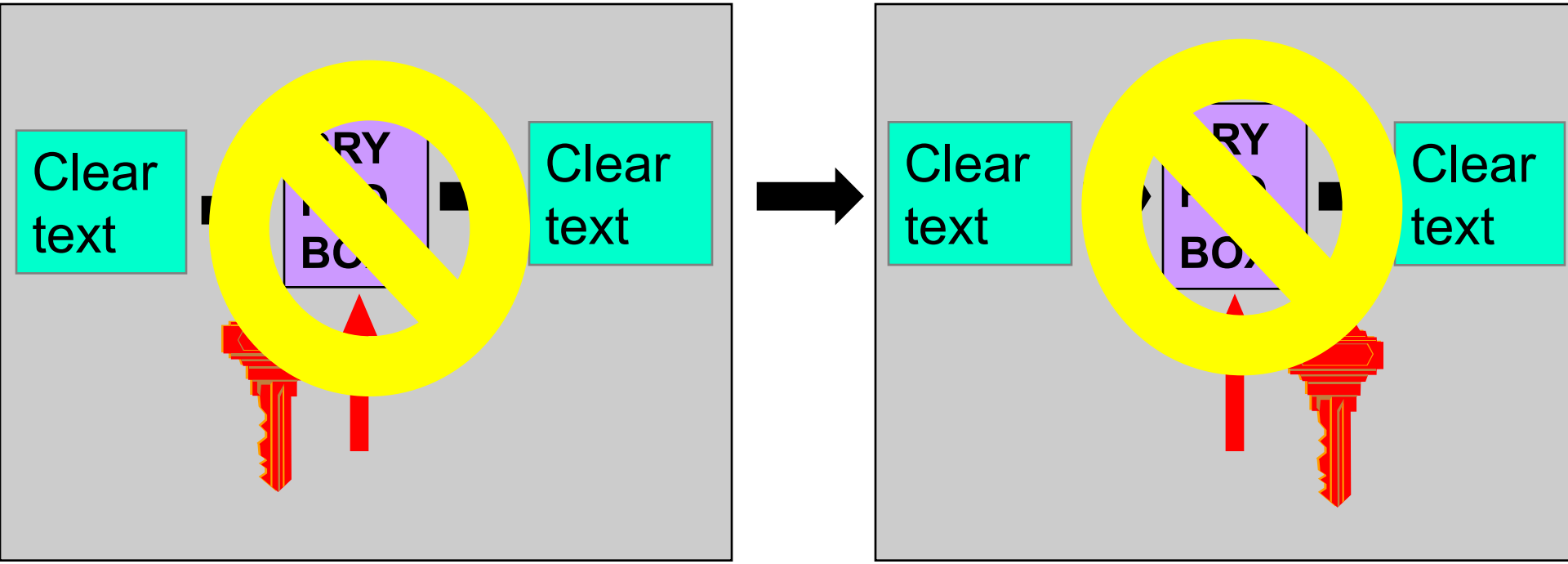
Bart Preneel
imec-COSIC KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
May 2017

Outline

- How nation states go after cryptography
- Undermining end systems
- Deployment of cryptography
- The road ahead

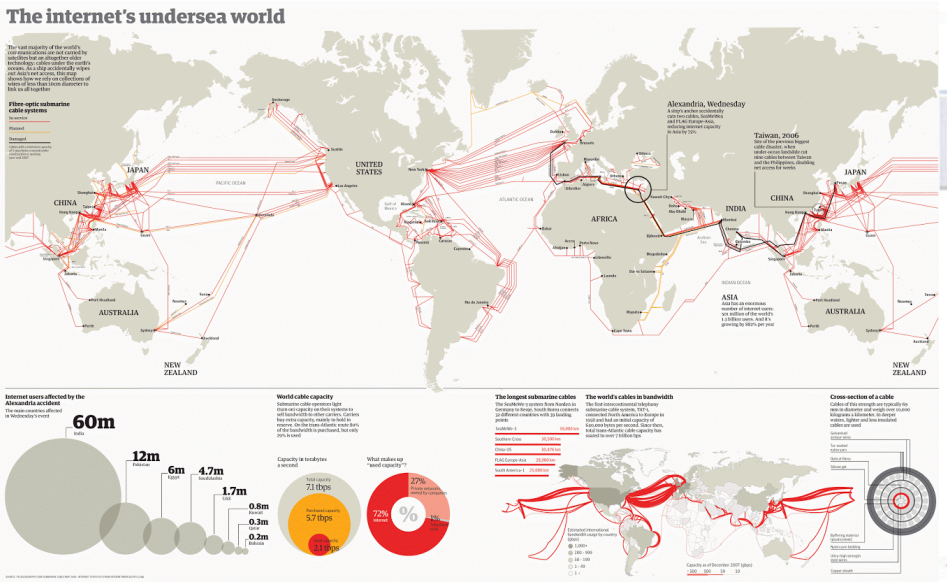
Rule #1 of cryptanalysis: search for plaintext [B. Morris]

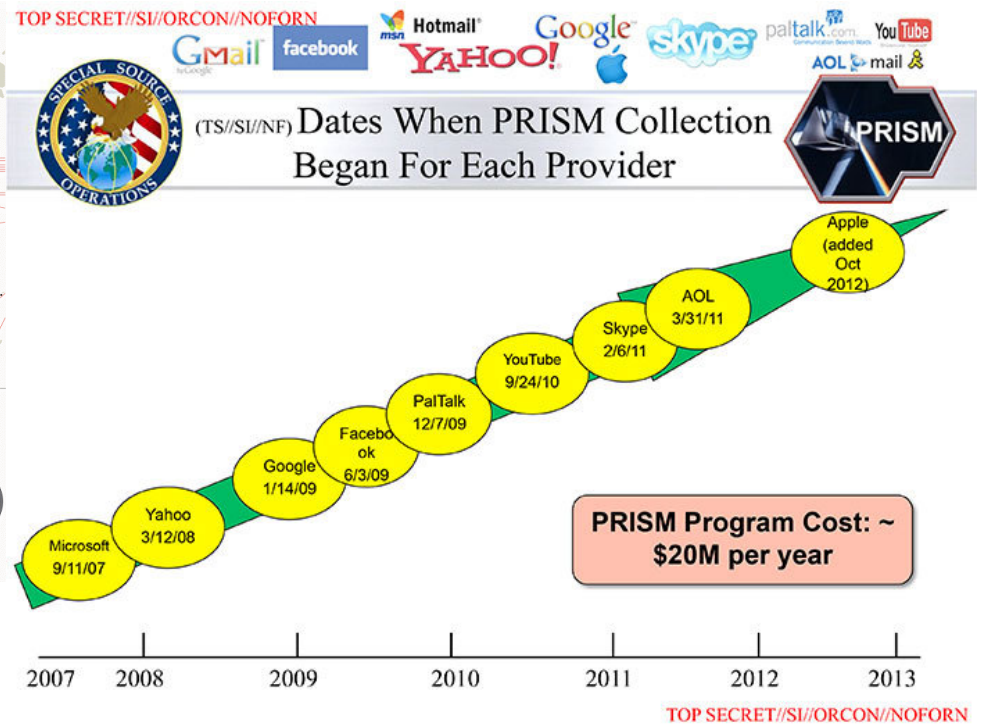
Alice **Eve/NSA** **Bob**



How to get plaintext

- Large scale interception and storage
- Request plaintext from service providers





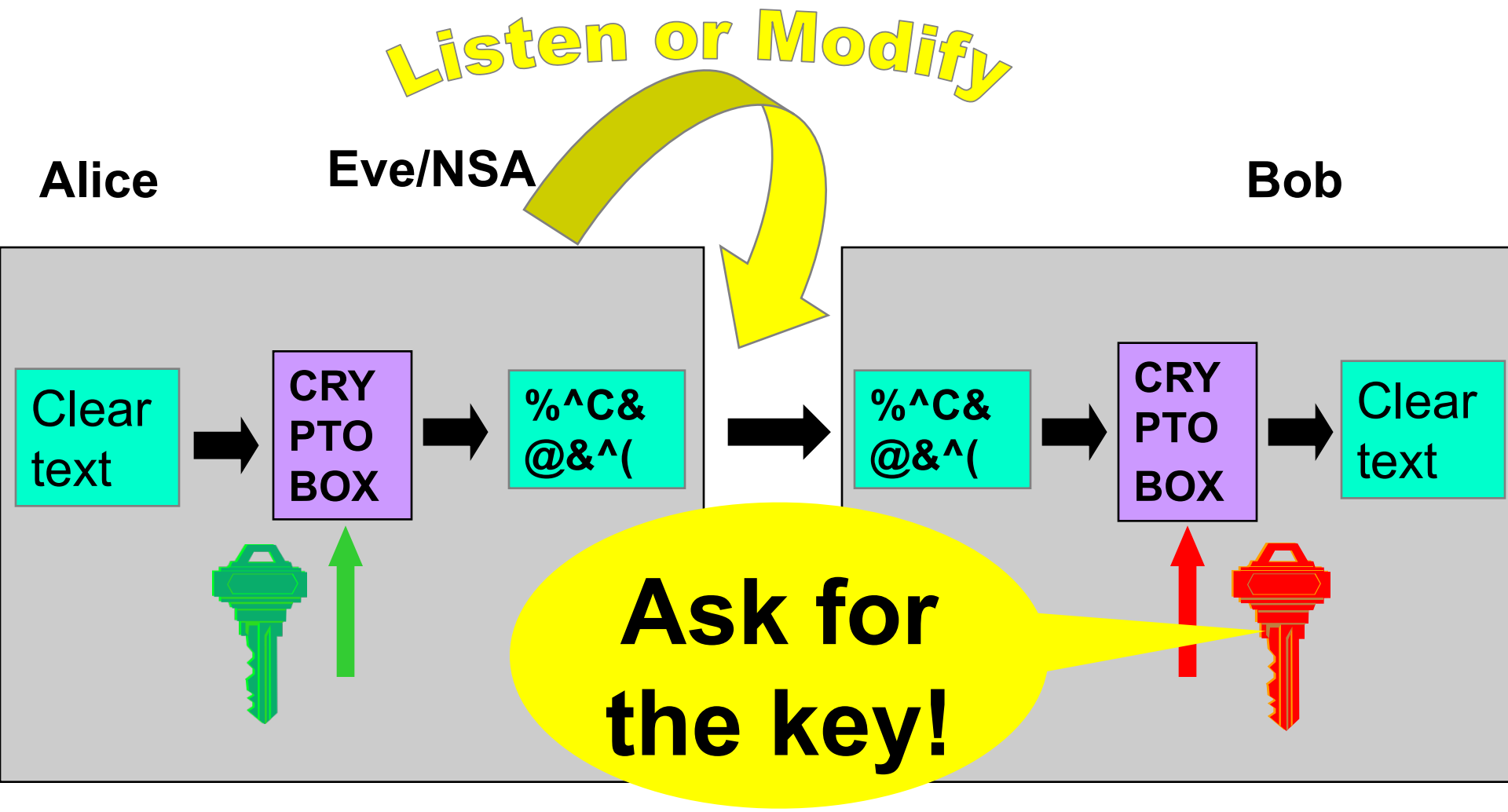
NSA foils much internet encryption

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

Server keys can be obtained in several ways

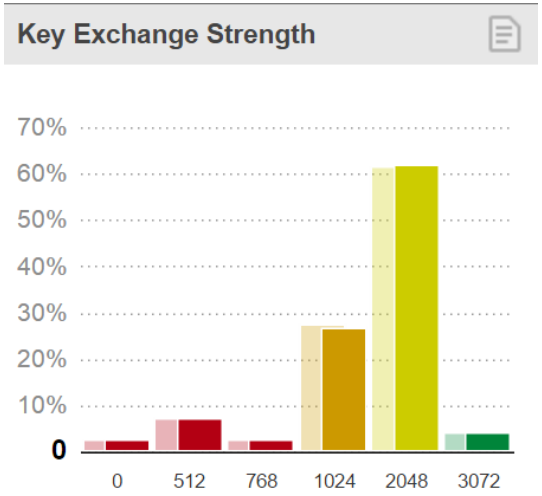
Solution: replace RSA by Diffie-Hellman (D-H) for perfect forward secrecy

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

Logjam (D-H downgrade)

- 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

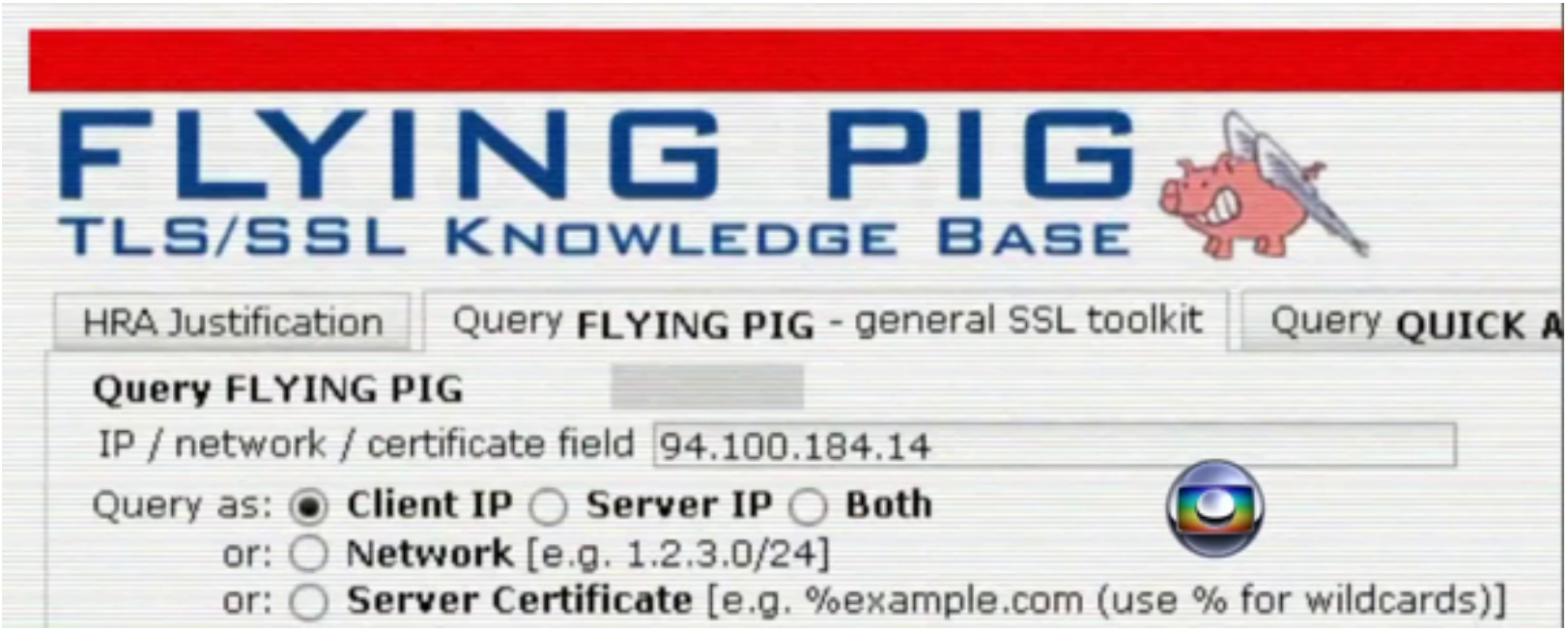
Same attack applies to large fraction of IPsec servers



Source: SSL Pulse

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

SSL/TLS keys: GCHQ Flying Pig



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

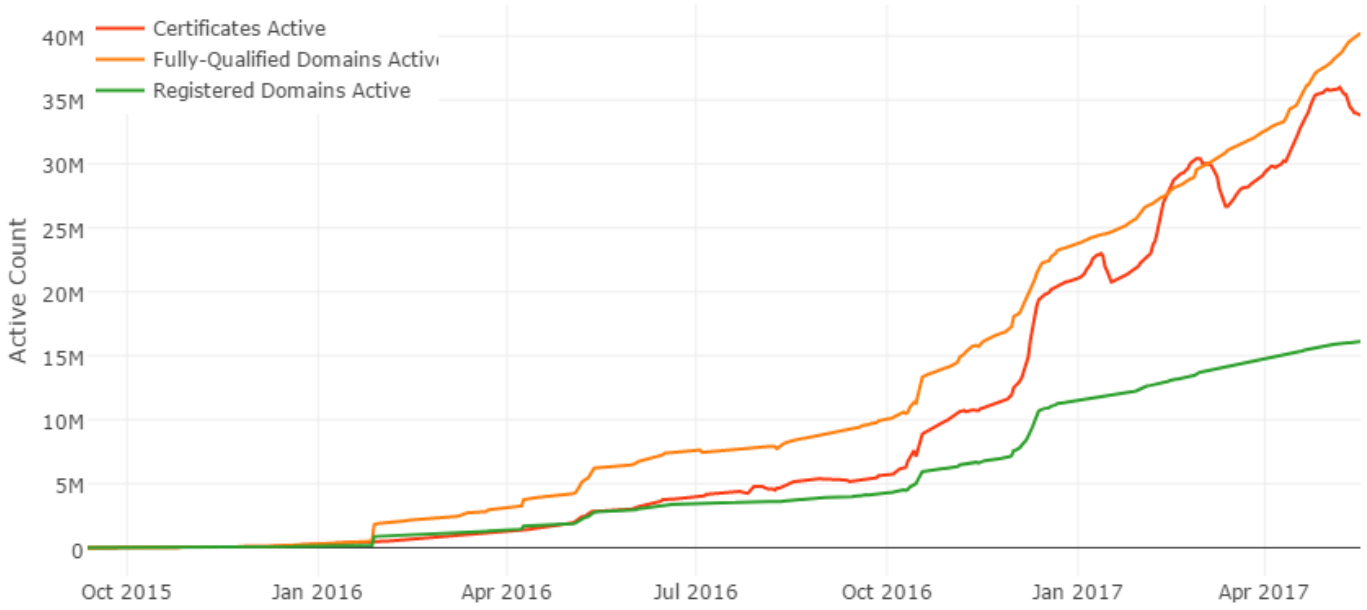
[Holz+] TLS in the Wild, NDSS 2016

[Stevens] Counter-cryptanalysis, Crypto'13

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

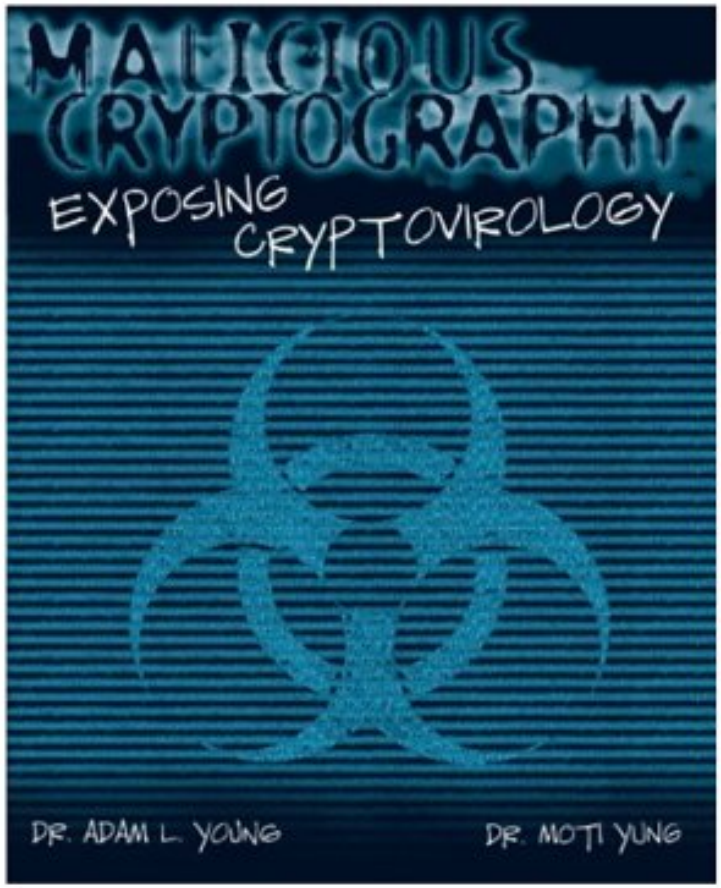
40M SSL/TLS servers

live since November 2015
https://letsencrypt.org/isrg/



If you can't get the key: cryptovirology

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

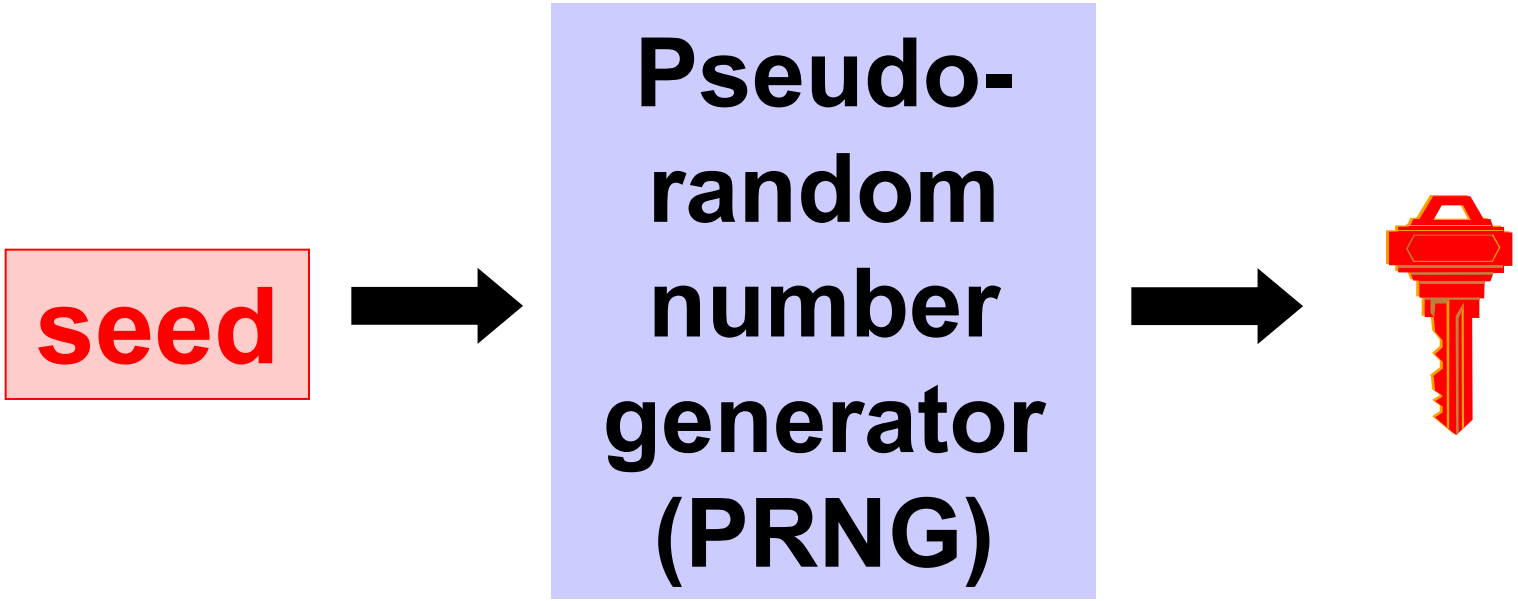


Adam Young, Moti Young, Malicious Cryptography - Exposing Cryptovirology, John Wiley & Sons, February 2004

Research started in 1996

Example: backdoor PRNG

Trapdoor allows to predict keys



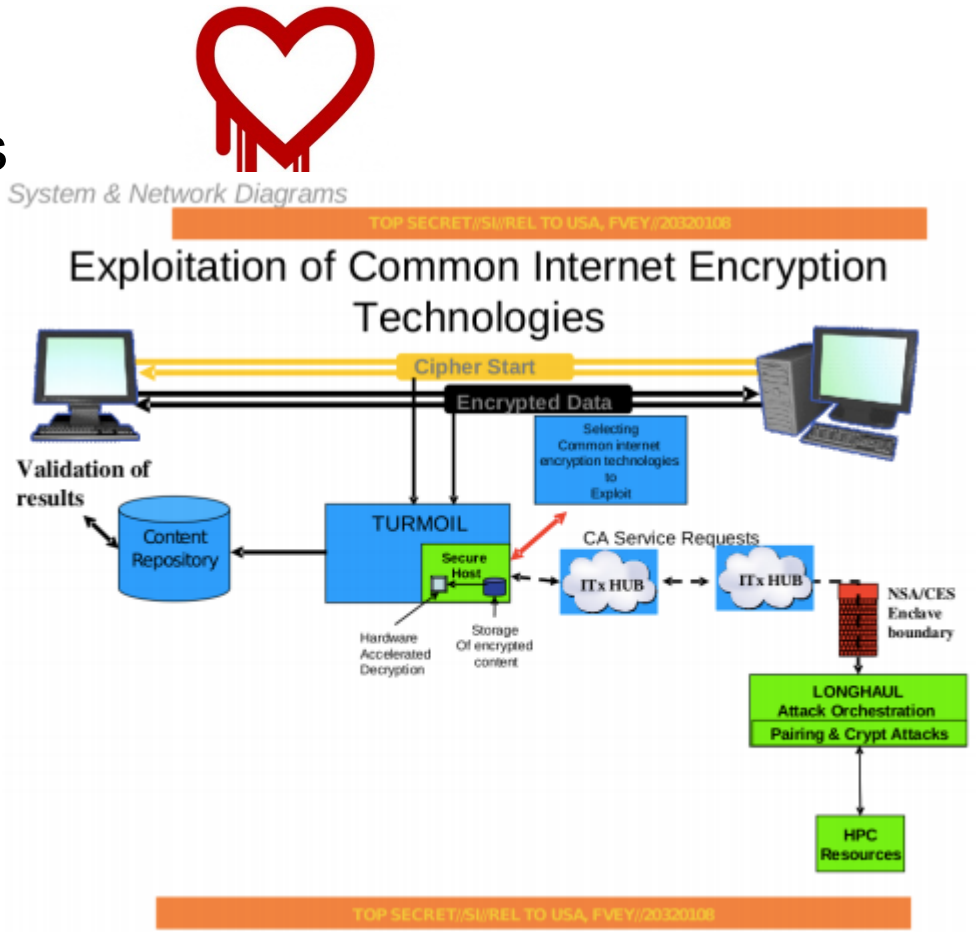
Dual_EC_DRBG

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

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

Outline

- How nation states go after cryptography
- Undermining end systems
- Deployment of cryptography
- The road ahead

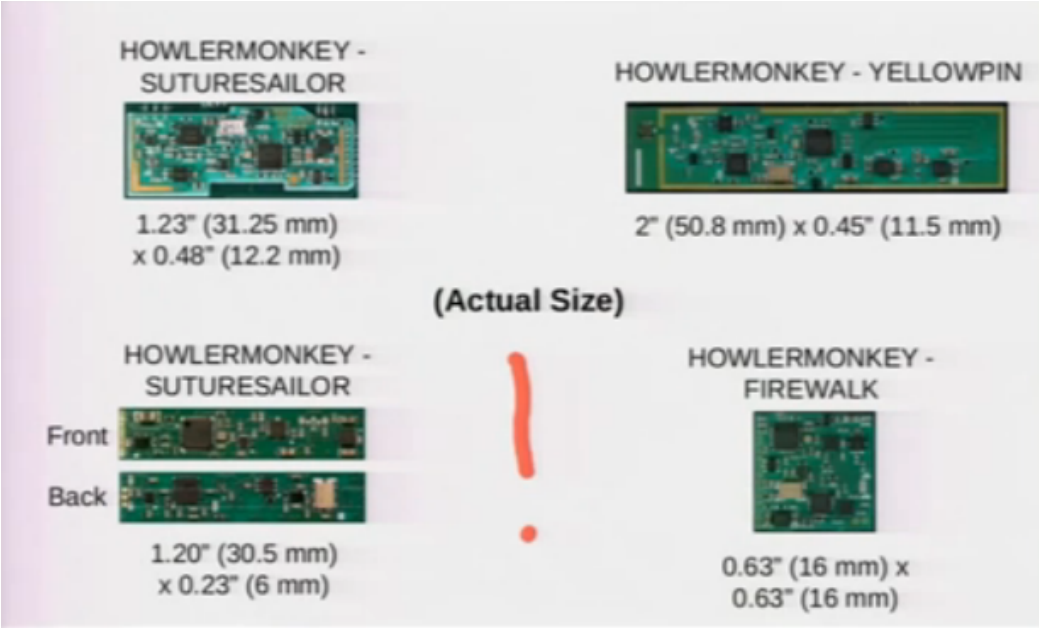
Hardware hacking

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

Hardware hacking

TAO: Tailored Access Operations

- many technologies
- bridging air gaps using wireless
- number of targets is limited by cost/effort

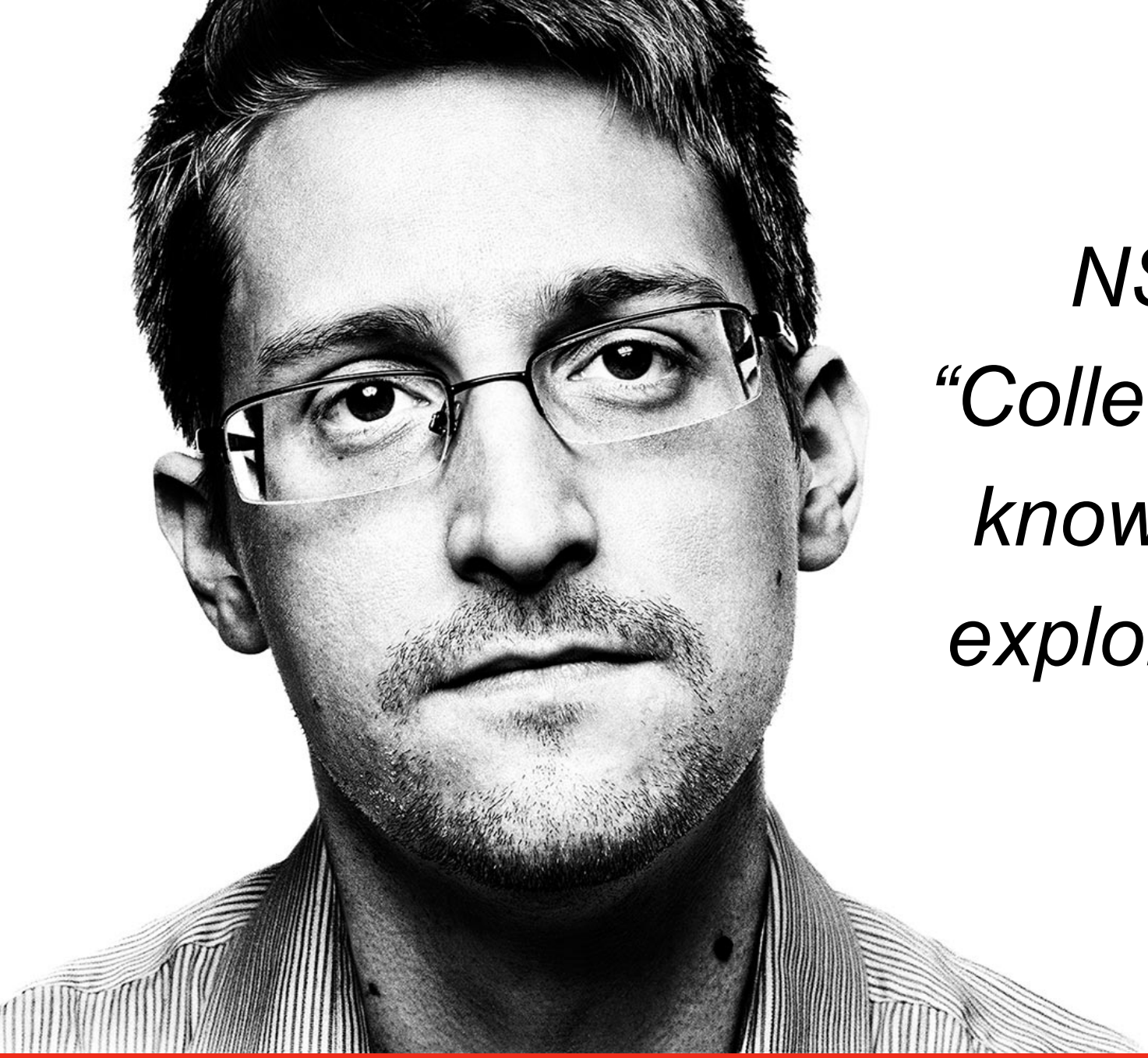


(U) Capabilities

(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.



NSA:

"Collect it all, know it all, exploit it all"

www.wired.com

Names and definitions of leaked CIA hacking tools

Posted Mar 9, 2017 by Devin Coldewey

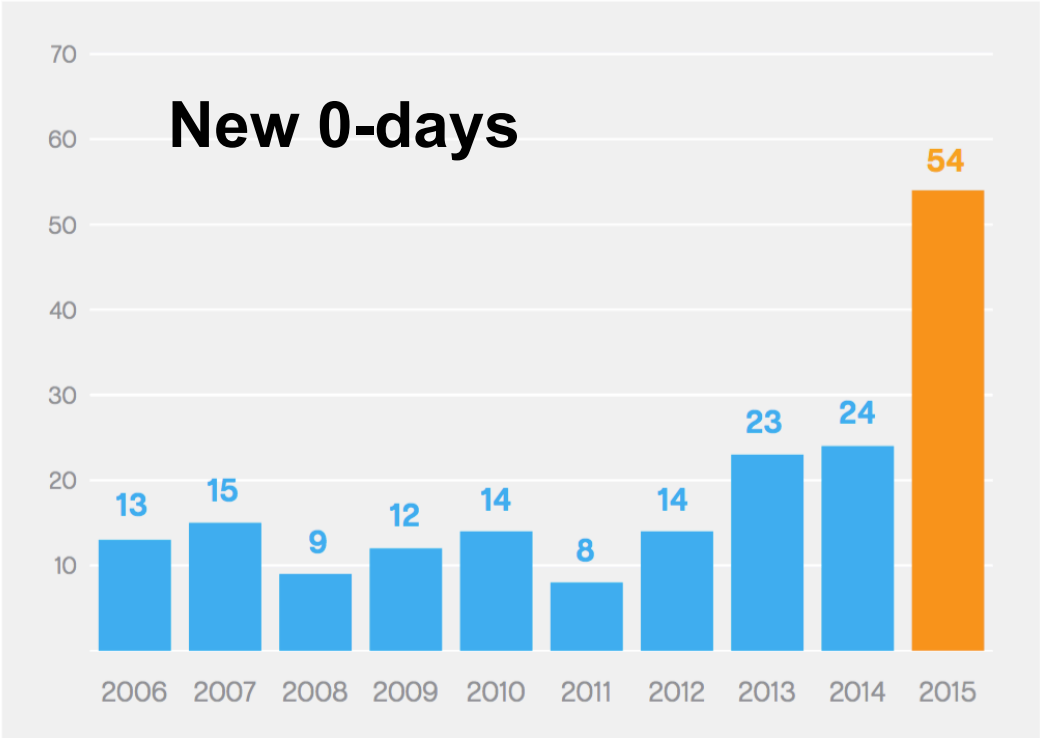
We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities

Offense over defense?

How many 0-days do our governments have?

Are they revealed to vendors?

If so when?



Software hacking

APTs: Aurora, Stuxnet, Regin,…
Quantum insertion: FOXACID
…
EternalBlue
EmeraldThread
EternalChampion
ErraticGopher
EsikmoRoll
EternalRomance
EducatedScholar
EternalSynergy
EclipsedWing

Fighting cryptography

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

- Increase complexity of standards
- Export controls
- Hardware backdoors
- Software 0-days
- Work with law enforcement to promote backdoor access and data retention

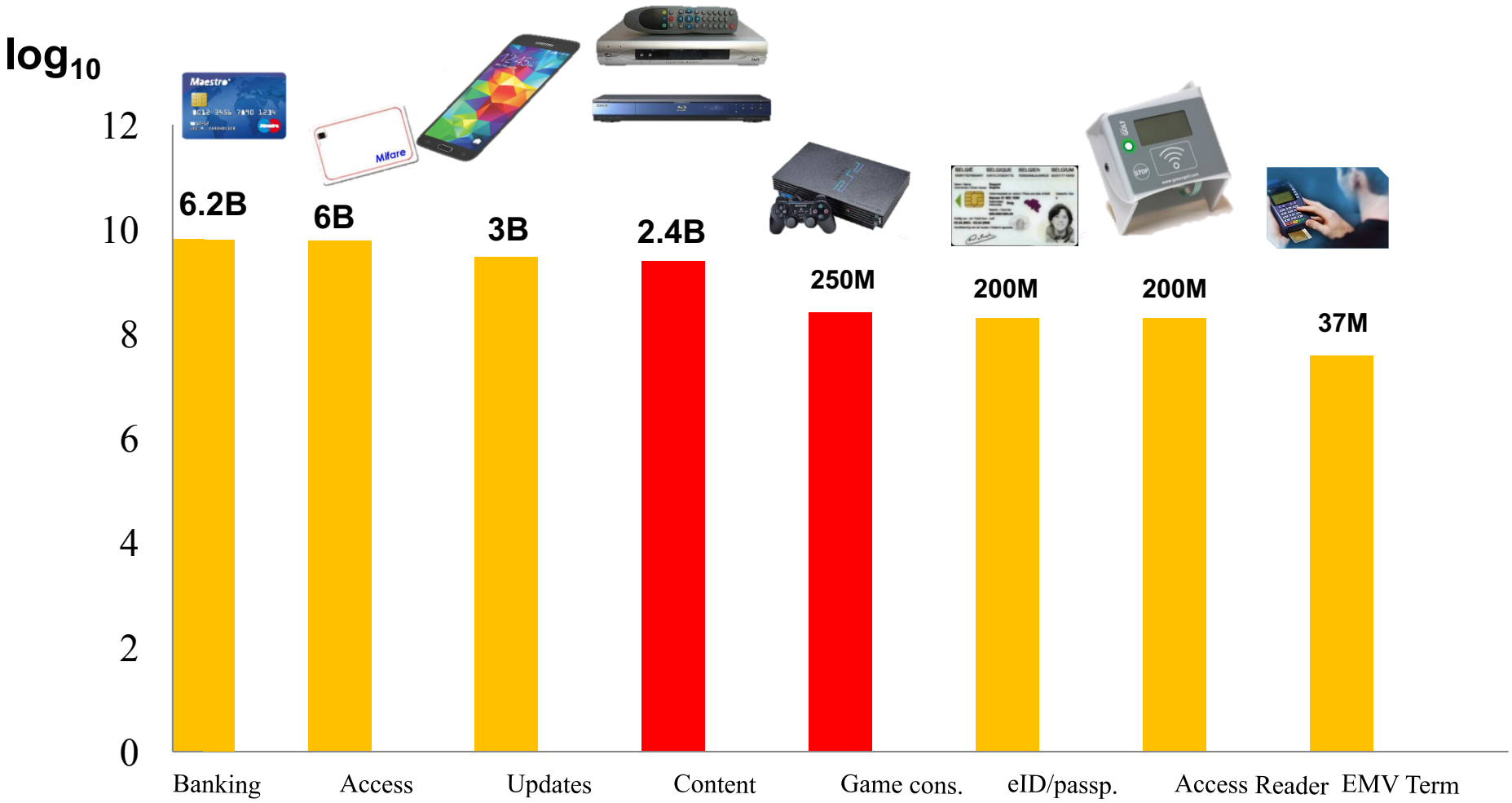
Outline

- How nation states go after cryptography
- Undermining end systems
- Deployment of cryptography
- The road ahead

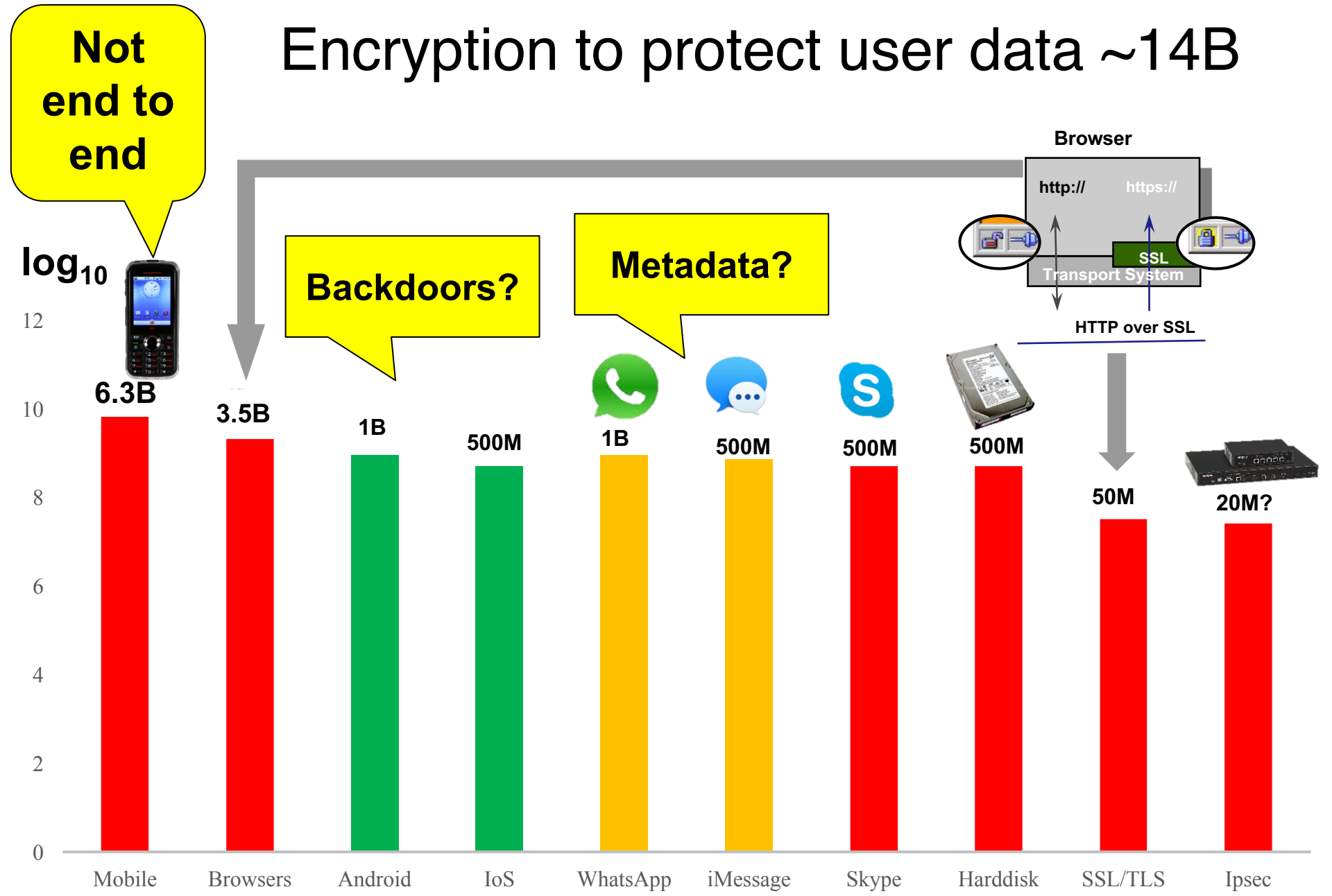
Mozilla reports

- More forward secrecy since November 2013
- By default in TLS 1.3
- Percentage of web pages loaded by Firefox using HTTPS:

Encryption to protect industry ~18.3B



Encryption to protect user data ~14B



COMSEC - Communication Security

Secure channels: still a challenge

- 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,…

Or start from scratch: Gnunet [Grothoff+], SCION [Perrig+]

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

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?

Architecture is politics [Mitch Kaipor'93]

avoid single point of trust that becomes single point of failure

Distributed intelligence is needed for IoT

- Many applications of machine-to-machine communications require latency of milliseconds
- Energy cost of sending everything to the cloud is too high

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

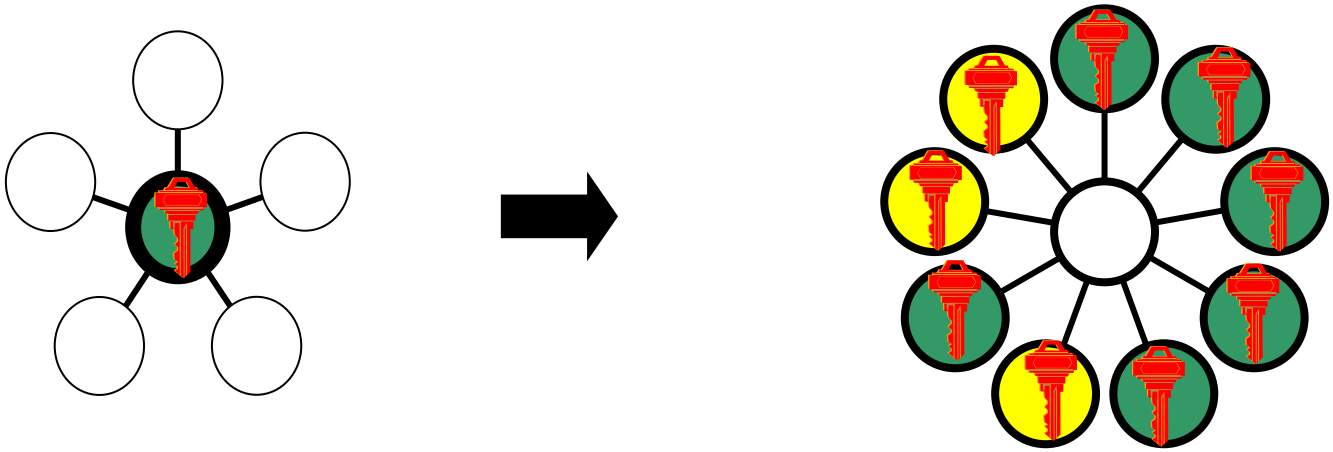
Distributed cryptography

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

Multi-Party Computation (MPC) feasible in many cases



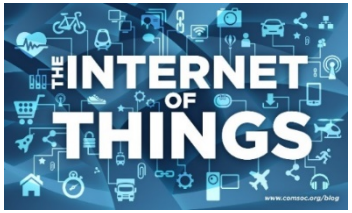
Distributed solutions work

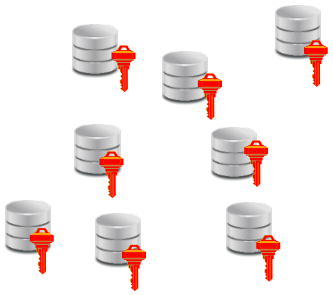
Root keys of some CAs

Skype (pre -2011)

Cryptocurrencies

From Big Data to Small Local Data





Data stays with users

Distributed systems with local data

Many services can be provided based on local information processing

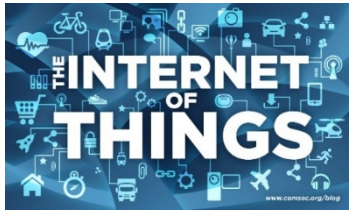
- advertising
- proximity testing
- set intersection
- road pricing and insurance pricing

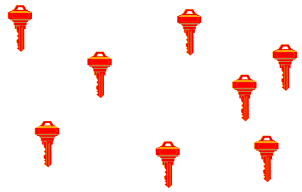
Cryptographic building blocks: ZK, OT, PIR, MPC, (s)FHE

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 Encrypted Data





Local encryption with low multiplication depth

Encrypted data

Can still compute on the data with somewhat Fully Homomorphic Encryption

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

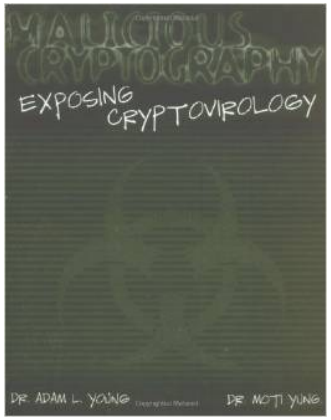
fascinating research topic but we should

favor local data

not oversell cryptographic solutions

Reconsider every stage

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



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

Open (Source) Solutions

Effective governance

Transparency for service providers

EU-FOSSA

EU Free and Open Source Software Auditing

Conclusions

Rethink architectures: distributed

Secure building blocks

Open technologies and review by open communities

Deploy more advanced crypto

We need a Digital Geneva Convention

Microsoft President Brad Smith:

"Nation states are hacking civilians in peace time"