Geographical passwords worth their salt

14 February 2014

It's much easier to remember a place you have visited than a long, complicated password, which is why computer scientist Ziyad Al-Salloum of ZSS-Research in Ras Al Khaimah, UAE, is developing a system he calls geographical passwords.

Writing in a freely available "open access" research paper in the *International Journal of Security and Networks*, Al-Salloum emphasizes how increasingly complicated our online lives are becoming with more and more accounts requiring more and more passwords. Moreover, he adds that even strong, but conventional passwords are a security risk in the face of increasingly sophisticated "hacker" tools that can break into servers and apply brute force to reveal passwords. Indeed, over the last few years numerous major corporations and organizations - LinkedIn, Sony, the US government, Evernote, Twitter, Yahoo and many others - have had their systems compromised to different degrees and overall millions of usernames and associated passwords have been harvested and even leaked online.

Al-Salloum has devised geographical passwords as a simple yet practical approach to access credentials that could provide secure access to different entities and at the same time mitigate many of the vulnerabilities associated with current password-based schemes. The new "geo" approach exploits our remarkable ability to recall with relative ease a favorite or visited place and to use that place's specific location as the access credentials. The prototype system developed at ZSS – Research has proven itself capable of protecting a system against known password threats. "Proposing an effective replacement of conventional passwords could reduce 76% of data breaches, based on an analysis of more than 47,000 reported security incidents," Al-Salloum reports.

The geographical password system utilizes the geographical information derived from a specific memorable location around which the user has logged a drawn boundary- longitude, latitude, altitude, area of the boundary, its perimeter, sides, angles, radius and other features form the geographical password. For instance, the user might draw a six-side polygon around a geographical feature such as the Eiffel Tower, Uluru (also known as Ayer's Rock), a particular promontory on the Grand Canyon, a local church, a particular tree in the woodland where they walk their dog…or any other geographical feature. Once created, the password is then "salted" by adding a string of hidden random characters that are user-specific and the geographical password and the salt "hashed" together. Thus, even if two users pick the same place as their geographical password the behind-the-scenes password settings is unique to them.

If the system disallowed two users from picking the same location, this will make it much easier for adversaries to guess passwords.

The guessability, or entropy, of a geographical password would increase significantly if the password comprised two or more pinpointed locations. Al-Salloum explains that a whole-earth map might have 360 billion tiles at 20 degrees of "zoom", which offers an essentially limitless number of essentially unguessable geographical passwords .

More information: "GeoGraphical passwords" in *Int. J. Security and Networks*, 2014, 9, 56-62. A PDF of the peer-reviewed research paper is available via Open Access to everyone here: www.inderscience.com/admin/osp … 48952&fromonsusy=yes

Provided by Inderscience Publishers