

Internet Anonymity

Mike Hoffert
Nathan Abramyk
Jeff Pereyma
Kari Vass

March 21, 2014

Internet anonymity is important

- Supports freedom of speech: governments can't censor you if they don't know who you are
- Skirting surveillance generally requires anonymity (perhaps to avoid government censorship)
- Oppressive governments often attempt censorship
 - Turkey recently blocked Twitter
 - Amnesty International stated that China "has the largest recorded number of imprisoned journalists and cyber-dissidents in the world"
 - In Iran, internet users must promise not to access "non-Islamic" websites

Internet anonymity is important

- Whistleblowers may need anonymity to prevent retaliation
- Undercover military and law enforcement agents often need anonymity for their protection
- Journalists may have to protect their sources
- One line of defence against targeted attacks
- Removes real life consequences for controversial opinions
- Some people feel uncomfortable speaking publicly

Threats to internet anonymity

- IP addresses can be tied to an ISP customer (but insufficient to identify a specific individual)
 - There could be another person using the computer
 - Drive by downloading
- A number of recent American actions would have implications on internet anonymity: SOPA, PIPA, PRISM, CIPA, etc
- ISPs that sell your information
- Tracking services (especially with online advertisers)
- Browsers have lots of identifying information – **this is what our project focused on**

Browser fingerprint

- TODO: Mention information that can be used to ID browser.
- This is a *high level* introduction to the topics that will be discussed in more depth in the next few slides
- Stress how the factors combine together to form a fingerprint (ie, a browser might be the only one with this specific combination of features)

Panopticlick

- The tool used to gauge the effectiveness of our changes was the EFF's Panopticlick research project
- Panopticlick <<https://panopticlick.eff.org/>> is an attempt to identify the uniqueness of a browser via some of the previously mentioned techniques
- We picked the most identifying techniques and attempted to thwart them
- Let's go into more detail on how we did that

HTTP headers

- TODO: Detail how HTTP headers ID the browser and our solution

Available fonts

- TODO: Detail how the list of available fonts impacts fingerprinting, why we weren't able to solve this, and what changes browsers/JS would need to prevent this
- Don't mention other methods of detecting fonts (Java, Flash) here, they get their own section

Available plugins

- TODO: Detail how the list of available plugins impacts fingerprinting, how we solved this, and the major shortfall of our solution
- Be sure to detail how the browser/JS implementation could offer a better solution than our hacky fix

Other fingerprinting threats

- TODO: Detail how things like Java, Flash, cookies, etc can be used to fingerprint
- Be sure to mention how Panopticlick uses Flash for its font detection
- Mention how to prevent these (Flashblock, Ghostery, etc)

Putting it all together

- Our Chrome plugin, named “Fingerprint Anonymizer”, adds several hooks and overrides to prevent or reduce fingerprinting
- The goal was not to flat out block actions that could be used to identify the user, but rather to let the user know that they were taking place and allow them to choose whether or not to allow them
- This goal was ultimately not possible, due to the fact that much of the data was accessed through parameters and not functions – we couldn’t add functionality to detect when information was read

Putting it all together

- A whitelist was implemented, which the user could add domains for which the blocking is not activated
- The user can manually add regex for matching domains to the whitelist in the extension's options page
- We also implemented a browser action (a button in the browser's main toolbar that opens a prompt) to add the current domain to the whitelist
- Rewriting the HTTP headers is done for all pages
- TODO: mention end result (panopticlick results)

Drawbacks

- TODO: Mention the limitations of our project
- Include mention of limitations of fingerprinting (frequently changes, tracks machine and not user, etc)
- Mention technical limitations such as having to block all plugins and not being able to block font detection

Conclusion

- TODO: Rough conclusion of the things browsers/JS can improve on to prevent fingerprinting, other extensions (like Flashblock, etc), and how effective we think our techniques are at stopping fingerprinting

Demo

Let's now consider a quick demo of the extension in action

TODO: Remove me

This slide demonstrates how source code is displayed

```
// Populate the text area with our previously saved array
chrome.storage.sync.get(
    'whitelist',
    function (result){
        // Get the stored whitelist array
        var whitelist = result.whitelist;

        // Iterate over array and populate our page
        for(var i = 0; i < whitelist.length; i++)
        {
            $('#whitelist').append(whitelist[i] + "\n");
        }
    }
);
```