Privacy Gets a New Round of Prominence

Greg Goth

If arriving at a consensus for assuring privacy on the Internet were only as simple as the instinctive ideal Thomas Roessler, the World Wide Web Consortium’s Technology and Society domain leader, describes: “The privacy policy you probably have personally is really very simple: ‘Don’t do anything creepy to me.’”

Roessler says a recent round of publicized privacy vulnerabilities on prominent websites has led technologists, regulators, and end users all to begin asking more detailed questions about how to achieve that ideal: what data leaves a user’s computer, what another party can observe about that user via that data, and then, vitally, what that party does do with it.

“As a community, we are struggling very much with that,” Roessler says. “The traditional approach has been that on a website you have a privacy policy, and the typical user has probably read at most one that is terribly convoluted and then probably gave up.

“The challenge we are facing is both for providers of services and developers of user agents to figure out how can we develop a scenario in which the user actually understands what will happen to their data — how can we get to the point where a site will explain succinctly, concisely, briefly, and simply to the user what is happening with the user’s data? That is a recurring theme in a lot of these discussions.”

Attaining Simplicity, Not So Simple

Two trends in particular might be most responsible for what will likely be an intense new focus on improving the technology and policy around privacy in the coming months. The first is the increasing deployment of technologies comprising the new HTML standard, dubbed HTML5, which have received scrutiny in both trade and popular press outlets (coverage that often misses the mark, according to veteran developers). The second is a proposal by the US Federal Trade Commission (FTC) for a mandated “do not track” capability on browsers (www.ftc.gov/opa/2010/12/dnttestimony.shtm).

“Consumers are not likely to be aware of the technical limitations of existing control mechanisms,” David Vladeck, director of the FTC’s Bureau of Consumer Protection, testified before Congress on 2 December 2010. “For example, they may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms.

“Given these limitations, the [FTC] supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as ‘Do Not Track.’ The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer’s browser, and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.”

However, Vladeck also admitted in his testimony that there are myriad avenues by which advertisers or other entities interested in tracking users can put tracking technology on a machine. In fact, a story reported by The New York Times on 10 October 2010 featured new capabilities in the latest version of HTML that allowed a persistent cookie dubbed Evercookie, developed by Samy Kamkar, to remain entrenched on a machine even if a user executed a “delete cookies” command (www.nytimes.com/2010/10/11/business/media/11privacy.html?_r=1&page_wanted=all).

Unfortunately, according to developers who’ve been involved in drafting or discussing the new HTML specification, the story also failed to mention that Evercookie used other technologies that had nothing to do with HTML5, while vaguely implying that the new HTML spec was an all-of-a-piece product such as an operating system or application that went through development, beta testing, and public release. Instead, these developers say the privacy implications around various elements of HTML5 should be far more granularly focused on each of those...
elements—and that the community of stakeholders must be increased for the discussion around those elements to succeed.

“It’s easy to make a sensational headline about Evercookie, but those things are small potatoes compared to what somebody can do if they have your data on a server and can give it willy-nilly to a partner—and there’s nothing about HTML5 that changes that,” says Yehuda Katz, one of the Ruby on Rails team’s core developers. “Most people don’t recognize the extent to which existing technology is used.”

For example, Katz says, a recent story in The Wall Street Journal raised alarms about referrer headers, which pinpoint the site from which a Web user arrived to a second site (http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html).

“The sad thing is you always get a referrer header,” Katz says. “It doesn’t matter what site you’re on, the other site gets your information. That’s how the Web works. It’s important for people not to include information in the URL that’s potentially sensitive. But it’s not new, it’s not like Facebook is providing information to ads. Facebook is doing what everyone does.”

Heat on the Browsers

The confusion surrounding which pieces of a user’s hard drive and network interface present the most potential vulnerabilities might be best exemplified by the persistent cookie example and the partial solutions, not particularly well publicized, most browsers already offer.

“Private browsing,” for example, is a feature of the latest releases of Internet Explorer, Firefox, Opera, and Safari (Google’s Chrome browser calls private browsing “Incognito”). This mode essentially keeps browser history, search history, download history, Web form history, cookies, and temporary Internet files from being logged onto the computer in use. However, tracking mechanisms placed on a computer by a plug-in, such as Flash, won’t be affected by private browsing mode, as illustrated by research conducted by Anonymizer.

“Flash stores data outside the scope of an individual browser, and private browsing mode doesn’t stop this from happening,” the company posted on its website (www.anonymizer.com/learningcenter/#ic_labs). “If you have both Firefox and Internet Explorer installed, and you visit a page in IE that uses Flash storage, the page will remember you even when you visit it in Firefox or another browser on the same computer. Flash storage objects are browser independent. This is also true of Microsoft Silverlight data objects.”

Browser vendors could possibly inform users about the vectors they can use to clear tracking technology. However, Mike Shaver, vice president of engineering for Firefox developer Mozilla, says such a strategy is problematic, especially given the anonymous nature of browser downloading for open source and free browsers.

“We should be doing a better job of surfacing information about how to use the browser to protect your privacy,” he says. “The only place you can have the logic to clear those things is in the browser, and we are working with plug-in vendors and our own implementations of the standards. It’s not something we can wake up in the morning and say, ‘That’s what we should do’ and do it, but it is the direction we’re moving in.”

“We are the user’s agent. They just want to get clean, and there should be a way for them to do that without having to understand what’s in HTML5, what’s in a particular storage spec, or Flash. That’s the direction we’re heading in; you’ll
see a lot of improvements in that in Firefox 4."

Katz believes there should be some sort of working group dedicated to cross-browser capabilities and responsibilities, in which security researchers and journalists have equal access with developers and standards writers.

“There should be a more concerted effort for people who are writing the sensational stories to participate in that process, and there isn’t a good injection point for that,” Katz says. “For example, there is no W3C user agent security task force — so I think journalists and security researchers belong as part of that.”

Cross-Organizational Communication at Cross Purposes?

In fact, the W3C, the Internet Society, the Internet Architecture Board, and the Massachusetts Institute of Technology cosponsored a privacy workshop to discuss these issues and others in December 2010. But one industry veteran says the idea of a cross-platform privacy mechanism failed once before — with the result that one prominent megasite, Facebook, has become the de facto privacy manager for many Web users because so many people not only sign into it directly, but also link to it and jump to other sites following other users’ links.

“We basically had people who really cared about privacy go off in [the] corner and develop a very complex technology, P3P (Platform for Privacy Preferences),” says Michael Mullany, vice president for products at Sencha, an application framework vendor. “And browser makers, though everyone thought it was a terrible idea, were pressured into implementing it. Nobody could figure out how to use it, either on websites or on the browser side, and we ended up basically selling our privacy to Facebook, and assuming that a big enough, important enough, and valuable enough company wouldn’t do something completely irresponsible with our private data.”

Both Mullany and Mozilla’s Shaver say that the standardization process around HTML5 has focused the entire Web development community around these new technologies and has beneficially re-emphasized the talk around privacy. But Mullany and Ian Hickson, the HTML specification’s editor, also say that, unless end users are willing to abdicate responsibility for their own experience on the Internet, they must also educate themselves.

“Ultimately, the whole notion of privacy is being master of your own fate and data,” Mullany says. “There’s a certain responsibility on the shoulders of individuals that if you care about this, you’ll learn about it. Otherwise, you’re relying on Facebook to take care of your privacy for you.”

“HTML really is the least problematic part of the stack as far as user tracking goes,” Hickson says. “Explaining user tracking risks, mitigations, and so forth, is a very hard problem, and I’ve no idea what the right long-term solution is.”

Greg Goth is a freelance technology writer based in Connecticut.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

Privacy Gets a New Round

cont. from p. 14

the “best superfast broadband network in Europe by 2015.” Among the plans announced in the new Britain’s Superfast Broadband Future report, Hunt spoke of “digital hubs” in every UK community. The nation’s new network will offer a foundation, Hunt said, for “new economic dynamism, creating hundreds of thousands of jobs and adding billions to our GDP.”


In a new report on climate change and the use of information and communication technologies (ICT), the International Telecommunications Union and Global e-Sustainability Initiative cite key ways to mitigate the effects of climate change and thereby take a critical step toward achieving sustainable development. Among the recommended approaches are to drive down ICT sector emissions and use energy-efficient ICT-based systems to monitor the global weather and environment and rapidly disseminate the resulting data. The report notes that saving one watt of energy each for one billion ICT equipment users eliminates the need for an entire power plant.

The report is available at www.itu.int/ITU-T/climatechange/itu-gesi-report.html.

After weeks of threats, the Apache Software Foundation officially resigned from the Java SE/EE Executive Committee (EC) on 9 December after 10 years of service. The resignation comes in the wake of a recent Java SE 7 vote, which Apache said was “the last chance” for the JCP EC to show its intent to defend the JCP as an open specification process.

More details are available at https://blogs.apache.org/foundation/entry/the ASF resigns from the.