Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M18-206P^
Published: 8/4/2022

Inventors

Yanchao Zhang

Dianqi Han

Contact

Shen Yan
shen.yan@skysonginnovations.com

Secure Zero-Effort Two-Factor Authentication for Mobile Devices

Mobile two-factor authentication (2FA) has become common for user verification and secure sign-in. Mobile 2FA adds a smartphone or other mobile device as a second layer of security for accessing online accounts, in addition to the traditional username and password. After a user enters a username and matching password, the online system will grant access only upon successful verification of a pre-registered mobile device. Recent efforts attempt to improve the usability of mobile 2FA schemes by eliminating required interactions with the user. Techniques include leveraging automated communication protocols between the registered phone and login device. However, these methods may be susceptible to (1) the so-called "man-in-the-middle" attack, in which an adversary stealthily relays messages between the enrolled mobile phone and an adversarial remote login device, and (2) the co-located attack, in which the adversarial remote login device is located near the enrolled mobile phone and can thus bypass proximity-based checks.

Researchers at Arizona State University have developed a novel two-factor authentication system that requires zero user effort. This is achieved by fully automating user-response transmission via high-frequency acoustic signals inaudible to humans. Specifically, the speaker of the enrolled phone emits acoustic signals that contain the user response; the login device receives these signals through its microphone and decodes the user response which is sent to the online system for verification.

Issued U.S. Pat. No. 11,436,311

Related Publication: Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication (PDF)

-Potential Applications:

- Mobile device user authentication
- Two-factor authentication

Benefits and Advantages:

- Does not require user interaction with enrolled mobile device
- Effective against main-in-the-middle attacks and co-located attacks
- Easy to implement in web browsers and smartphones
- Easy to integrate into commercial mobile two-factor authentication schemes