Researchers propose novel solution to better secure voice over internet communication

January 29 2018, by Tiffany Westry Womack

Credit: University of Alabama at Birmingham

Researchers at the University of Alabama at Birmingham have developed a novel method to better protect crypto phones from eavesdropping and other forms of man-in-the-middle attacks.

Crypto phones consist of smartphone apps, mobile devices, personal computer or web-based Voice over Internet Protocol applications that

use end-to-end encryption to ensure that only the user and the person they are communicating with can read what is sent. In order to secure what is being communicated, crypto phones require users to perform authentication tasks.

"Research has shown that these tasks are prone to human errors, making these VoIP applications and devices highly vulnerable to man-in-the-middle and eavesdropping attacks, said Nitesh Saxena, Ph.D. associate professor in the UAB College of Arts and Sciences Department of Computer Science.

In a paper published at the Association for Computing Machinery Conference on Computer and Communication Security in November, Saxena and Ph.D. student Maliheh Shirvanian introduce Closed Captioning crypto phones to address the issues in currently deployed crypto phones.

To ensure that a man-in-the-middle attacker does not interfere with the transmission of the message, traditional crypto phones rely on the users to verbally communicate and match a key, called a checksum, that is displayed on each user's device. The users must verify that the voice announcing the checksum is indeed the voice of the other user they wish to communicate with. Closed Captioning crypto phones fully automates checksum comparison.

"Closed Captioning crypto phones remove the human element from the checksum comparison process by utilizing speech transcription," Saxena said.

When a user announces the checksum to the other person CCCP automatically transcribes the spoken code and performs a code or checksum comparison for the user. In an online experiment designed to mimic a real-life VoIP call, more than 1100 audio files containing

4-word and 8-word checksums spoken by a variety people CCCP eliminated the chances of the data being intercepted or captured via a man-in-the-middle attack due to human errors or clicking through the task and complete detection of mismatching checksums was made.

"Our work shows that by automating the checksum comparison verification, users are unburdened by only having to perform a single verification task, Saxena said. CCCP not only eliminates the human errors, but also facilitate use of longer checksums, which further strengthen the security. "This may also help increase the awareness of human users in detecting malicious voice imitation attempts by attackers."

In a study analyzing the security and usability of user-centered code verification tasks, Saxena, Shirvanian and collaborator Jesvin James George, found that most end-to-end encryption code verification methods offer poor security and low user experience ratings. The study was published at the 2017 Annual Computer Security Applications Conference in December.

In a monitored lab setting, 25 participants were asked to perform and report the success or failure of QR, image and numeric code verification while using the internet-based communication applications, Telegram, WhatsApp, Viber and Signal in a close proximity setting and a remote setting. Security and usability security under remote verification settings was found to be significantly lower than in a close proximity code verification setting due to human errors.

Provided by University of Alabama at Birmingham

voice-internet.html