Archived Content

SMARTPHONES THAT CAN AUTOMATICALLY IDENTIFY USERS

DHS research into continuous authentication will take security to whole new level

By Vincent Sritapan

In today's connected world, mobile technology provides law enforcement with the means to access critical information at any time, from any location. Most law enforcement officers already carry a department-issued mobile phone, and with the right enterprise security, these devices can provide significant operational benefits to individual officers, as well as their agencies.

Smartphones now include a rich set of features, with numerous sensors to support logistics, coordination, and real-time access to sensitive information, as well as to enable data collection.

A critical aspect of making mobile technology work for the law enforcement community is ensuring the right person has the right access when he or she needs it. A simple compromise could jeopardize the reliability of information, confidentiality of law enforcement operations, and much more. The confidentiality, integrity, and availability of mobile devices, applications, and data must be safeguarded.

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is conducting applied research and development (R&D) on continuous authentication to strengthen security. Continuous authentication is the method of leveraging the various sensors built into smartphones to automatically identify users based on their behavior to create a trust model to grant scalable access. Through the R&D of continuous authentication, law enforcement officers soon will have new technology to ensure greater mission security and provide reliable access without hindering the overall mobile experience.

The password dilemma

Traditionally, IT departments require strong authentication for access to sensitive information. However, strong passwords are not the only answer. Passwords can be shared, hacked, and/or guessed. And once someone has unauthorized access to a mobile device, access to applications or enterprise data is traditionally left open to anyone in possession of the compromised device.

> "A critical aspect of making mobile technology work for the law enforcement community is ensuring the right person has the right access when he or she needs it."

What is more troublesome is that mobile users who are forced to use passwords are likely to choose ones that are short or easy to remember. The dilemma of requiring pass-

words is between allowing weak passwords for ease of use, or enforcing long, complex passwords that are cumbersome to the user and may negatively impact the mission, especially if the officer has to look one up.

Equipment is another challenge for the law enforcement community; officers may need to wear gloves or carry heavy equipment, which could introduce an obstacle to entering passwords on smartphones. The answer to the password dilemma lies with continuous authentication.

Innovating to achieve continuous authentication

The capability and reliability of today's mobile device sensors offer a unique opportunity to obtain higher levels of security without hindering the mobile experience or the officer's ability to execute his or her mission. DHS S&T is taking advantage of this to develop new technologies in both hardware and software to achieve continuous authentication on modern smartphones.

In a continuous authentication system, while a person is using his or her mobile device, its environmental characteristics—such as networks, connections, and sensors—are monitored to create a user profile that then becomes the norm. The technology continuously compares the normal device profile to real-time, measured usage patterns to continuously update system confidence regarding the authenticity of the user.

The level of required authentication within the technology is based on the user's level of interaction with the mobile device. As more sensitive tasks are performed, the user will have a higher authentication level that ensures information is safe. This technology will enable organizations to set higher levels of authentication confidence per user to protect the mobile device and the enterprise system from imposters.

Conclusion

Law enforcement already is taking advantage of the significant benefits—including convenience, increased efficiency, and lower costs—that mobile device technology provides to policing functions.

Within the next two years, continuous authentication technology for smartphones is planned for the commercial market. At that time, police agencies will be able to deploy continuous authentication in existing smartphones via software addition(s) and integrate the technology into their enterprise security solutions to provide officers the best possible resources.

The implementation of the technology would need only minimal setup and training for a seamless user experience. The agency's IT experts can set the appropriate level of security authentication and then step aside as the officer and the device interact to automatically establish a secure, automatic identity login.

The continuous authentication technology currently being developed by DHS S&T will ensure easier access to devices by officers and decrease the likelihood that the sensitive information stored on their phones will fall into the wrong hands.

For more information, visit *dhs.gov/science-and-technology/csd-mds.*

Vincent Sritapan is program manager for mobile device security in the Department of Homeland Security Science and Technology Directorate's Cyber Security Division.

DHS S&T currently is developing mobile device security solutions in the following project areas:

R&D Performer	Title	Approach
HRL Laboratory	Continuous Behavior-Based Authentication for Mobile Devices	A neuromorphic hardware chip uses early warning signals to identify users based on gait technology (e.g., how a user walks while carrying the device). Starting with only 60 seconds of movement, this chip can learn from the user's behavior to detect anomalies and identify the user with a confidence level above 90 percent.
Kryptowire	Quo Vadis: A Framework for Mobile Device and User Authentication	This is an Android software approach to using movement, touch, battery usage, geolocation information, and more to profile a user for strong authentication. The on-device sensor system learns to authenticate and authorize a user based on the level of trust generated. It requires a minimum of 10 minutes to train the device.
IBM	Multi-Modal Mobile Security Management for User Behavior Anomaly Detection and Risk Estimation	This is an iOS software (with graphics processing unit acceleration) approach that supports automated identification of sensitive information (i.e., image-to-text and object-to-context). It tracks user identification using geolocation information and user behavior to detect anomalies and set risk detection.
United Technologies Research Center	ASTRA: Context-Aware Security Technology for Responsive and Adaptive Protection	This is a cloud-based approach that leverages device sensors to automatically identify the user and provide adaptive protections to grant varying access. This technology can be used beyond smartphones for electronic locks and "smart" cities.