Three decades of cybersecurity policy:
Lessons learned

Bart Preneel
COSIC, KU Leuven
@bpreneel1
22 June 2022

The only thing we learn from history is that we are learning nothing from history [Hegel]

Crypto is creating a problem
I mean cryptography, not cryptocurrencies

Crypto is creating a problem

1987 1989 1991 1994
Free certs - live since November 2015
260 M active certificates
No revocation but certs only valid for 90 days

Options for Law Enforcement (1/4)

• do nothing
• use built-in key escrow (“special access” or “backdoor”)
  • key management feature
  • secret sharing
  • functionality inside device that can be activated locally or remotely

Law Enforcement Access
So 1990s

CALEA [1994]
Communications Assistance for Law Enforcement Act

• Intercept calls or meta data with warrant
• Extended to VoIP (2004)
• EU:
  • Lawful interception:
    • Council Resolution of 17 January 1995
    • Added to 3G standards
  • Data Retention directive 2006/24/EC
    • ECJ declares it invalid for violating fundamental rights (8 April 2014)
    • EU extends data retention to over the top services (2022)
Three decades of cybersecurity policy:
Lessons learned Bart Preneel

France lifted ban on strong encryption in 1999

[2013] Growing gap between law enforcement’s legal authority to conduct electronic surveillance, and its ability to conduct such surveillance

Former FBI Director Robert Mueller

[2014] We are going dark. We aren’t seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process.

Former FBI Director James Comey

“[I]n our country, do we want to allow a means of communication between people which we cannot read?” [Jan 2015]
At the request of the FBI, based on an all writs order (1789), a U.S. federal magistrate judge has ordered Apple to break the security of the iPhone.
Three decades of cybersecurity policy: Lessons learned

Bart Preneel

Court case ends
March 28, 2016 FBI gets access with help of a company at the cost of US$ 900K … yielded almost no useful information

Sept. 2016: Sergei Skorobogatov (Cambridge University) shows that access is feasible with $100 of equipment

Netherlands (2016)


France and Germany push for encryption limits (2016)
Three decades of cybersecurity policy: Lessons learned Bart Preneel

Laws of mathematics 'do not apply' in Australia
Encryption law: 8 December 2018

Australian PM Malcolm Turnbull 16 July 2017

What's needed is "responsible encryption … secure encryption that allows access only with judicial authorization."

Deputy attorney general Rod Rosenstein 9 Nov. 2017

The Law Enforcement argument

• The role of law enforcement is to protect society
• We have always had warrants to get access to information
• Technology should not change this

"Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety."

Three decades of cybersecurity policy:
Lessons learned Bart Preneel

The Law Enforcement argument

• Supporting data limited
• Washington Post, May 22, 2018: locked phones in 2017 << 7800

Encrochat (2020) and Sky ECC (2021)

Which access is needed?

Communications: voice
  • telephony: phone or cell tower
  • VOIP

Communications: data
  • messages
  • meta data

Stored data
  • cloud
  • media (USB)

Devices
  • confiscated
  • remote

The civil society/academic argument

[Keys under doormats 2015]

• The state of security and privacy is not good while society is becoming critically dependent on information technology
• Adding intercept capabilities will further undermine security by increasing complexity
• Risk of abuse by bad actors (e.g. non-democratic nations) and for mass surveillance
  • Example: Juniper
• Incompatible with technologies such as perfect forward secrecy and 1-key authenticated encryption
• Will not help for smart criminals and spies
• No solutions are known that offer reasonable tradeoffs

https://blog.xot.nl/2015/12/08/the-second-crypto-war-is-not-about-crypto/
Can cryptography solve the problem created by cryptography?

[2018] We can find solutions to the Going Dark problem.

... If we can develop driverless cars ... surely we should be able to design devices that both provide data security and permit lawful access with a court order.

Technical proposals (2017-2018)

- (Bellare-Goldwasser, Verifiable partial key escrow, 1997)
- Ray Ozzie: "Clear" – decryption key with corporations
  - Steven Levy, Cracking the Crypto War, Wired, 25 April ’18
- Stefan Savage: Lawful device access without mass surveillance risk, ACM CCS 2018: 1761-1774
- Ernie Brickell: A Proposal for Balancing the Security Requirements from Law Enforcement, Corporations, and Individuals, May ’17
- Robert Thibadeau

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
- 24 96 extra people for Europol

- encourages the countries to collaborate in developing a toolbox with alternative investigation techniques
  - Key search machines? 0-days? Malware?
Three decades of cybersecurity policy: Lessons learned Bart Preneel

General William Bar
Office of Public Affairs

FOR IMMEDIATE RELEASE
Sunday, October 11, 2020

International Statement: End-To-End Encryption and Public Safety

- We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy […]
- Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children. […]
- Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and prosecution of offences and safeguarding the vulnerable;
- Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate […]

The CSAM story (Child Abuse Sexual Material)

- Driven by NCMEC (US)
- Detects CSAM content
  - PhotoDNA: secret perceptual hash function
  - secret list of hash values of content
- Many 100K detections per year
- Threatened by end-to-end encryption

Threshold private set intersection (PSI) with associated data (tPSI-AD) [August 2021]

- Cryptographically optimal way to detect abusive material
- Secure two-party computation (2PC)
  - server provides scanning algorithm
  - learns metadata only and only if there are multiple matches
- Cryptographically solid but…
- Needs perceptual hash function: NeuralHash (96 bits)
Three decades of cybersecurity policy:
Lessons learned	Bart Preneel

Problem 1: Mission Creep

COVID contact tracing sheet leaves ‘creepy’ barman to text model

Problem 2: Unauthorized Surveillance

The 2018 Democracy Index
[Economist Intelligence Unit]

Problem 3: Framing through NeuralHash collisions
https://blog.roboflow.com/neuralhash-collision/

Birthday paradox also works: need 2^48 images

Problem 4: Correctly detecting grooming in written and spoken language is likely well beyond the state of the art
Are there other options for law enforcement?

Options for Law Enforcement (2/4)

- exploit operational security weaknesses: operating a system securely is difficult
  - e.g. password cracking
- obtain technical assistance from industry to bypass decryption or to access keys
  - remote update
  - backup in cloud
  - iPhone unlock from Cellebrite or Grayshift
- use metadata
- use AI
Options for Law Enforcement (3/4)

- Exploit known and unknown vulnerabilities (0-days) to get access
- DE: Bundestrojaner: key logger, screenshots, Skype calls

Options for Law Enforcement (4/4)

- NSA: “Collect it all, know it all, exploit it all”
- Collaborate with intelligence services

The bigger picture

Response of the NSA after 1994

- Going after keys: hacks, replacing public keys, security letters (300K 2001-2016)
- Weak implementations
- Undermine standards (DUAL_EC_DRBG)
- Cryptanalysis
- Increase complexity of standards
- Export controls
- Hardware backdoors
But who shall watch over the (cyber) guards?

No objective way to weigh solving crimes to fundamental right to privacy

Conclusions: policy

Crypto wars ongoing
- limited support for key escrow/backdoors
- backdoors are now imposed in more countries (UK/Australia)
- CSAM may be game changer (policy wise)
- hacking by police is much more risky
- Main problem is still building secure systems for citizens
- Need open debate with all elements on the table

Conclusions: research

Research needed on future options
- risks: don't make the current insecurity worse
- accountability
- transparency

Researchers need to engage in public policy
Three decades of cybersecurity policy:
Lessons learned Bart Preneel