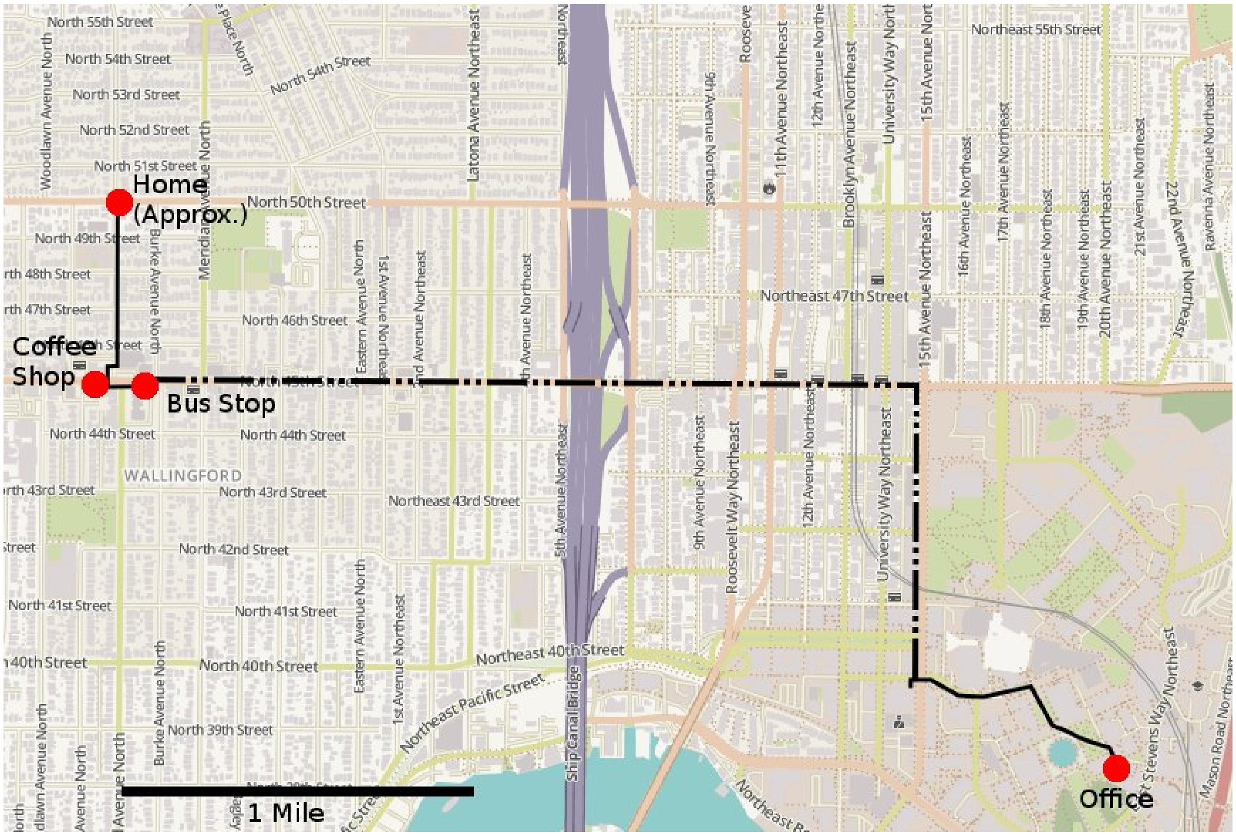
TechXplore

For $1000, anyone can purchase online ads to track your location and app use

October 18 2017, by Jennifer Langston



This map represents an individual's morning commute. Red dots reflect the places where the UW computer security researchers were able to track that person's movements by serving location-based ads: at home (real location not shown), a coffee shop, bus stop and office. The team found that a target needed to stay in one location for roughly four minutes before an ad was served, which is why no red dots appear along the individual's bus commute (dashed line) or walking route (solid line.) Credit: University of Washington

Privacy concerns have long swirled around how much information online advertising networks collect about people's browsing, buying and social media habits—typically to sell you something.

But could someone use mobile advertising to learn where you go for coffee? Could a burglar establish a sham company and send ads to your phone to learn when you leave the house? Could a suspicious employer see if you're using shopping apps on work time?

The answer is yes, at least in theory. New University of Washington research, to be presented in a paper Oct. 30 at the Association for Computing Machinery's Workshop on Privacy in the Electronic Society, suggests that for roughly $1,000, someone with devious intent can purchase and target online advertising in ways that allow them to track the location of other individuals and learn what apps they are using.

"Anyone from a foreign intelligence agent to a jealous spouse can pretty easily sign up with a large internet advertising company and on a fairly modest budget use these ecosystems to track another individual's behavior," said lead author Paul Vines, a recent doctoral graduate in the UW's Paul G. Allen School of Computer Science & Engineering.

The research team set out to test whether an adversary could exploit the existing online advertising infrastructure for personal surveillance and, if so, raise industry awareness about the threat.

"Because it was so easy to do what we did, we believe this is an issue that the online advertising industry needs to be thinking about," said co-author Franzi Roesner, co-director of the UW Security and Privacy Research Lab and an assistant professor in the Allen School. "We are sharing our discoveries so that advertising networks can try to detect and mitigate these types of attacks, and so that there can be a broad public discussion about how we as a society might try to prevent them."

The researchers discovered that an individual ad purchaser can, under certain circumstances, see when a person visits a predetermined sensitive location—a suspected rendezvous spot for an affair, the office of a company that a venture capitalist might be interested in or a hospital where someone might be receiving treatment—within 10 minutes of that person's arrival. They were also able to track a person's movements across the city during a morning commute by serving location-based ads to the target's phone.

The team also discovered that individuals who purchase the ads could see what types of apps their target was using. That could potentially divulge information about the person's interests, dating habits, religious affiliations, health conditions, political leanings and other potentially sensitive or private information.

Someone who wants to surveil a person's movements first needs to learn the mobile advertising ID (MAID) for the target's mobile phone. These unique identifiers that help marketers serve ads tailored to a person's interests are sent to the advertiser and a number of other parties whenever a person clicks on a mobile ad. A person's MAID also could be obtained by eavesdropping on an unsecured wireless network the person is using or by gaining temporary access to his or her WiFi router.

The UW team demonstrated that customers of advertising services can purchase a number of hyperlocal ads through that service, which will only be served to that particular phone when its owner opens an app in a particular spot. By setting up a grid of these location-based ads, the adversary can track the target's movements if he or she has opened an app and remains in a location long enough for an ad to be served—typically about four minutes, the team found.

Importantly, the target does not have to click on or engage with the ad—the purchaser can see where ads are being served and use that information to track the target through space. In the team's experiments, they were able to pinpoint a person's location within about 8 meters.

"To be very honest, I was shocked at how effective this was," said co-author Tadayoshi Kohno, an Allen School professor who has studied security vulnerabilities in products ranging from automobiles to medical devices. "We did this research to better understand the privacy risks with online advertising. There's a fundamental tension that as advertisers become more capable of targeting and tracking people to deliver better ads, there's also the opportunity for adversaries to begin exploiting that additional precision. It is important to understand both the benefits and risks with technologies."

An individual could potentially disrupt the simple types of location-based attacks that the UW team demonstrated by frequently resetting the mobile advertising IDs in their phones—a feature that many smartphones now offer. Disabling location tracking within individual app settings could help, the researchers said, but advertisers still may be capable of harvesting location data in other ways.

On the industry side, mobile and online advertisers could help thwart these types of attacks by rejecting ad buys that target only a small number of devices or individuals, the researchers said. They also could develop and deploy machine learning tools to distinguish between normal advertising patterns and suspicious advertising behavior that looks more like personal surveillance.

More information: Paper: adint.cs.washington.edu/ADINT.pdf

Provided by University of Washington

Citation: For $1000, anyone can purchase online ads to track your location and app use (2017, October 18) retrieved 20 March 2024 from https://techxplore.com/news/2017-10-online-ads-track-app.html