PrimeLife – Privacy and Identity Management in Europe for Life
Privacy Dashboard

We Are All Under The Microscope

Have you ever wondered what information is being collected about you as you browse the Web? Increasingly, many websites are working with third parties to collect more and more data on users. Data that can be pooled and analysed to create detailed profiles of their user's habits, likes and dislikes, where they live, their age, gender, race, income, marital status and health concerns. The Privacy Dashboard, developed within the PrimeLife project, is an extension for the Firefox browser that enables you to see some of the practices that websites are using, e.g. whether they include 3rd party content, perhaps with lasting cookies that can track you across the Web, or are using a variety of other techniques.

"No one would have believed in the early years of the twenty first century that this world was being watched keenly and closely by inhuman intelligences; that as men busied themselves about their various concerns they were scrutinised and studied, perhaps almost as narrowly as a man with a microscope might scrutinise the transient creatures that swarm and multiply in a drop of water. With infinite complacency men went to and fro over this globe about their little affairs, serene in their assurance of their dominion over personal matters."

with thanks to H.G. Wells

Information About The Current Website

The Dashboard collects information about the current website as pages load. This is presented by an icon that appears on the browser's navigation toolbar next to the location field. The icon displays one of three aspects: a happy face, a thoughtful face and an indignant face. This is based upon rules of thumb that classify the website. The indignant face is shown if the site uses external 3rd party HTTP cookies or external 3rd party flash cookies. The thoughtful face appears if the site has lasting HTTP cookies, flash cookies or external 3rd party content, and lacks a link to a machine readable (P3P) privacy policy. Otherwise the happy face appears. These rules of thumb are to some extent arbitrary, and simply intended to draw the user's attention to the data collected.

The first time you visit a website, the Privacy Dashboard displays a privacy alert in a notification bar at the top of the page. This is the same bar as used by Firefox to ask users for permission to save their user id and password for the site. The notification bar doesn't appear if the site is classified with the happy face. You are invited to choose between 'accept always' (i.e. don't bother me again for this site), 'protect me', or to 'tell me more'. The 'protect me' button ensures that for subsequent loads, scripting is disabled along with cookies and 3rd party content. The 'tell me more' button displays the Privacy Dashboard dialogue window. The dialogue can also be displayed at any time by clicking on the Privacy Dashboard icon on the navigation toolbar.

The Privacy Dashboard dialogue has five tabs labelled "Data Track", "Location", "Current

Website", "Share Findings" and "About". By default it opens with the current website tab. This shows information about the current website, your preferences for this site, and some buttons for checking the website with third party tools which if clicked open up in a new browser tab. The buttons cover Norton SafeWeb, Free Trust Seal, and TRUSTe.

The information shown for the site covers HTTP cookies, Flash cookies (Flash Local Shared Objects), 3rd party content, DOM storage, geolocation, HTML5 pings, invisible images and suspicious URLs indicating the possible use of web-bugs (tracking devices). Cookies are classified according to whether they are retained beyond the current browser session, and whether they are used for this site, an internal 3rd party site (one with a common base domain) or are for external 3rd party sites.

Querying The Data Track

The Data Track tab in the Privacy Dashboard dialogue allows you to query the database of information the extension collects on each

site you visit. You select from a drop-down list of queries together with a text box for typing in the domain name for a website, or a datum name or value. The queries include:

- Which data has been sent to a given website?
- Which sites a given datum value has been sent to?
- Which sites a given datum name has been sent to?
- Which sites use long lasting cookies?
- Which sites use session cookies?
- Which sites use Flash cookies?
- Which sites use DOM storage?
- Which sites are 3rd parties?
- Which internal 3rd parties are used by a given site?
- What cookies are used by a given site?
- Which sites use invisible images?
- Which sites use HTML5 pings?
- Which sites offer P3P policies?
- Which sites have you given access to your geographic location?

Further work is underway to make it easier to browse the data track, including backward and forward buttons by analogy to a web browser.

Protecting Your Privacy

The Dashboard allows you to set personal privacy preferences on a site by site basis. The preferences are available at two levels: simple and advanced, offering a choice between three predefined levels of privacy (carefree, thoughtful and paranoid), or detailed control over a range of settings:

- Never block content from this site
- Block external 3rd parties
- Block external 3rd party cookies
- Block all lasting cookies
- Clear Flash Cookies
- Disable web page scripting
- Disable access to your geolocation
- Disable HTML5 pings
- Don't send HTTP referrer header
- Disable access to DOM storage

The Firefox extension is able to implement these by directly intercepting and blocking HTTP requests, or by setting browser options.

The latter is imperfect since the option to disable scripting applies to all new pages and not just to the current tab. The extension does its best to limit changes to browser wide options to the time the page is being loaded, but if several pages are being loaded concurrently on different tabs, then problems may well arise. Hopefully this problem will be resolved by browser vendors offering more fine grained options that can be set on a per tab or per website basis.

The Adobe Flash plug-in is ubiquitous and installed on pretty much all web browsers. It runs in isolation from the rest of the web browser and as such makes it impractical for the Privacy Dashboard to intercept HTTP requests and to set Flash specific options. The extension is however able to access the local file system to examine and when requested to delete the files used for Flash Local Shared Objects.

Enhanced Support For Geolocation

The Privacy Dashboard also improves upon the browser's built-in support, making it easier to track and revoke which sites you have told Firefox to provide your geolocation to. If you are on a WiFi connection you can check to see just where Google thinks you are based upon your WiFi neighbourhood.

Sharing Your Findings With Others

The data collected by the Privacy Dashboard as you browse gives a view about a small part of the Web. By pooling data from many users it will be possible to build up a much more detailed picture of how sites are tracking users. To this end, the Privacy Dashboard allows you to choose to share your findings with others. The information uploaded is limited to data about the site and its relationship to third party sites, and avoids any information that could be used to identify you. You can determine the server the uploads are made to, along with the frequency of the updates.

To encourage users to share their data, the Privacy Dashboard invites users to opt in when run for the first time. Thereafter, users can review and change their sharing preferences on the "Share Findings" tab on the Privacy Dashboard user interface.

Servers that pool the data should avoid logging the client's IP address, time of upload, and the set of sites covered. This should be made clear in the server's privacy policy. If you are at all concerned you can of course set your sharing preferences to use an anonymizing proxy for your uploads.

Lighting Up The Dark Side Of The Web

We are all familiar with big name websites and the brands they present. This can be likened to a brightly lit high street packed with attractive shops calling out for our attention. Behind the high street is a maze of dark alleyways that few of us are aware of. This is made up of the third party sites used for advertising and data gathering activities. It is time to light up the dark side of the Web, and create some transparency as to who, what and how personal information is being collected, bought and sold.

To kick start this, the Privacy Dashboard is being adapted to act as a web 'bot to visit the top 1000 sites as listed by Google and to collect data on the tracking techniques they are using, and the relationships amongst the hidden ecosystem of third party tracking sites. The challenge is to find ways to present this data in informative and appealing ways.

The Privacy Dashboard 'bot will provide data for the most popular sites, but to reach out to the long tail of progressively less well known sites, it will be essential to pool data gathered by large numbers of individual users of the Dashboard extension.

Related Work

There are a number of other Firefox extensions related to privacy, e.g., Adblock Plus, NoScript and BetterPrivacy. These seek to block out web page ads, to disable scripting or to offer greater control over cookies and other tracking devices. The Privacy Dashboard also does that and adds the means for users to gain greater visibility into how sites are tracking them, and the means to query this data, as well as to contribute to a broader understanding of tracking across the Web.

The Privacy Dashboard is one of a group of three experiments looking into the role of browser extensions for privacy. The others include a fresh take on P3P, using the vocabulary defined by P3P for machine readable privacy policies, but constrained to make it easier to provide a user interface for setting preferences and generating human readable descriptions of the conflicts between the user's preferences and the site's policy. The browser extension looks for a link to the site's privacy policy which is represented in JSON (JavaScript Object Notation) for ease of processing.

The other extension enables websites to support anonymous credentials, where zero knowledge proofs are exploited to show that the user is in possession of a credential from a recognized authority. The site can check that the user is say over 21 or under 16 years old, or is a member of a given group, or lives in a given city, but without learning any more. This fulfils the principle of minimal disclosure of personal information. The demonstration couples the Firefox extension to the Java-based idemix library developed by IBM Research.

Availability And Next Steps

The Firefox extension can be downloaded from the PrimeLife project website, and will shortly become an opensource project of its own right on W3C's servers. The aim is to encourage a community of people interested in a better understanding of how websites collect data on users, and the further development of tools and presentation mechanisms to support this goal.

References

1. http://www.w3.org/2010/09/raggett-fresh-take-on-p3p/

2. http://www.w3.org/QA/2010/11/boosting_privacy_online_-_anon.html

3. http://idemix.wordpress.com/

4. https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/

5. http://www.primelife.eu/results/opensource/76-dashboard

PrimeLife at a glance