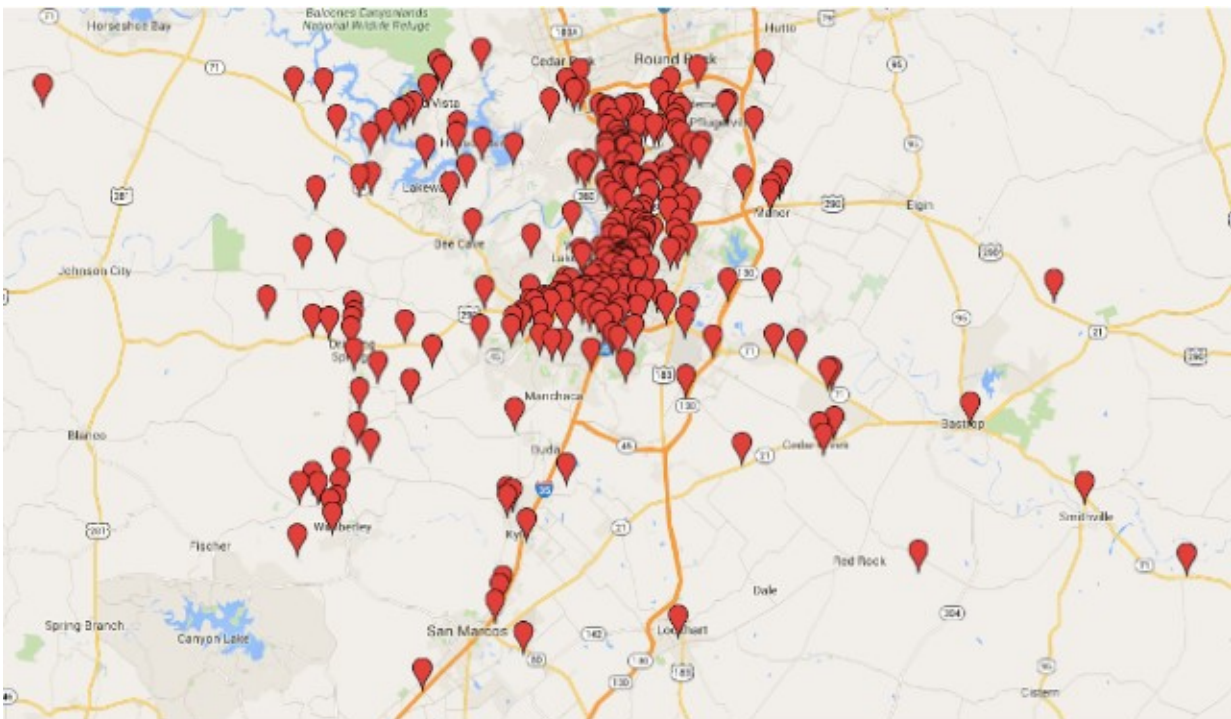# Shortened URLs may open a window on your life

May 24 2016, by Bill Steele

Map directions obtained by scanning short URLs show locations visited by a single user in Austin, Texas.

It may be convenient to shrink a long, convoluted web address into just a few characters that will fit into a tweet, but the trend of using shortened URLs offers a new opportunity for hackers to invade your privacy, Cornell Tech researchers warn.

URLs for photos or news postings, for example, can run to several lines of miscellaneous characters, a challenge to type in by hand and often broken into separate lines in an e-mail. So services like bit.ly will generate a short address consisting of six or more random letters and numbers – something like "bit.ly/abc123xyz}" – that redirect to the site.

But a computer can easily be programmed to generate such random strings of characters and try out each one as a web address until it gets a hit.

It's not a big problem if a hacker finds a link to a YouTube video you wanted to share, but cloud-based file storage services such as Microsoft OneDrive and Google Drive use URL shortening for links to your documents.

"Online resources that were intended to be shared with a few trusted friends or collaborators are effectively public and can be accessed by anyone," explained Vitaly Shmatikov, a Cornell Tech professor of computer science. Shmatikov is one of four faculty members at Cornell Tech specializing in security and privacy, in collaboration with several on the Ithaca campus.

Google Maps creates short URLs for its driving directions, which could reveal a lot of personal information: where you live and who your friends are, for starters, and what businesses or services you work with. A map might show visits to an addiction treatment center, for example.

As a demonstration, Shmatikov and doctoral student Martin Giorgiev generated and tested more than 42 million six-character short URLs and found 2,130 that led to live files on OneDrive. They were careful not to read or save any of them. From the addresses, they noted, they could find all other files belonging to the same user. One hit could lead to another 200 or so files, Shmatikov said.

Cloud storage services allow users to edit their files via the web. Many of the files the researchers discovered were "writeable," so a visiting hacker could insert malicious content, such as a Word macro virus. It might also be possible to upload completely new files to the storage area, including malware. Cloud storage services continuously sync with a user's computer, phone or other device, so malware might automatically be downloaded to the user's device.

The researchers offer several suggestions to service providers:

- Make the URLs a little longer, forcing intruders to spend a lot more time and effort. With a 10-character string, the researchers said, It would be 15 million times harder to find a working link than it is with 6-character URLs.
- Cloud storage services offer the option to shorten URLs, and many users happily accept, but the offer should come with a warning that the choice might have a downside.
- Cloud services should generate their own short URLs, rather than relying on services that have publically accessible databases.
- URL shortening services should be alert for massive scans of their databases.
- Cloud storage providers should change their systems so it is no longer possible for an intruder to go from one discovered file to all the other files belonging to the same account.

Since their warning appeared, the researchers reported, Google has lengthened the URLs of its map links and Microsoft has dropped the "shorter URL" option for OneDrive users (causing users to complain). A lot of other problems have been fixed in various ways, but the thought to keep in mind: "Any document shared on a cloud service is effectively public."

Sharing a link to cloud-based documents can be safe, Shmatikov said,

but only if proper precautions are taken, like having access control and requiring users to authenticate before accessing the document.

Provided by Cornell University