Privacy and the Government

Lecture 6-1

Computers & Society (CPSC 430)

Kevin Leyton-Brown

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.

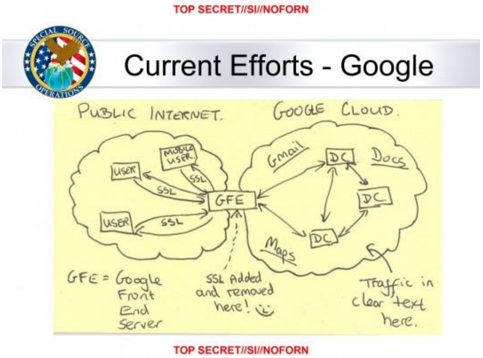
Strong Encryption

- 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?*

Snowden and the NSA Scandal

- In Fall 2013, it emerged that the NSA was engaged in a very wide range of wiretapping

https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)



TOP SECRET//SI//NOFORN

Current Efforts - Google

PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER.
SSL
SSL
GFE
USER
SSL
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

- Washington Post summary of the leaks:
  - Taken together, the revelations have brought to light a global surveillance system that cast off many of its historical restraints after the attacks of Sept. 11, 2001. Secret legal authorities empowered the NSA to sweep in the telephone, Internet and location records of whole populations.

Xkeyscore

https://en.wikipedia.org/wiki/XKeyscore

“What could you do if you would use XKeyscore?” Snowden:

- *You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information. ... You can tag individuals ... Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity.*

Greenwald: low-level NSA analysts can, via systems like Xkeyscore:

- *“listen to whatever emails they want, whatever telephone calls, browsing histories, Microsoft Word documents. And it's all done with no need to go to a court, with no need to even get supervisor approval on the part of the analyst.”*
- *analysis can listen "to the calls or read the emails of everything that the NSA has stored, or look at the browsing histories or Google search terms that you've entered, and it also alerts them to any further activity that people connected to that email address or that IP address do in the future".*

Discussion

Do you think Snowden behaved unethically?

What do you think about wiretapping more broadly?