Researchers find leaky apps that put privacy at risk

March 22 2018, by Allie Nicodemo

Credit: Northeastern University

A bug in Facebook's advertising platform made it possible for potential hackers to uncover users' phone numbers, according to a paper presented by Northeastern associate professor Alan Mislove at the the Federal

Trade Commission conference PrivacyCon last month.

The Facebook advertising system is incredibly effective at targeting specific audiences, which is what has made the company so lucrative, Mislove said. But because anyone can become an advertiser, and there is very little transparency in what ads are being placed, the platform "could be used for nefarious purposes," Mislove said. He demonstrated how in his own research.

In earlier versions of the Facebook ad platform, advertisers could target people based on traits and preferences. For example, a company selling waterproof speakers might set up ads to target men and women aged 16 to 40 who have an interest in swimming, boating, or water sports.

Facebook has updated the system to give advertisers the option to create custom audiences based on an existing customer list. That means a company could upload a database of email addresses to Facebook, and the platform will find any corresponding users on the site and serve those users an ad.

Many Facebook users choose not to make their email addresses or phone numbers public. And the Facebook ad system is not designed to let advertisers learn users' identities based on private information. But Mislove found that by creating multiple custom audiences, he could cross-reference and match up users to their private information.

Mislove and his colleagues alerted Facebook to the bug. It was fixed, and the researchers received $5,000 through the bug bounty program. But the ad feature is not unique to Facebook, Mislove explained. LinkedIn, Twitter, and other platforms have similar custom audience capabilities. "Our worry is that these could be inadvertently leaking information," Mislove said. "We wanted to call attention to the complexity of these systems and the ways they can be abused."

Another Northeastern group, led by doctoral student Michael Weissbacher, also presented research at PrivacyCon. Weissbacher showed that dozens of popular browser extensions were leaking users' web history.

Weissbacher and his team created a tool called Ex-Ray to detect data leaks based on network traffic. They found that the larger a user's browser history, the more data was being leaked. Ex-Ray identified 32 browser extensions—used by a combined total of 8 million people—that were actively leaking web history data. These included popular extensions like AdBlocker for Google Chrome, and Speak It, a text-to-speech extension.

Weissbacher said Google removed many—but not all—of the extensions from its web store after learning they leaked browser history. He added that the creators of these extensions may not have been aware they leak. However, the web store should assume responsibility for scanning the extensions to ensure they are secure, Weissbacher said. Until then, he recommends users delete extensions they don't regularly use in order to reduce the risk of privacy violations.

"Whether the leaks are happening maliciously or inadvertently, it's still exposing the user," Weissbacher said.

Privacy is also a concern on mobile platforms. Jingjing Ren, a doctoral student in computer science, presented research at PrivacyCon showing that some Android applications have become less secure over time. Her team discovered 13 apps that leaked users' personal information in at least one version of the app.

"One notable example is Pinterest," Ren said, referring to a popular app for uploading and saving a variety of content. Pinterest's mobile app has about 140 million active users. "In two versions we investigated, the app

accidently sent users' credentials to an undisclosed third party that seemed to provide user interface services for Pinterest."

Ren said the developers at Pinterest fixed the problem within a month of her team finding and disclosing it. However, four other apps— Meet24, FastMeet, Waplog, Period & Ovulation Tracker—have yet to address their privacy leaks.

"At the end of day, mobile privacy is still an ongoing conversation among consumers, app developers, app distribution platforms, third parties, policy makers, and other stakeholders," Ren said.

Provided by Northeastern University