

GeoGraphical Passwords



A study on cybersecurity suggests that visual map-based passwords would make life harder for thieves but easier for the rest of us who struggle to remember jumbles of letters and numbers. But will users just get frustrated? Adena Schutzberg considers the challenges and potential benefits for our industry.

I read about research recently that suggests using map locations as part of a computer security protocol in place of traditional passwords. The idea is that memorable places or patterns on maps could stand in for the strings of numbers and letters that we currently use. Cybersecurity researcher Ziyad S. Al-Salloum hopes to make the passwords easier to remember and harder for online thieves to crack. The new codes are called “GeoGraphical” passwords.

An actual implementation might present a new website visitor with an online map where the account creation “Input password” field might have been. The to-be account holder would have to create a map-based visualisation they could reproduce on a return visit. A runner might draw a rectangle around the high school track. Then, each time she returns to the site, she’d need to create the same drawing, within a tolerance, for re-entry in the account.

The Variables

A study suggests that these maps might be easier to remember and use than the current solutions because humans are better at remembering places than meaningless strings. From a personal standpoint, the tricky part might be remembering which place relates to which website. It’d be easy for me to draw a circle around my dorm at my college to gain access to my alumni e-mail account, but how would I associate a 1980 trip to Europe with my Facebook page?

The actual navigation to the place of interest and drawing the graphics around it provides a number of variables that create long alphanumeric strings in the background. Among the variables are the location, zoom level and the size, shape and angle of the figure that’s drawn. Another benefit: the complexity of these passwords might mean they need to be changed far less often.

Increasing Spatial Literacy

There are a number of reasons the GeoGraphical password approach is appealing. First off, everyone will have a different set of geographies to use as the basis of their new passwords. Individuals could tap into places they’ve lived at a variety of scales. They might use their own or, perhaps even better, the home of a childhood friend. Or they might identify and enclose the boundary of the first county they visited outside of their own. Other options might include all the places an individual wants to visit. Baseball aficionados could use ballparks while opera fans might include opera houses. It’s fun to just think about creating such passwords, isn’t it?

Second, this is a great way to increase spatial literacy. The requirement to look at a map, even a map of the same place, regularly turns on the spatial thinking part of the brain. Moreover, a clever implementation of these GeoGraphical passwords could also help teach geography. An optional “gamification” enhancement might offer a geographic tidbit at each visit. Visitors might be asked, after inputting the password, to locate Tanzania or explore patterns of homelessness in a European city. These short learning experiences might enhance the return on investment on a visit to a social media website.

The Bottom Line

The big challenge to this kind of solution, of course, is how well it’s implemented. Will it be easy for applications or websites to include in their code base? Will users be able to navigate a password that involves a map creation and drawing with ease? Will there be a reasonable “margin of error” so that users are not frustrated? Will users consider it “fun” at the outset and for the long term? And, of course, there is the bottom line: will using such a system help prevent breaches that cost online organisations significant revenue?

Maps are tools used to answer questions and solve many problems. In the future, they might address the challenges of computer users’ weak and easily forgotten passwords.

This article was published in GIS Professional April 2014