Social anxiety

Cookies, tracking and you

@nosmo: #Cryptoparty Dublin, Nov 2012

Topics

- Cookies
- Flash cookies
- Browser fingerprinting
- Mitigation

Cookies

- Pieces of data
  - Downloaded from sites
  - Stored & returned by browser
- Key-value storage
  - “name” - “nosmo”
  - “sessionid” - “9c3d4b3fad7”

Cookies make life easy

- Remember logins for websites
  - Successful login sets cookie
- Remembers preferences
  - Sort by date/name

Cookies can make life hard

- Stolen cookies => stolen login
- Browsers are *very* permissive

What's in a cookie?

- *Data*
- In theory, anything
- Most effectively: numbers
  - Unique IDs

What's in a number

- Unique IDs
  - Single number in huge number space
  - UUID: between 1 and 340282366920938463463374607431768211456
  - Uniquely identify users

Setting a cookie

- In many browsers, default is autoallow
- Some only allow from the visited site
  - No cookie setting by embedded elements
  - A good start...

Getting a cookie

- Much more negative scenario
- Default behaviour
  - Once a cookie is set, it can be read by setter...

Example

- User visits evilsite.com
  - evilsite.com can set evilsite.com cookie
  - evilsite.com can’t get facebook.com cookie

Counterexample

- User revisits myawfulblog.com
  - Myawfulblog.com gets its cookie
    - Sees unique ID, can correlate results
- Awful blogs tend to feature awful buttons...

Bastards.

Social buttons

- Ostensibly for sharing etc
- Consistently set cookies
  - Containing unique IDs
- Embedded *from* the site it corresponds with
  - ∴ can read cookies

Tracking

- User uniquely identified by cookie
  - Even without membership on site
  - UID read from cookie every load of social button
  - Cookie-setting site can see all visits to corresponding sites

Google analytics

- In 90% of websites
- Google claim no linkage
- *If* it happened - linkage trivial
  - Correlate google.com cookie with GA
  - G+ (real name), mail, browsing history

- [Collusion demo]

Flash cookies

- Shared object storage in Flash
- Enabled by default
- Shared between browsers
- In 2009, 54 of top 100 websites
- Can be used to “respawn” HTTP cookies
- Situation once dire, improved somewhat

Not quite solutions

- VPN / Tor
  - IP changed, but fingerprint stays the same
  - Correlate browser profile with IP

Browser fingerprints

- EFF study
  - Of 2.5 browsers, 83.6% were uniquely identifiable
- Websites can gather huge amounts of data from browsers

Browser profiles

- Font config (JS/Flash/ Java)
- Screen size (JS)
- User agent
- Timezone (JS)
- Plugins accepted

Mitigation

- Clean cookies regularly
- BetterPrivacy for FF flash cookies
  - Or just disable local storage in flash config
- Ghostery blocks some tracking elements
- RequestPolicy - cross-site requests

Mitigation

- Whitelisting
  - Java
  - Flash
  - Silverlight
  - Javascript

- Panopticlick: panopticlick.eff.org
  - Browser fingerprinting
- Ghostery: ghostery.org
  - Block tracking elements on most browsers
- RequestPolicy: addons.mozilla.org
  - Whitelist cross-site loading
- Collusion: addons.mozilla.org
  - Correlate sites with tracking elements