Feed Journal

Issue #5 for AUEB CIS 1/12/2011 - 1/26/2011 feedjournal.com

Mozilla Leads the Way on Do Not Track

(EFF.org Updates)

Submitted at 1/24/2011 3:16:39 PM

Earlier today, Mozilla announced plans to incorporate a Do Not Track feature into their next browser release, Firefox 4.1. Google also announced a new privacy extension today, but we believe that Mozilla is now taking a clear lead and building a practical way forward for people who want privacy when they browse the web. Why We Need Do Not Track

Privacy advocates have been calling attention to issues of pervasive online tracking for some time. Often intertwined with the issue of behavioral targeting, online tracking refers to the difficult-to-elude mechanisms by which most or all of our reading and other activities on the Web are recorded by third parties, without our knowledge or permission.

The technical details of online tracking are multifarious. They include traditional HTTP cookies as well as flash cookies and many other kinds of supercookies, web bugs, JavaScript trackers, HTTP Referrers, and fingerprinting. And new ways to track browsers will continue to be invented. Even consumers who take steps to delete their cookies or use private browsing mode remain unable to prevent third parties from observing their clickstreams.

Currently, a subset of advertisers offer a mechanism for opting out of behavioral advertising through the Network Advertising Initiative— a project that has been widely criticized for failing to provide consumers with meaningful control. The NAI opt-out suffers from several problems: the biggest is that there is no consistency on what "opt out" means. Some tracking companies recognize that an "opt out" should be an opt out from being tracked, others insist on interpreting the opt out as being an opt out for receiving targeted advertising. In other words, the NAI allows its members to to tell people that they've opted out, when in fact their web browsing is still being observed and recorded indefinitely.

The cookie-based opt-out scheme also suffers from serious technical drawbacks. Some of these are issues of complexity — tracking companies need to opt-in before it can work and new types of cookie need to be created for each of them. There is also the issue of fragility — privacy conscious users delete their cookies regularly, which means the opt-out keeps turning itself off.

The "Keep Your Opt-Outs" Chrome extension announced by Google today is an attempt to address that last problem. In that respect it is similar to the TACO Firefox Extension, though it doesn't set any opt-out cookies for companies that are not NAI members. It also doesn't fix the other fundamental problems with the NAI's approach: complexity, the lack of a clear signal that can be observed and interpreted by any website, and allowing fake opt-outs that only protect you from targeted advertising but don't prevent any tracking.

For these reasons, we believe that the only sensible way forward for privacy opt-outs is a Do Not Track header, and we're very pleased to see Mozilla planning to offer this option in their future browser versions. How Will Do Not Track Work?

Every time your computer sends or receives information over the Web, the request begins with some short pieces of information called headers. These headers include information like what browser you're using, what language your computer is set to, and other technical details. The Do Not Track proposal is to include a simple, machine-readable header indicating that you don't want to be tracked.

The header-based Do Not Track system appeals because it calls for an armistice in the arms race of online tracking. Currently, advertisers constantly invent new ways of tracking consumers and security researchers work to block this tracking with new technology. A header-based Do Not Track model sends out a signal with every online communication indicating a user's preference not to be tracked. This puts the onus on the tracking companies to comply with Do Not Track mechanisms — rather than on the user to discover and counter every type of possible online tracking.

Some important things to note about this proposal:

- There is no "list" that consumers need to sign up for. Early discussion of Do Not Track included proposals about a list-based registry of users, similar to the Do Not Call Registry. This proposal does not collect data on consumers in a central list.(Security and privacy researcher Christopher Soghoian has more about the history of Do Not Track.)
- Consumers won't need to update software for Do Not Track regularly. Early versions of Do Not Track proposed installing software on an individual's computer that listed all the known tracking companies. As more companies were identified, the list would need to be updated. The current proposal does not store a list of companies on your computer and so does not need to be repeatedly updated.
- You can still clear your cookies without fear of disrupting the header-based Do Not Track.
- The header-based Do Not Track model won't threaten ad-supported businesses.

The Next Steps

EFF will be submitting formal comments to the Federal Trade Commission responding to questions they raised in their privacy report. In the meantime, users should consider using some of the Mozilla Firefox addons that have already incorporated the header-based advertising opt-out. The Universal Behavioral Advertising Opt-Out is the easiest way to set the header today, though it is also set by development versions of AdBlock Plus and NoScript, and will be in future stable releases of those extensions. Because many advertisers do not yet respect the header, for the time being, we recommend installing it along side beef TACO and AdBlock Plus(with EasyPrivacy) for the time being.

We plan to continue posting articles that will explore and explain Do Not Track. Our next article will discuss the semantics and server side responses that are appropriate in response to a Do Not Track header. In other words, what does the "Track" in Do Not Track mean?

Early Lessons from the Tunisian Revolution

(EFF.org Updates)

Submitted at 1/21/2011 6:50:58 PM

Last week's post about the increasingly draconian and desperate measures the Tunisian government was taking to censor bloggers, journalists, and activists online was rapidly made irrelevant by subsequent events. Over the next few days, Tunisian dictator El Abidine Ben Ali promised not to run for re-election in 2014, then offered widespread reforms, including freedom of expression on the Internet, and finally stepped down from power and fled the country. The steps that EFF called on Facebook, Google, and Yahoo to take in order to protect the privacy and safety of their Tunisian users soon lost their urgency. For now, Tunisians are experiencing unprecedented freedom online after years of extensive government filtering and censorship of websites.

One early lesson from the Tunisian revolution has been that social networking sites can be powerful tools for communication. There has been a great deal of argument about the role of social networking sites in the Tunisian revolution. The Berkman Center's Ethan Zuckerman observes that the riots and protests in Tunisia did not receive even a fraction of the social media coverage that was lavished on Iran's Green Revolution:

For users of social media, the protests in Iran were an inescapable, global story. Tunisia, by contrast, hasn't seen nearly the attention or support from the online community.

Even so, Zuckerman credits social media with giving Tunisians a view of the protests that they did not get through heavily-censored government television, radio, and newspapers. YouTube had been blocked in Tunisia since 2007, but that did not stop Tunisians from using the site to share videos of the riots and protests with the world. Tunisians shared details about the clashes between the unarmed protesters and police using live ammunition on Twitter. The first rumors of a coup on January 12th were also spread on the social networking site. The interim government includes blogger Slim Amamou, who had been detained by the Tunisian government as a political prisoner just last week. Slim made the announcement that he would be joining the new government as Secretary of State for Sports and Youth Affairs on his Twitter stream.

Another early lesson from the Tunisian revolution is that activists in repressive regimes must take steps to minimize risk to themselves when communicating online. While social networking sites played a role in allowing Tunisians to communicate about the riots and protests among themselves and to the outside world, the Tunisian government also exploited social networks to track down dissenters. Bloggers, journalists, and online activists in Tunisia faced detention as well as government attacks against their Facebook and email accounts, which serve as a reminder that online activists in repressive regimes may be vulnerable to government reprisal. EFF urges online activists to read our Surveillance Self-Defense International page, which gives practical advice for people living in repressive regimes who want to speak out while minimizing the risk of surveillance and censorship by their governments.

The threat to Tunisian activists appears to have abated for now, but the opportunity to learn from their successes and failures is just beginning. The precautions outlined in SSDI are essential reading for everyone who wants to follow in their footsteps.

House Subcommittee Revives Mandatory Data Retention Debate...With a Surprise Attack on EFF

(EFF.org Updates)

Submitted at 1/25/2011 6:47:09 PM

This morning, the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security held a hearing on mandatory Internet data retention, once again reviving the debate over whether Congress should pass legislation to force ISPs and telecom providers to log information about how users communicate and use the Internet. The hearing, awash with rhetoric about targeting Internet crime and including an unexpected condemnation of EFF's privacy advocacy, was purportedly an information- and fact-finding hearing to explore the issue of data retention and consider what Congress' role should be. However, it's already clear where the new House Judiciary Chairman, Representative Lamar Smith, stands on the issue: he introduced data retention legislation just last year and likely will do so again this year.

EFF believes that government-mandated data retention would be an overwhelmingly invasive and costly demand, raising serious privacy and free speech concerns — points well-argued at the hearing by John Morris, General Counsel of CDT[written testimony], and Kate Dean, Executive Director of the United States Internet Service Provider Association[written testimony].

Although the Obama Adminstration has not yet put forward a specific data retention proposal, any such proposal would likely have ISPs and perhaps other online service providers preemptively recording data about the online activities of millions of Americans who haven't committed any crime. Advocates for data retention typically focus narrowly on the benefits afforded to law enforcement without accounting for the massive costs and extreme security risks that come with storing significant quantities of data about every Internet user — databanks that will prove to be irresistible not only to government investigators but also civil litigants (read: ex-spouses, insurance companies, disgruntled neighbors) and malicious hackers of every stripe. A legal obligation to log users' Internet use, paired with weak federal privacy laws that allow the government to easily obtain those records, would dangerously expand the government's ability to surveil its citizens, damage privacy, and chill freedom of expression.

Perhaps the biggest surprise in the hearing was Deputy Assistant Attorney General Jason Weinstein's attack on EFF and our Best Practices for Online Service Providers (OSPs) whitepaper. As Weinstein testified, "In 2008, the Electronic Frontier Foundation published a user guide or a guide that was titled Best Practices for Online Service Providers which I think is unintentionally the best argument for Congress to intervene in this space than anything that I can say today." Weinstein went on to object to some of the guidelines in the whitepaper, designed by attorneys and technologists to best balance the business and technical needs of OSPs and their users' privacy and civil liberties. Apparently, the Justice Department thinks that informing Internet companies that data retention is not legally required, and also suggesting strategies for protecting their users' privacy, is a clear and present danger to online safety.

On the contrary, we think that the Best Practices for OSPs encourages sound privacy policy, a position borne out in 2009 when the Justice Department illegally demanded logs reflecting the IP address of every single person who had visited any page on the political news site Indymedia.us. Lucky for the readers of Indymedia.us, that site followed our OSP best practices and didn't keep such logs, and with EFF's help, beat back the government's overreaching subpoena. However, a mandatory data retention regime would inevitably lead to even more such illegal demands for Internet users' data being made and complied with, to the detriment of Americans' digital rights.

Unfortunately, today's hearing is the first signal that the Obama Administration, like the Bush Administration before it, hopes to push a new data retention law through Congress. Thankfully, at least some representatives present at the hearing seemed to recognize that when Americans' privacy and security are at risk, a healthy level of skepticism and rigorous investigation will be vital to avoid creating disastrous legislation. EFF plans to keep Congress and the public well-appraised of the threat to civil liberties posed by mandatory data retention, so stay tuned to Deeplinks and the EFF Action Center for updates as the issue works its way through Congress.

Fedora servers breached after external compromise

(Hack In The Box)

Submitted at 1/25/2011 6:05:00 PM

Servers belonging to the Fedora Project were breached over the weekend by an unknown hacker who gained access though a team member's account. The compromise of fedorapeople.org meant that the attacker had the ability, however briefly, to push changes to Fedora's SCM system. There's no evidence any such updates were made or that Fedora's systems were subject to any vulnerabilities or exploits. â€œWhile the user in question had the ability to commit to Fedora SCM, the Infrastructure Team does not believe that the compromised account was used to do this, or cause any builds or updates in the Fedora build system,â€ Fedora Project Leader Jared Smith wrote. â€œThe Infrastructure Team believes that Fedora users are in no way threatened by this security breach and we have found no evidence that the compromise extended beyond this single account.â€

EFF Urges California Court to Grant Public Access to Electronic Mapping Data

(EFF.org Updates)

Submitted at 1/21/2011 7:24:08 PM

Last week, EFF joined a coalition of public interest and media groups in filing an amicus brief (pdf) urging a California Court of Appeal to uphold the public's right to access electronic files created and stored by local governments. The case, Sierra Club v. Superior Court, focuses on the public's right to access geographic information system (GIS) basemaps created by local governments in California.

GIS basemaps integrate basic property information such as parcel boundaries, addresses, and other property data. Additional information can then be "layered" on top of the basemaps, enabling users to understand, interpret, and visualize data in ways that simply aren't possible through the rows and columns of a spreadsheet. Individuals and organizations then use these maps for a variety of innovative purposes — for example, scientists use them, journalists and the media use them, and public interest organizations use them(pdf).

The Sierra Club filed a request under the California Public Records Act (CPRA) for Orange County's property information — information the County used and maintained in a GIS format. The Sierra Club requested the GIS basemap as part of its mission to protect open spaces in California: using the basemaps, the Sierra Club makes detailed maps of proposed real estate developments and suggests possible alternatives to those developments. The County, however, refused to turn over the information in the requested GIS format, despite its obligation under California law to provide public records in "any electronic format in which it holds the information." Instead, the County offered to provide the property information in a pdf, even though the County already had the information available in GIS format.

Orange County claimed that information stored in GIS format is exempt from disclosure under the "software exception" of the CPRA. While the CPRA does exempt government entities from disclosing "computer software developed by a state or local agency," public information processed or formatted for that software is not exempt. Coupled with the County's obligation to provide public records in the format requested, it seems clear that Orange County is illegally withholding its GIS basemap from the Sierra Club.

Unfortunately, the trial court sided with Orange County and inexplicably held that the GIS basemap constituted software that was exempt from disclosure. The Sierra Club appealed the decision, and the appellate court ordered full briefing. Our amicus brief argued that simply because information is stored in a specific electronic file format, that format does not change the public nature of the information itself.

The amicus brief was spearheaded by the First Amendment Coalition(FAC), an organization that litigated, and won, a similar case in 2009. Along with FAC, EFF joined the brief with the Associated Press, the Reporters Committee for Freedom of the Press, the Citizen Media Law Project, and Wired, among numerous other public interest and media organizations dedicated to open government and freedom of information.

```
<HTML>
<HEAD>
<TITLE>Moved Permanently</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<H1>Moved Permanently</H1>
The document has moved <A HREF="http://[illegible]/m28sx.html">here</A>.
</BODY>
</HTML>
```

New Twitter worm redirects to Fake AV

(Securelist / Blog)

Submitted at 1/20/2011 8:35:00 AM

A new Twitter worm is spreading fast, using the "goo.gl" URL shortening service to distribute malicious links.

The malicious links go through a number of redirections which are described below. The redirection chain may push Twitter users to a fake anti-virus (scareware) serving the "Security Shield" Rogue AV. The webpage is using exactly the same obfuscation techniques as a previous version (Security Tool), which is an implementation of RSA cryptography in JavaScript to obfuscate the page code.

Our users are protected from this worm and all the URLS are being blacklisted in our products.

Here are some of the technical details:

• Redirection Chains Those "goo.gl" links are redirecting users to different domains with a "m28sx.html" page: This html page will then redirects users to a static domain with a Ukrainian top level domain: As if that was not enough, this domain redirects the user to another IP address which is related to Fake Anti Virus distribution: This IP address will then do its final redirection job, which leads to the Fake AV website:• The Rogue AV site Once you are on this website, you will get warning that your machine is running suspicious applications and you are encouraged to scan it: After approval, the scanning begins: The user is invited to remove all the threats from their computer, and will download a fake Anti Virus application called "Security Shield": The graphical user interface gets translated to the language of the OS the Rogue AV is running on. During my test, a French version of Windows XP was used, hence the French translation of the interface.• Rogue AV web site uses RSA for code obfuscation Obfuscation techniques are very common for malicious web sites. Here is a quick look into the one used by the Rogue AV web site. While looking at the obfuscation, I found out that it is comprised of two steps: • Base64 Decode (trivial)• RSA with a very small Modulus

Here is chunk of code from the obfuscated page: Both the Class and the Method used are using random names. The "camunqjr" method is taking a BASE64 decoded parameter. If we investigate the class, we end up right inside the RSA algorithm: Anyone familiar with cryptography will recognize the RSA algorithm here. We have a function taking 3 parameters: C, D and N which is using the "powmod" operator.

They are using RSA to decrypt the JavaScript locally

• 'c' is known as the cyphertext• 'd' is known as the secret exponent or decryption exponent.• 'n' is known as the modulus

In order to get 'm' (Message) , the decryption goes like this: m = c d mod n

RSA is used as an obfuscation technique more frequently than any other, since the private key is available in the JavaScript page. The modulus "N" seems to be 26 bits in length most of the time, which is ridiculously small.

Here is a screenshot of the parameters taken from the JavaScript: Bear in mind that clicking on random links may lead to severe infection of your machine.

Microsoft Security Advisory 2488013

by US-CERT (US-CERT Current Activity)

Submitted at 1/12/2011 7:58:19 AM

Microsoft Security Advisory 2488013 addresses a vulnerability in Internet Explorer. This advisory has been updated to include Microsoft Fix It 50591 that prevents the recursive loading of CSS style sheets in Internet Explorer as a mitigation for this vulnerability. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.

US-CERT encourages users and administrators to review Microsoft Security Advisory 2488013 and implement the suggested workarounds to help mitigate the risks. Microsoft Fix IT 50591 is available from Microsoft Knowledgebase Article 2488013. Additional information regarding this vulnerability can be found in US-CERT Vulnerability Note VU#634956.

US-CERT will provide additional information as it becomes available.

Banks may soon require new online authentication steps

(Hack In The Box)

Submitted at 1/25/2011 6:05:00 PM

The Federal Financial Institutions Examination Council (FFIEC) could soon release new guidelines for banks to use when authenticating users to online banking transactions. The new guidelines will clarify the FFIEC's existing guidelines on the subject and more explicitly inform banks about

BANKS page 4

Wanted: Incident Handler in Michigan

by Richard Bejtlich (TaoSecurity)

Submitted at 1/19/2011 9:11:00 AM

Do you know how to detect and respond to intruders in a multinational organization? Do you want to join a team with that mission? Are you an experienced information security professional who is looking for a challenge? If your answer to these three questions is yes, please consider applying for the last open Incident Handler role in GE-CIRT. In this role you will mentor intermediate and junior CIRT members and work with some of the best detection and response staff in the world.

The role is located at our Advanced Manufacturing & Software Technology Center in located at Visteon Village, Van Buren Township, Michigan. By the end of the month, 19 of my team (about half of GE-CIRT) will be located there. (I have 2 new hires arriving within the next two weeks.) In addition to normal operations there, our extended team meets at the AMSTC facility regularly for training and planning sessions.

If you would like more information on the role, apply for job 1259804 and I will review your resume. Please read the qualifications carefully -- I'm looking for an experienced person for this role. Thank you.

Tweet

Oracle Releases Critical Patch Update for January 2011

by US-CERT (US-CERT Current Activity)

Submitted at 1/19/2011 7:27:44 AM

Oracle has released its Critical Patch Update for January 2011 to address 82 vulnerabilities across multiple products. This update contains the following security fixes:

7 for Oracle Database Server
16 for Oracle Fusion Middleware
2 for Oracle Enterprise Manager Grid Control
16 for Oracle Applications
3 for Oracle Supply Chain Products Suite
11 for Oracle PeopleSoft and JDEdwards Suite
2 for Oracle Industry Applications
23 for Oracle Sun Products Suite
2 for Oracle Open Office Suite

US-CERT encourages users and administrators to review the January 2011 Critical Patch Update and apply any necessary updates to help mitigate the risks.

Top 10 Web Hacking Techniques of 2010 Revealed

(Hack In The Box)

Submitted at 1/25/2011 6:10:00 PM

A Web hack that can endanger online banking transactions is ranked the No. 1 new Web hacking technique for 2010 in a top 10 list selected by a panel of experts and open voting. Called the Padding Oracle Crypto Attack, the hack takes advantage of how Microsoft's Web framework ASP.NET protects AES encryption cookies. If encryption data in the cookie has been changed, the way ASP.NET handles it results in the application leaking some information about how to decrypt the traffic. With enough repeated changes and leaked information, the hacker can deduce which possible bytes can be eliminated from the encryption key. That reduces the number of unknown bytes to a small enough number to be guessed.

RIM Releases Security Advisory for BlackBerry Enterprise Server

by US-CERT (US-CERT Current Activity)

Submitted at 1/12/2011 7:16:29 AM

RIM has released a security advisory to address a vulnerability in the PDF distiller of the BlackBerry attachment service for BlackBerry Enterprise Server. This vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.

US-CERT encourages users and administrators to review BlackBerry security advisory KB25382 and apply any necessary updates to help mitigate the risks.

BANKS

continued from page 3

what they need to do to bolster online authentication, said Avivah Litan, an analyst at Gartner. Litan and others recently met with the FFIEC's IT subcommittee to discuss the updates. "They have been talking about it and debating it for a while," Litan said. "My understanding is that [the subcommittee meeting] was the last step in the process before they issue the new guidance."

Google Releases Chrome 8.0.552.237

by US-CERT (US-CERT Current Activity)

Submitted at 1/14/2011 7:10:11 AM

Google has released Chrome 8.0.552.237 for all platforms to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.

US-CERT encourages users and administrators to review the Google Chrome Releases blog entry and apply any necessary updates to help mitigate the risks.