



The Kaspersky Lab Security News Service

Published on *threatpost* (<http://threatpost.com>)

[Home](#) > [Malware Attacks](#) > Q&A: Evercookie Creator Samy Kamkar

Q&A: Evercookie Creator Samy Kamkar

By *Dennis Fisher*

Created 10/27/2010 - 2:15pm

[1]Samy Kamkar has been making quite a bit of noise lately, beginning with his release of the [Evercookie](#) [2] earlier this month and continuing with his talk at the SecTor conference this week on novel [methods for stealing users' cookies](#) [3] without any browser bugs. In this interview, he discusses both of those methods, as well as a new technique he developed that can use Google data and simple attacks to find a user's physical location within a few feet.



Dennis Fisher: How did you come across the techniques you talked about for stealing session cookies?

Kamkar: I wanted to learn about crypto. I read Bruce Schneier's book "[Applied Cryptography](#)" [4] and I wanted to see if I could actually apply it. So I decided to look at PHP because it's so popular, it's everywhere. So I just looked at the PHP code and I found this random number generator and I didn't understand it very well, so I kept looking at it and I found the seed that it uses and it didn't look very strong. I probably spent a week looking at it, going back and forth and having little breakthroughs here and there. I was working full time, so it was off and on. That was the start of it and then it went from there.

Fisher: How difficult is it for someone else to reproduce this?

Kamkar: I released a lot of code for this, so I made it pretty easy. The attack is pretty difficult, but the code I released makes it a lot easier. It's still a tough attack, I think. But I notified PHP about it and they fixed it, but I don't know how many people update PHP. If your server is working, you leave it alone, right? The right thing to do would to at least be on the security mailing list, but generally I don't think people do that.

Fisher: The way you described this in the talk is going after the services around your target, rather than the person himself or his specific machine.

Kamkar: Yeah, I think that's easier honestly. It's a lot easier to attack a service or a combination of services. If you can get them to do something else that helps you, like sending a big message to someone that has a lot of data in it, that helps.

Fisher: The other thing you talked about is a technique for essentially using a combination of cross-site scripting and publicly available data to find a user's physical location. How exactly does that work?

Kamkar: It all starts with a user going to a Web page that you control. The site uses an iFrame to determine what wireless router the user is using and then it determines what XSS attack will work against that router. Every wireless router is vulnerable to some kind of XSS, at least every one that I've ever tested. That loads some remote JavaScript that gets the MAC address of the router. That's the key. That's one of the things that Google has collected in its Street View data. They have this huge database and you can send it the MAC address and the signal strength and it will return the location of that router. It's extremely accurate. Every time I've tested it, it works. I'm assuming that Google has done this triangulation on the routers because that's the way it looks from the data. It will also work with Android phones instead of routers.

Fisher: So anyone can just query that database?

Kamkar: If you know how to do it you can. I only found because I was messing around with Firefox and HTML5 and saw what was happening. If you're using an HTML5-enabled browser and using the geolocation services, it will ask you if you want to share your location with a site. If you say yes, it will send the SSID and MAC address to Google and get back your location. I saw that and figured out that I could do it myself without you using a browser that supports HTML5.

Fisher: It seems like the fact that this is possible is sort of getting lost amid all the controversy about Google collecting user names and passwords when they were mapping the WiFi hotspots.

Kamkar: I think it's huge. It's a serious thing and I think it's gonna blow up at some point. People have no idea this is happening and I think it'll blow up when people realize Google has all of this. I can get it down to within a few feet of your location, depending on where the router is. It's absolutely crazy. It's easy to recreate this.

Shorten URL: [Copy Shortened URL](#). Click to copy to clipboard or [post to Twitter](#) ^[5]

[Malware Attacks](#) | [Vulnerabilities](#) | [Web Application Security](#) | [google](#) | [Internet Security](#)
[Samy Kamkar](#) | [Web Application Security](#)

[Home](#) | [Topics](#) | [Blogs](#) | [Resources](#) | [Videos](#) | [About](#) | [Newsletter Sign-up](#) | [Linking Policy](#) | [Contact Us](#)

[Compliance & Regulations](#) | [Data Breaches](#) | [Encryption](#) | [Government Security](#) | [Malware Attacks](#) | [Patch Management](#) | [Privacy](#) | [Vulnerabilities](#) | [Web Application Security](#)
[Ryan Naraine](#) | [Dennis Fisher](#) | [Guest Posts](#) | [Best of the Net](#) | [Series](#)



Source URL: http://threatpost.com/en_us/blogs/qa-evercookie-creator-samy-kamkar-102710

Links:

[1] http://threatpost.com/en_us/blogs/qa-evercookie-creator-samy-kamkar-102710

[2] http://threatpost.com/en_us/blogs/researchers-find-methods-kill-persistent-evercookie-101910

[3] http://threatpost.com/en_us/blogs/even-without-browser-flaws-attackers-have-upper-hand-web-102610

[4] <http://www.schneier.com/book-applied.html>

[5] http://www.twitter.com/home?status=Q&A: Evercookie Creator Samy Kamkar http://threatpost.com/en_us/cev