Crypto and Interception Wars & Privacy Preserving

2020's - "The Force Strikes Back"

José Legatheaux Martins

(Professor jubilado da FCT/UNL)

Agenda

- Use of cryptography by civil society and the 70's crypto wars
- Privacy and trust
- Privacy in Rule-of-Law States
- Client Side Scanning - The "force strikes back"

Use of Cryptography by Civilians and the 70's Crypto Wars

Cryptography Technology - Early Usage

- Since many centuries ago cryptography was only available to the elite
- It was highly used by military personnel, diplomats and conspirators
- Most messages were written on paper or parchment and messengers were easily intercepted

Civilians Enter The Scene

- In the XIX century, after the invention of the telegraph, electrical communications become open for business and, if terrestrial, were easily tapped

- During this century, international and long range business expanded and businesses start using encryption for secrecy

Civilians Become Targets of Surveillance

- Governments and big business become interested in civilian usage of cryptography and surveillance of secret messages

- Most encryption methods used by civilians were easy to break by skilled crypto analysts (mostly using statical methods)

- During World War I, all US telegraph users using cryptography had to deposit their code books with authorities

World Wars I and II

- Armies and spies heavily relied on encryption for their communication needs

- Electrical and mechanical coding machines allowed more sophisticated methods of encryption - e.g the German Enigma machine

- Breaking enemy codes was one of the main drives for the invention of modern computers

The First Crypto Wars

- RFC 9446 - Reflections on Ten Years Past Snowden Revelation
    - Chapter 5 - Steven M. Bellovin - Governments and Cryptography - The Crypto Wars Begin

- Around 1970, US Intelligence discovered that Russia Intelligence was tapping some US business phone calls, and recognised that civilians also needed encryption (preferably one easily breakable by US intelligence but robust to others)

DES - Data Encryption Standard

- In 1974 NBA (National Bureau of Standards) open a call for a modern encryption algorithm. The call was won by Lucifer, an algorithm proposed by , using 112 bits long keys

- NSA (National Security Agency) “suggested” modifications and a shorter key with 56 bits

- For long, many suspected that the modifications were a form of weakening the algorithm, **but later this allegation was found false**

- However, 56 bit long keys were deemed as breakable by NSA using brute force attacks. **Later, a Senate Committee recognised this accusation was true**

Cryptography Considered a Weapon

- About the same period, public key cryptography was invented and the RSA algorithm made it usable
- In the 70's and 80's strong cryptography was considered a weapon that could not be exported. Some NSA employees suggested that conferences discussing these methods were unlawful
- NSA tried to block several patents on new methods (e.g. stream cipher) and asked academia to send them papers on cryptography for revision before publication

“The Battle is Joined”

- In early 1990 Phil Zimmerman released PGP (Pretty Good Privacy) for email encryption in open source - He was criminally prosecuted by NSA
- In 1993 ATT announced an easy-to-use phone encryptor - NSA required a modification introducing a key escrow mechanism that allowed NSA to decipher communications
- In 1994 Netscape Released SSL (Secure Socket Layer) an ancestor of TLS (Transport Layer Security) for web traffic - NSA accepted its export with a short key size - 40 bits
- In the 90’s USA industry was prevented from exporting products using high quality encryption, while abroad competitors could use it since **it was known and available as open source**.

One Doesn't Go Through Security, One Goes Around it (Steve Bellovin)

- By 2000 NSA and US Government stopped fighting against the civil use of encryption
- In 2007 researchers found that a NIST-standardised random number generator could be parametrised with some specific constants allowing to predict future generated numbers
- In 2014 Snowden revelations included data suggesting that NSA had a eavesdropping worldwide network targeting known hacks and bugs in systems, to intercept traffic before or after it gets encrypted

Pervasive Monitoring is an Attack

- Read: RFC 7258 (IETF) - Pervasive Monitoring is an Attack, May 2014

- “The IETF will work to mitigate pervasive monitoring”

- By 2024 almost 90% web servers use TLS and content is only disclosed to clients and servers, not third parties. Digital certificates are available for free (e.g. LetsEncrypt).

Today's Situation

- Symmetric key encryption methods as well as public key encryption are in general not breakable, if
  - Encryption algorithms and methods are correctly implemented,
  - Key sizes are considered safe against brute force attacks and
  - no new attack methods are discovered

- In reaction to Snowden Revelations, today almost 90% web servers use TLS and content is only disclosed to clients and servers, not third parties. Digital certificates are available for free (e.g. LetsEncrypt).

- Encrypted messaging and email systems are widely deployed (e.g. WattsApp, Signal, Proton mail, …)

- **Security and reliability of the Internet is build on top of encryption**

Privacy and Trust

Privacy and Trust

- I need to control the degree of disclosure of information I give to any other party I deal with in my life
- If I disclose something on myself to someone else, I want that this will be not used against me later
- If there is information asymmetry, one is in a unfavourable position
- Business relations rely on trust and secrecy. Secret trades, price negotiation, development of business cannot be relayed to the competition

Who Is the Other Party?

- The other party that knows something about me or the company may be a <u>person, a company or a government</u>
- In general, when powerful, these other parties have lots of employees and serves diverse interests - yet more people
- Later, if they want, they can use that information against me
- The most valued is the collected information and the most valuable is the result of its discloser, the most critical the discloser will be
- The value of the discloser may be economical as well as political

Privacy and The Law

- Article 12 of United Nations Declaration of Human Rights
- Article 8 of the European Convention on Human Rights
- US constitution
- Article 35º of the Constituição da República Portuguesa
- Lei de proteção de dados – Lei n.º 67/98 de 26 de Outubro
- General Data Protection Regulation (GDPR) - Regulation EU 2016/67

Privacy Is Not an Absolute Right

- Cover for illegal or immoral activities of all kinds
- Hides dysfunctional families and family violence
- It may be an obstacle to give help to those in distress and may also increase distance among human beings
- **Privacy should be limited in the sense that it cannot be used to harm others or commit a crime at home**

Privacy and the Police

- In Dictatorial States, Police can always violate the privacy of individuals since “normal people has no rights”

- In Rule-of-Law States (e.g. EU), police can only intercept personal communications if authorised by a investigation judge (“juiz de instrução”) that recognises the interception relevance for the criminal investigation, or to produce a proof in court

- In Portugal for example, there are exceptions - for example, communications with my priest, my doctor or my lawyer cannot be intercepted

(Legal) Interception Implementation

- Phone communications are easily intercepted
  - Small number of licensed providers
  - All communications go through a central hub
  - With mobile phones, the operator knows the keys

- When End-to-End Encryption (E2EE) is used, data can only be intercepted before encrypted, or after its decryption

Privacy Under Siege

The "Force Strikes Back"

- In recent years, authorities of USA, Canada, UK, EU, Australia, … are proposing new anti CSAM (Child Sexual Abuse Material) regulations to combat pedophiles (the EU proposal also encompass terrorists)

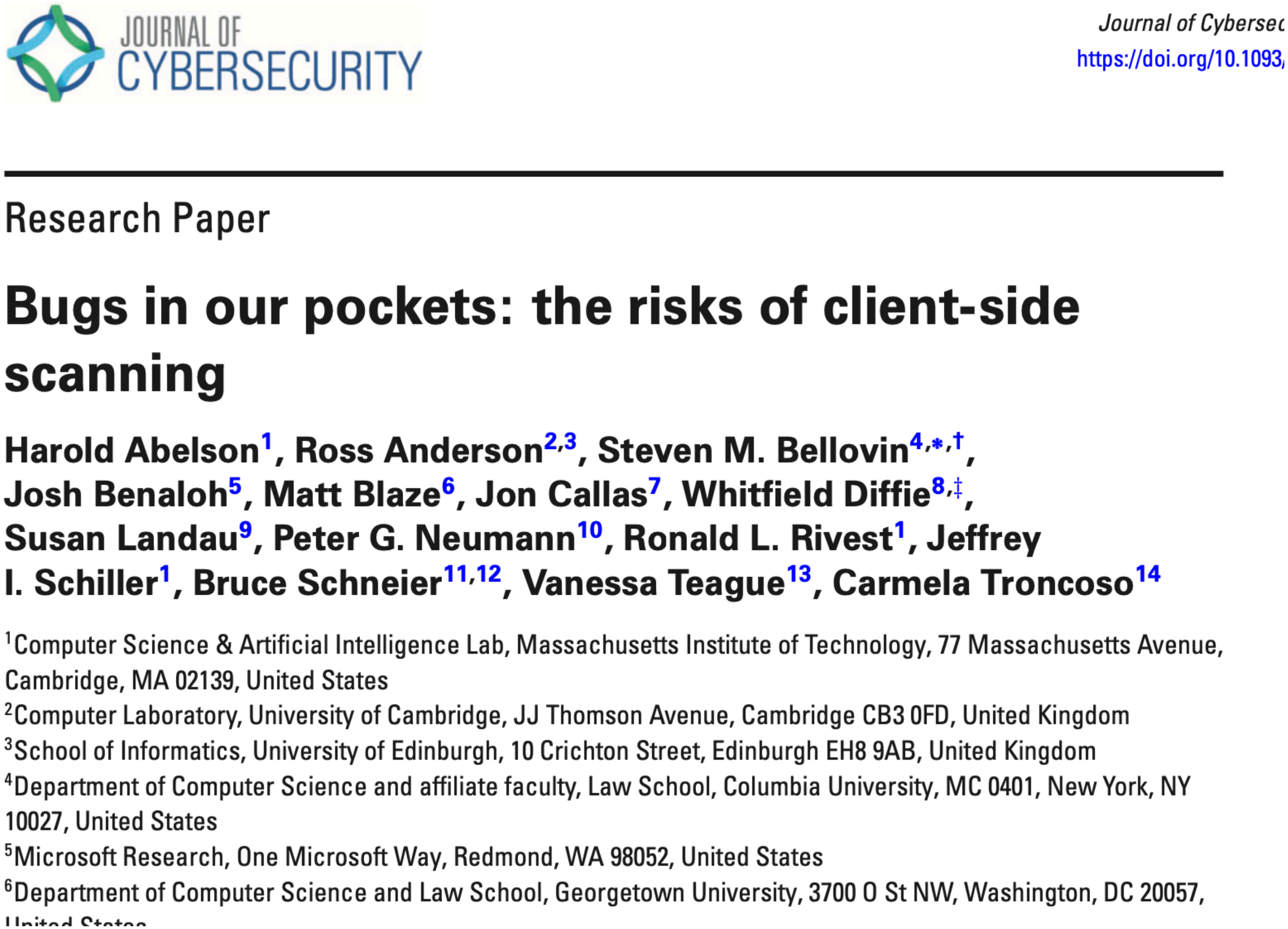
- Proposals main goals:
  - Sites, platforms and devices must detect and eliminate CSAM (and terrorism related content)
  - E2EE is not be forbidden, but detection and reporting should include material exchanged even using E2EE

Possible Implementations

- Forbid the use of E2EE - a no goal according to the proposed regulations!
- Store the used encryption keys in a repository accessible, if required, by authorities - key escrow. Recognised as extremely fragile under security considerations
- Complement server-side scanning (SSS) with client-side scanning (CSS)

- **CSS methods:** code that executes in clients (phones, laptops, small private servers, …) that uses technics to detect signatures of dangerous content in the device and warns authorities if a positive result is found

Bugs in our Pockets



JOURNAL OF CYBERSECURITY

Journal of Cyberse
https://doi.org/10.1093/

Research Paper

Bugs in our pockets: the risks of client-side scanning

Harold Abelson[1], Ross Anderson[2,3], Steven M. Bellovin[4,*,†], Josh Benaloh[5], Matt Blaze[6], Jon Callas[7], Whitfield Diffie[8,‡], Susan Landau[9], Peter G. Neumann[10], Ronald L. Rivest[1], Jeffrey I. Schiller[1], Bruce Schneier[11,12], Vanessa Teague[13], Carmela Troncoso[14]

[1] Computer Science & Artificial Intelligence Lab, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, United States
[2] Computer Laboratory, University of Cambridge, JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
[3] School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom
[4] Department of Computer Science and affiliate faculty, Law School, Columbia University, MC 0401, New York, NY 10027, United States
[5] Microsoft Research, One Microsoft Way, Redmond, WA 98052, United States
[6] Department of Computer Science and Law School, Georgetown University, 3700 O St NW, Washington, DC 20057, United States

Possible Outcomes (1)

- While trying to combat pedophiles outlaw activity, a disproportionate "big brother like" system of social control is being proposed

- All personal (and commercial or governmental), data, plus highly sensitive personnel communications (to doctors, attorneys, priests, etc.) could be scanned with (or without?) court authorisation

- **This is quite different from a controlled interception of phone calls**

Possible Outcomes (2)

- Crooks and criminals will be able to continue to use E2EE systems since the technology is known and readily available (unless CSS implementation is inside a set of known operating system and nobody uses other operating systems?)

- Experts have warned several times that these measures will be quite ineffective
  - Most pedophiles are children's family
  - Real crooks have other ways to circumvent known surveillance methods

- **Even in dictatorial countries, criminals like mafias of all kinds are active (Russia, China, …)**

The Role of Platforms

- Being liable for CSAM users content, platforms use machine learning detection systems or alternative technologies (perceptual hashing) to scan for its presence

- With low human intervention, which is highly expensive and hard to implement in all national and different culture contexts, these methods will produce many false positives

Traditional Media versus New Media

- Traditional (e.g. physical) media can only diffuse content locally produced, bought or accepted after human control
- Even publicity, must be explicitly marked as such and is curated before publication

- But social media (the dominant media today?) diffuses third party content to millions, subject to what type of control? Why is CSAM the only subject of control?

Other Contradictions

- DSA and DMA are EU regulations aimed at taming big platforms

- However, anti CSAM measures for platforms reinforce their power by making them "cheap law enforcing partners"

Bad News and Good News

- An anti CSAM / State security bill has been approved in UK. Its implementation is still ongoing but, for example, it enforces that all security measures introduced by applications and platforms should be subject to previous analysis by the regulator

- The House of Commons of Canada “Online Harms Act - Bill C-63,” of last February, explicitly excludes personnel messaging from being subject to surveillance

Disproportionate Proposals

- Many law experts consider these proposals disproportionate (e.g. Legal Service of the Council of the European Union, "Advice 8787/23 on proposal COM(2022) 209 final. Advice on detection orders in interpersonal communications – Right to privacy and protection of personal data – proportionality")

- European Parliament has also raised concerns to the Commission proposals - COM(2022) 209

Civilians' right to freely use encryption is an ongoing battle

Privacy is neither an absolute right, nor a valueless right