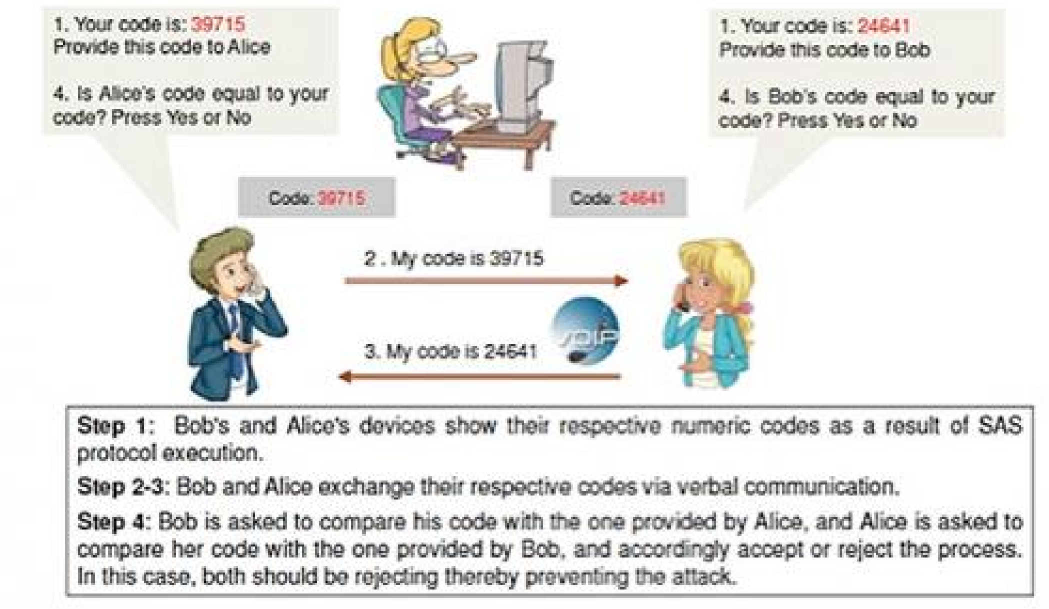
New research shows vulnerability in mobile phones' applications offering voice communication security

November 6 2014, by Katherine Shonesy



Step 1: Bob's and Alice's devices show their respective numeric codes as a result of SAS protocol execution.

Step 2-3: Bob and Alice exchange their respective codes via verbal communication.

Step 4: Bob is asked to compare his code with the one provided by Alice, and Alice is asked to compare her code with the one provided by Bob, and accordingly accept or reject the process. In this case, both should be rejecting thereby preventing the attack.

University of Alabama at Birmingham researchers are explaining why there are concerns with the end-to-end security of an increasingly popular means of communication, and what users can do to defend against potential threats.

Through a project funded by Cisco Systems, researchers in the

Department of Computer and Information Sciences examined the vulnerabilities in security of video- and voice-over-Internet protocol, or VoIP, communications. The team developed attacks that uncovered these vulnerabilities in a currently used security scheme, and once those weaknesses were identified, the team suggested alternatives that may protect against potential attacks.

These results are being presented today at one of the world's top security conferences, the ACM Conference on Computer and Communications Security, held in Phoenix, Arizona.

VoIP systems are becoming one of the most popular means of communication over the Internet. VoIP is used on a variety of devices, including traditional computers, mobile devices and residential phones, enabled by popular applications and services such as Skype, Google Hangouts and Vonage.

Establishing secure VoIP communications is a crucial task necessary to prevent eavesdropping and man-in-the-middle attacks, in which a malicious third party makes independent connections with the victims and intercepts or fabricates messages between them. Such attacks can put each user's device at risk and make confidential information vulnerable.

"Given the surge in popularity of computing devices, ensuring the security of VoIP connections is very important for personal users, and especially for business users," said Nitesh Saxena, Ph.D., associate professor of CIS, a member of the Center for Information Assurance and Joint Forensics Research (CIA|JFR), and the director of the UAB Security and Privacy in Emerging computing and networking Systems (SPIES) research group.

Securing VoIP sessions requires each user to agree upon a shared cryptographic key. Rather than relying on a third-party entity to provide such a key, this project focused on a peer-to-peer mechanism known as Crypto Phones. Crypto Phones are a security measure claiming to completely address the problem of wiretapping. Users orally exchange the information resulting from a cryptographic protocol employing Short Authenticated Strings, or SAS, to confirm each other's identity.

The results of this study show that this security tool is in fact vulnerable to automated voice mimicry attacks, which were designed and implemented by Saxena's team as part of this research.

The team developed and executed these attacks using off-the-shelf speech recognition and synthesis tools, and comprehensively evaluated them with respect to both manual detection and automated detection. Manual detection was tested with a group of 30 human users. The results demonstrate the effectiveness of the attacks against three prominent forms of SAS encodings: numbers, PGP word lists and Madlib sentences. These attacks can be used by a wiretapper to compromise the confidentiality and privacy of Crypto Phones' voice, video and text communications.

Saxena's research also highlights the vulnerability of relying upon multiple preceptory channels rather than just audio. In other words, if the attacker performs the voice impersonation against SAS, users may not be able to detect this attack by looking at and analyzing the accompanying video of the communicating party, which will show that the lip movement of the person stating the SAS does not match the spoken SAS. Most users either do not look at the video or cannot detect the mismatch between the audio and the video.

After defining the potential threats, Saxena's team sought to identify potential solutions to those threats that could help increase the security of the underlying SAS validation process. One potential defense to these attacks could be integration of an automated voice recognition or voice biometrics system into Crypto Phones. That is, in place of, or addition to, human voice recognition, a software component may be used to detect potential SAS forgeries.

Yet another potential solution to thwart the voice impersonation attacks against Crypto Phones is to perform the SAS validation over an auxiliary channel that can be more resistant to voice and packet manipulation. For example, if the communicating devices support both Internet connection and cellular connection, the non-SAS communication can take place over the former and SAS validation can take place over the latter. This solution is suited for use on mobile phones in particular.

While these potential solutions could serve as a useful defense to these attacks, they are not completely foolproof. Saxena's team contends that a comprehensive investigation in the future is needed to better address a viable mechanism that could thwart such attacks.

"We believe our findings from this project will make strong impacts—not only on networking security, but also on human-computer interaction and real-world usability," said Maliheh Shirvanian, the Ph.D. student who led the project. "The results bring to light the threats of conceived voice privacy, and should serve as notice to users to pay careful attention to the potential security weaknesses in the future."

Provided by University of Alabama at Birmingham

Citation: New research shows vulnerability in mobile phones' applications offering voice communication security (2014, November 6) retrieved 3 July 2024 from https://phys.org/news/2014-11-vulnerability-mobile-applications-voice.html