Usability

If a plaintext is encrypted in the forest...

Lecture Overview

- If security is annoying, people won't use it
- If security is optional, people won't use it
- If security is confusing, people will mess it up

Annoying Security

PGP

- The gold standard for document cryptography
- How was using it?

PGP

- The gold standard for document cryptography
- How was using it?
  - Why Johnny Can't Encrypt: A Usability Evalua
    PGP 5.0 (1999)
  - Why Johnny Still Can't Encrypt: Evaluating the
    Usability of Email Encryption Software (2006)
  - Why Johnny Still, Still Can't Encrypt: Evaluatin
    Usability of a Modern PGP Client (2015)

Glenn Greenwald & Edward Snowden

- January/February - April/May
- “Mr. Greenwald wrote back that he did not have such software”
- “Mr. Snowden later sent him a homemade video with step-by-step instructions for installing it, which Mr. Greenwald watched but never completed.”
- Asked Laura Poitras, who had “a lot of experience” with encryption, but, according to her, “what he was asking for was beyond what I was using in terms of security and anonymity.”

Guardian reporter delayed e-mailing NSA source because crypto is a pain

Passwords

- Poster child of bad usability
- 91% of all passwords in top 1000
- Writing down your passwords is better?
  - 2005
  - 2010
  - 2014

Passwords

https://www.youtube.com/watch?v=dcjViYTDk-A

Optional Security

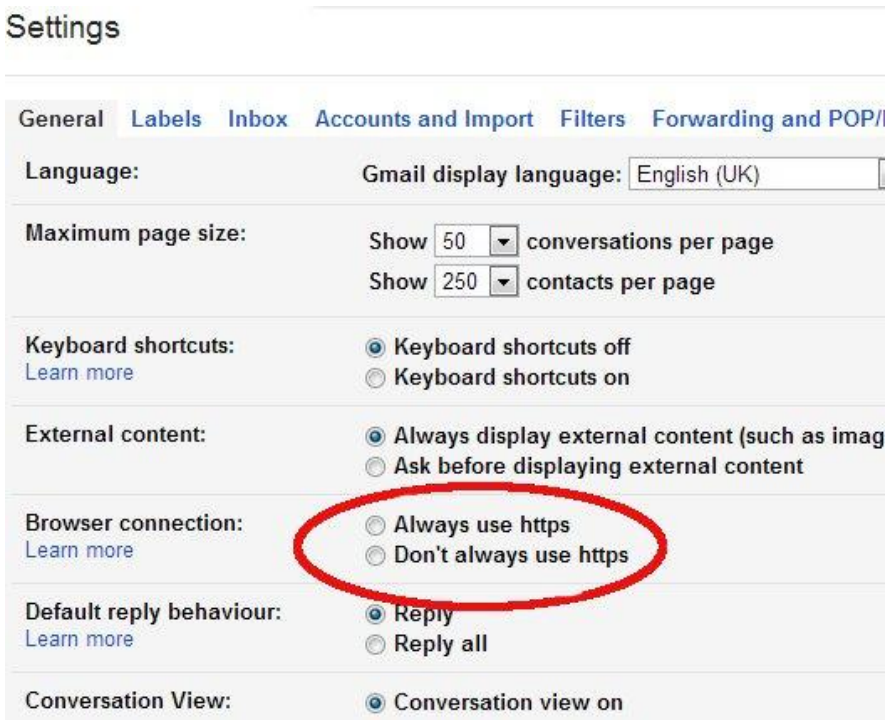
Optional Security

- Key point: people rarely change defaults

Gmail and HTTPS

- In 2008, Gmail added HTTPS support

Gmail and HTTPS



https://1.bp.blogspot.com/-5qa-N9uc0eg/UNwb43MdMsI/AAAAAAAAAqI/P23hYIIzl8w/s160

Gmail and HTTPS

- In 2008, Gmail added HTTPS support
- In 2009, 38 security/privacy experts signed an open letter to Eric Schmidt, asking for HTTPS to be turned on by default
- In 2010, default HTTPS added
- In 2014, HTTPS made non-optional

Default Credentials

- Many products come with default credentials
- In 2012, someone made a botnet ("Carna")
- Non-malicious
- Only used default or empty credentials
- Only went after routers, switches, etc
- Guess how many bots at peak?

Default Credentials

- Many products come with default credentials
- In 2012, someone made a botnet ("Carna")
- Non-malicious
- Only used default or empty credentials
- Only went after routers, switches, etc
- Guess how many bots at peak?
- 420,000

Confusing Security

Confusing Security

- Phishing
- Auto-update

“I once discovered a computer system that was missing essential security patches. When I queried the computer's user, I discovered that the continual warning against clicking on links or agreeing to requests from pop-up windows had been too effective. This user was so frightened of unwittingly agreeing to install all those nasty things from "out there" that all requests were denied, even the ones for essential security patches.”

- When Security Gets in the Way

Confusing Security

- Java apps vs. Java applets: a personal story

Confusing Security

- Browser “security” icons
- badssl.com

Good Usability

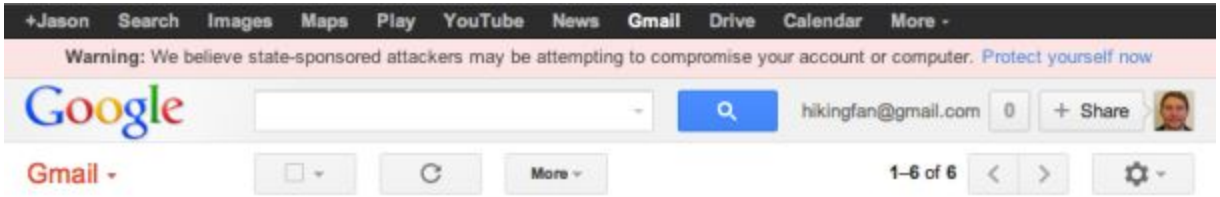
Good Usability

- Goal: Security that is
  - Unobtrusive
  - Intuitive
  - Secure by default
- Examples?

Good Usability

- Goal: Security that is
  - Unobtrusive
  - Intuitive
  - Secure by default
- Examples
  - Two-factor authentication
  - Newer home routers (random default passwords)

Good Usability



http://www.pcworld.com/article/257039/google_warns_gmail_users_over_state_sponsored_attacks.html

Usability Trade-off

- Good but usable is better than perfect but unusable
- Schneier: we need pervasive, decent security