Privacy and the Government

Lecture 6-1

Computers & Society (CPSC 430)

Kevin Leyton-Brown (Section 101)

Giulia Toti and Melissa Lee (Section 102)

https://www.cs.ubc.ca/~kevinlb/teaching/cs430

Encryption

- Method for concealing the content of a message
- Symmetric encryption:
  - Single key used to encrypt and decrypt a message
  - Problem: How does sender get key to receiver?
- Public-Key encryption (e.g., RSA):
  - Each person has two keys: public and private
  - To send *R* a message, encrypt it with *R*'s public key
  - *R* decrypts message with *R*'s private key
  - No need to communicate private keys
- SSL (https://...) is based on public-key encryption:
  - Upon connection, server reports its public key and a trusted certificate authority that can verify it. The client may verify the key.
  - The client encrypts a random number with the server's public key and sends the result to the server.
  - The server decrypts it with its private key.
  - From the random number, both parties generate key material for encryption and decryption.

Strong Encryption

- Strong encryption: encryption at a level that is believed not to be breakable by any other than sender/receiver
  - e.g., 256-bit AES
  - mathematical reasons to believe governments can't break it either
- Availability of strong encryption
  - Previously classified as a munition by US, regulated
  - 1991: US Senate passed a law requiring all encryption systems to include a "back door"
  - In response, Phil Zimmerman created PGP
  - Government tried to shut it down
  - 1999, 2000: courts ruled that these restrictions are illegal, encryption protects privacy and free speech
- *Questions*
  - *Should there be laws against use/distribution of strong encryption?*
  - *How should governments respond to its existence?*

FBI–Apple encryption dispute (2015-2016)

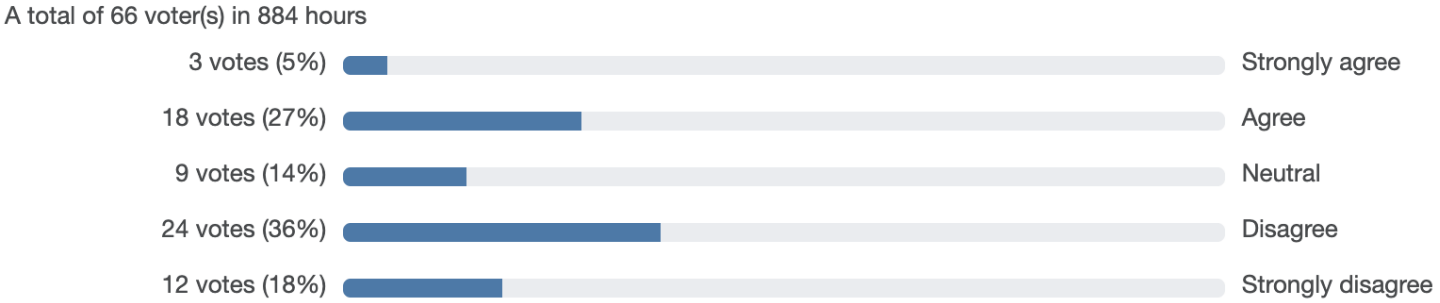
Follows https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute

- In 2015 and 2016, Apple Inc. received and objected to or challenged at least 11 orders issued by United States district courts seeking to compel it “to use its existing capabilities to extract data like contacts, photos and calls from locked iPhones running on operating systems iOS 7 and older” in order to assist in criminal investigations and prosecutions
  - Newer phones use strong encryption, which Apple can’t break
  - The government has sought to compel Apple to write new software that would let the government bypass these devices’ security and unlock the phones
- Best known case:
  - Feb 2016: FBI wanted Apple to create and electronically sign new software that would enable the FBI to unlock a work-issued iPhone 5C it recovered from one of Dec 2015 San Bernardino terrorists (killed 14 people, injured 22)
  - The phone was locked with a four-digit password; set to erase all data after ten failed password attempts
  - Apple declined to create the software
  - A day before the hearing, the government obtained a zero-day exploit and unlocked the phone itself
  - The Los Angeles Times later reported that “the FBI eventually found that Farook's phone had information only about work and revealed nothing about the plot”

Privacy and the Government

"It should be illegal to sell a mobile phone that cannot be decrypted by the police if so ordered by a court."

Section 101



Section 102