Yui Kee Computing Ltd.

Newsletter

May 2010

Contents

Browser Fingerprints Threaten Your Privacy

<web-link for this article>

Research by the Electronic Freedom Frontier (EFF) has shown that most web browsers are uniquely identifiable, leading to serious privacy concerns. The EFF used a test website to collect configuration information from 470,161 visiting browsers, and found that 84% of the configurations were unique.

The data collected was grouped in eight categories:

- User Agent
- HTTP ACCEPT headers
- Cookies enabled?
- Screen resolution
- Timezone
- Browser plugins, plugin versions and MIME types
- System fonts
- Partial supercookie test

This is just one possible method of fingerprinting a browser, and the EFF suggested that commercial companies are already using these and other methods to track users across multiple websites. Paradoxically, some supposedly "privacy enhancing" tools, such as Privoxy and Browzar are ineffective or counter-productive. However, TorButton and NoScript reduced fingerprintability.

Browser fingerprinting techniques could also be used in investigations to link a particular browser (and, by implication, the user of that browser) to an incident or crime, but the techniques cannot be expected to produce forensically strong evidence. Browser fingerprints do not stay constant, any change to plugins, fonts or other settings could affect them. Also, some potential fingerprint parameters could be strongly linked to each other, and the location of the incident, for example, timezone and system fonts - many browsers in Hong Kong could be expected to have Chinese fonts, and a GMT+08:00 timezone.

More Information

How Unique - and Trackable - is Your Browser?
How Unique Is Your Web Browser?
Most browsers leave fingerprint that can ID users

Human Computer Virus Infection Scare Story

<web-link for this article>

Reseacher Dr Mark Gasson from the University of Reading has claimed that he is the first human being to be infected by a computer virus. The "infection" was a deliberate part of his research at the University's School of Systems Engineering. Dr. Gasson claims that he contaminated an RFID chip, which was then embedded in his hand. The normal function of the chip is to allow Dr. Gasson to pass security doors and activate his mobile phone, but Dr Gasson showed in trials that the chip was able to cause external control systems to be infected by the computer virus.

The research has bee widely criticised, by anti-virus experts such as Graham Cluely and the technical press as a meaningless publicity stunt. Infection can be defined as the detrimental colonisation of a host organism by a foreign species. Dr. Gasson's stunt does not fulfil this definition - the computer virus is restricted to the RFID chip which has no information interaction with his body. The location of the RFID chip is incidental - just as having an infected thumbdrive in your pocket when you get into a car does not make the car infected.

Furthermore, even a far lesser claim that an RFID chip can infect other devices is on shaky ground. Note that the claim is that "external control systems" became infected - why wasn't the system named? Graham Cluley explained, "The fact is that that code would not be read until an RFID reader came into contact with the affected RFID chip and even then the software connected with the RFID reader would need to have a vulnerability that would allow the code to be run". Therefore, it seems that the "system" was not a standard computer or phone, but one which had been specially modified to read and execute commands from an RFID chip. Then there is the question of what was stored on the RFID chip. RFID chips do not have large storage, 1Kbi is considered "large". Those who remember boot sector viruses might recall that this is sufficient for a complete virus, but most recent viruses are larger and more complex. The BBC video interview with Dr. Gasson shows a fragment of the code stored on the RFID chip. This appears to include a SQL statement and "<script>" tags surrounding a URL. So, the RFID chip does not contain the virus itself, merely a link to where a suitably-programmed device can go to download the virus and infect itself.

There are serious security concerns to be addressed when there are practical, effective systems for direct two-way communication between biological and non-biological information systems, but they are closely related to the current concerns we have with today's indirect two-way communication. Dr. Gasson's stunt is detrimental to the public understanding of the real issues.

More Information

Captain Cyborg sidekick implants virus-infected chip
First human 'infected with computer virus'
Scaremongering scientist claims to have infected himself with computer virus
We've replaced this hooker's regular herpes with the Win32/Wisp.A BackDoor-EMN virus. Let's see if anyone notices…
Our 'human "infected with computer chip virus"' story

PCI DSS: The Mother of Compliance Issues

<web-link for this article>

Handshake Networking Ltd. Consultant Richard Stagg compares PCI DSS (Payment Card Industry Data Security Standard) with a mother warning a child to tidy their room. Writing in Computerworld Hong Kong, Mr. Stagg argues that forced PCI DSS compliance is a necessary baseline without which lazy online merchants will continue to undermine public trust in online transactions. He also claims that the innocent majority aren't responsible for contributing to the poor security situation.

In a follow-up blog post he berates security-negligent merchants as "not even incompetent".

Well, kiddies, it's time to clear up your security policies, or (with apologies to Beowulf) the Mother you'll need to worry about is not the PCI DSS, but the next monster security breach.

More Information

Why does the PCI remind me of my mother?
Not even…
Why does the PCI remind me of my mother? (PDF)

Privacy and Facebook

<web-link for this article>

A storm of controversy has recently engulfed the currently most popular social networking website, Facebook. In January 2010, Facebook founder Mark Zuckerberg's responded to growing privacy concerns saying, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time", in a live interview with TechCrunch founder Michael Arrington. However, a strong negative reaction to the comments made it clear that social norms have not changed as much as Mr. Zuckerberg believed.

The storm really gathered force in May, with a series of revelations, that Facebook was leaking data marked as private and Facebook was breaking its own privacy policy by giving advertisers users' names and locations. In a Washington Post article Mr. Zuckerberg announced Facebook would be making controlling your information simpler, and providing a switch to turn off all third-party services, writing, "Sometimes we move too fast". This is a clear indication that he still believes that privacy will disappear, and will will all become relaxed about sharing everything about ourselves with everyone.

The new privacy controls are now explained, and they are being made available to users gradually.

Yui Kee's Chief Consultant, Allan Dyer, commented, "I use Facebook and other social networking websites myself, and, event though I try to be selective about how much personal information I make public, it is not easy. Information may also be used for unintended purposes, such as authentication. The simplification of the privacy choices appears to be a positive step, but Mr. Zuckerberg must tread carefully: privacy is, and will continue to be, important. Facebook must continue to adapt to users privacy concerns, or the users will leave."

More Information

Facebook unveils simpler privacy controls to spur sharing
The Evolution of Privacy on Facebook
Security's Top 4 Social Engineers Of All Time
Controlling how you share
Mark Zuckerberg on 'Making Control Simple'
Facebook's Zuckerberg Says The Age of Privacy is Over

Why Facebook is Wrong: Privacy Is Still Important
One-on-one with Facebook CEO Mark Zuckerberg
Facebook founder called trusting users dumb f*cks
Facebook users 'don't want complete privacy': Zuckerberg
Why I Left Facebook
Facebook simplifies controls but continues exposing users
Facebook unveils simpler privacy controls to spur sharing
Facebook forces users to expose or remove connections
Facebook boss admits privacy 'errors' and promises revamp
rom Facebook, answering privacy concerns with new settings
Facebook gives users' names to advertisers
Facebook scrambles to close hole exposing private data
World+bitch flocking to expose self on Facebook
Authentication - a trivial pursuit?

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/