SecureIDNews

January 24, 2014

The quest for a 'friction-less' authentication system

By Zach Martin

When discussing different identification or authentication technology, the term "friction" is often heard. This doesn't refer to the act of physically rubbing a token on to laptop or smart phone, but rather how much more difficult authentication technology is going to make it to gain access to a web site or service.

User names and passwords aren't a great authentication mechanism, but unless an individual can't remember them, they work. The problem with longer, complex passwords are the added friction.

Simply put, no authentication scheme is without some friction. But the aim of technology providers and the replying parties who will deploy these new systems is to develop a scheme that is as friction-less as possible.

Kenneth Weiss, developer of the token-based authentication technology that became RSA's SecurID, is working on a smart phone app that would enable users up to three-factor authentication to a laptop or PC – with no additional hardware. "You're protecting your device with something you already have," says Weiss, now founder and CEO at Universal Secure Registry.

After downloading an app to a handset and computer, authentication would be performed via Bluetooth, Weiss says. The individual would authenticate to the handset and app with a PIN or passcode, which would then authenticate to the computer for two-factor security. If the handset had a biometric reader– like the iPhone 5s – then it would be three-factor security.

The handset would send a passcode to the computer via Bluetooth every 30-seconds offering continuous authentication, Weiss says. When out of range the computer would be locked. The app could also be set up for mutual authentication, meaning that not only would the handset authenticate to the computer, but also the computer could authenticate to the handset.

While the app will initially be used for access to computers, there are plans to create an API so that it can be enabled for access to web sites and secure networks as well, Weiss says. Users could be automatically logged into sites and networks that accept the authentication technology.

Additionally, there are plans afoot for an enterprise version of the app that would also enable multiple encryption seeds. A user would be able to use different seeds for different reasons. For example, he might choose one seed for use at home and another for work, Weiss says.

Universal Secure Registry also plans to change the seeds on a periodic basis, Weiss explains. If a seed is compromised through a breach – as with the case with RSA some years ago – it could automatically be changed. Also, in the case of lost handset, the app can be destroyed remotely.

Battery life is always a concern with smart phones and Weiss says the Bluetooth use won't produce negative effects. The latest Bluetooth 4 specification, which is used by the most recent iPhones and Android handsets, has very low battery consumption and won't impact overall life.

Universal Secure Registry is working on apps for both iOS and Android and is hoping for a release some time in the second quarter of 2014, Weiss says. The system will also be designed to support cross-platform computing, i.e. an iOS device on a Windows machine and Android on an Apple operating system, etc

###

http://secureidnews.com/news-item/the-quest-for-a-friction-less-authentication-system/#