Passwords no more? Researchers develop mechanisms that enable users to log in securely without passwords

June 4 2014, by Katherine Shonesy

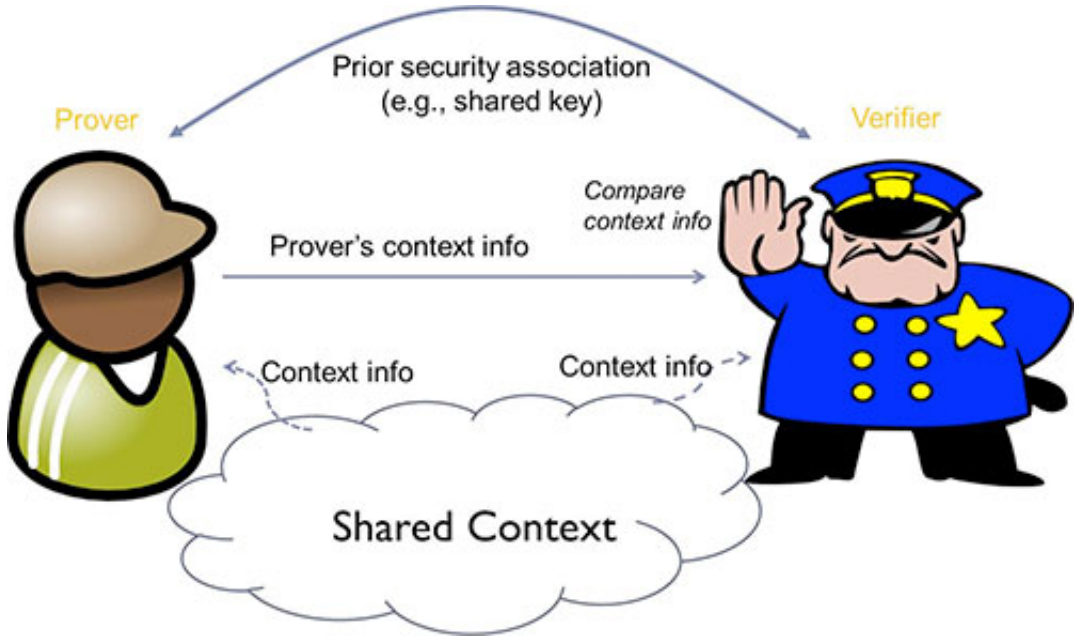
(Phys.org) —Passwords are a common security measure to protect personal information, but they don't always prevent hackers from finding a way into devices. Researchers from the University of Alabama at

Birmingham are working to perfect an easy-to-use, secure login protection that eliminates the need to use a password—known as zero-interaction authentication.

The research is led by Nitesh Saxena, Ph.D., associate professor in the Department of Computer and Information Sciences and co-leader of the Center for Information Assurance and Joint Forensics Research. The work, in collaboration with the University of Helsinki and Aalto University in Finland, was recently presented during the International Conference on Pervasive Computing and Communications and the Financial Cryptography and Data Security conference.

Zero-interaction authentication enables a user to access a terminal, such as a laptop or a car, without interacting with the device. Access is granted when the verifying system can detect the user's security token—such as a mobile phone or a car key—using an authentication protocol over a short-range, wireless communication channel, such as Bluetooth. It eliminates the need for a password and diminishes the security risks that accompany them.

A common example of such authentication is a passive keyless entry and start system that unlocks a car door or starts the car engine based on the token's proximity to the car. The technology also can be used to provide secure access to computers. For instance, an app called BlueProximity enables a user to unlock the idle screen in a computer merely by physically approaching the computer while holding a mobile phone that has been set up to connect with it.



However, existing zero-interaction authentication schemes are vulnerable to relay attacks, commonly referred to as ghost-and-leech attacks, in which a hacker, or ghost, succeeds in authenticating to the terminal on behalf of the user by colluding with another hacker, or leech, who is close to the user at another location, Saxena says.

"The goal of our research is to examine the existing security measures that zero-interaction authentication systems employ and improve them," Saxena said. "We want to identify a mechanism that will provide increased security against relay attacks and maintain the ease of use."

The researchers examined two types of sensor modalities that could protect zero-interaction systems against relay attacks without affecting usability. First, they examined four sensor modalities that are commonly present on devices: Wi-Fi, Bluetooth, GPS and audio. Second, they looked at the capabilities of using ambient physical sensors as a

proximity-detection mechanism and focused on four: ambient temperature, precision gas, humidity and altitude. Each of these modalities helps the authentication system verify that the two devices attempting to connect to each other are in the same location and thwart a ghost-and-leech attack.

The research showed that sensor modalities, used in combination, provide added security. "Our results suggest that an individual sensor modality may not provide a sufficient level of security and usability," Saxena said. "However, multiple modality combinations result in a robust relay-attack defense and good usability."

Platforms that employ sensor modalities to prevent relay attacks in mobile and wireless systems are available on many smartphones or can be added using extension devices, and they will likely become more commonplace in the near future, Saxena says.

"Users will be able to use an app on their phones to lock and unlock their laptops, desktops or even their cars, without passwords and without having to worry about relay attacks," said Babins Shrestha, a UAB doctoral student and co-author on the papers. "Our research shows that this can be done while preserving a high level of usability and security."

More information: www.percom.org/

Provided by University of Alabama at Birmingham