# Improving the security and usability of Zoom's end-to-end encryption protocol

27 October 2020, by Yvonne Taunton

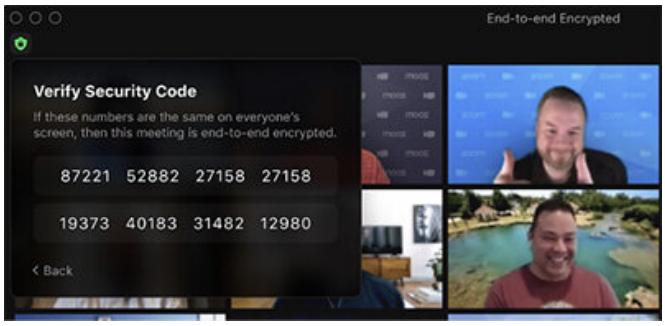


Figure 1: Zoom's method to verify the cryptographic key of the host of the call. Being manual, this approach is prone to security and usability problems. Credit: University of Alabama at Birmingham

During the global coronavirus pandemic, many people have been working, teaching and learning from home and utilizing Zoom as a way to have face-to-face communication. Although this is a main resource for virtual human interaction, there are still concerns for back-end security issues and meeting hackings.

After a major hiccup in the earlier versions of Zoom with no support for end-to-end encryption, Zoom made significant headway by acquiring Keybase, a secure communications company, and hiring several security and crypto researchers to work on a secure end-to-end encryption protocol. They released a white paper detailing their protocol, which Zoom is rolling out soon per their blog.

The University of Alabama at Birmingham's Nitesh Saxena, Ph.D., professor in the College of Arts and Sciences' Department of Computer Science, led a team of researchers to investigate Zoom's end-to-end encryption protocol and suggested changing its meeting security code validation method necessary to verify the cryptographic keys.

In the proposal, Saxena discusses the fundamental problems with Zoom's meeting security code validation and its susceptibility to human errors.

"If you ask users to manually compare the codes (as shown in Figure 1), they will do a poor job at it or may often skip the task completely," Saxena said. "These human errors then will have negative consequences for the security and usability of the approach."

Saxena's approach addresses these concerns with a new model using meeting codes which can be validated more reliably, significantly improving both security and usability of Zoom's current design.

His proposal carefully leverages the strengths of humans and machines to make the security code comparison significantly more robust to human errors or skip-through, and will improve the security of the signaling channel.

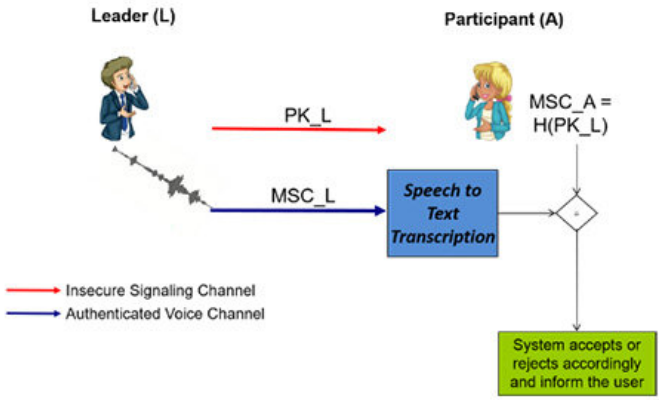


Figure 2: Saxena's method to verify the cryptographic key automatically via speech to text transcription. Credit: University of Alabama at Birmingham

"The main idea behind our approach, initially

proposed in our paper published at the ACM Conference on Computer and Communications Security in 2014, is to automate the process of code comparison by using the current transcription technology," Saxena said.

This approach (shown in Figure 2) simply requires the leader to announce the meeting code MSC_L; but now, instead of the human participant, a Natural Language Processing or speech recognition algorithm running on the participant's client machine will automatically transcribe the spoken code and perform the comparison on behalf of the participant.

Saxena says the results of their investigation show that, by using automated meeting code comparison, their approach can drastically reduce the chances of false positives under signaling channel attacks to 0 percent, and reduce the overall false negatives down to about 5 percent, much lower than the traditional design.

While Saxena and his team have an effective prototype, more engineering work is needed to optimize, refine and further test it toward the deployment in Zoom's specific environment.

Saxena also warns that Zoom should not use numeric meeting codes, as they are easily susceptible to reordering attacks—as studied in Saxena's other related prior work, whereby the attacker can simply copy the user's voice speaking the digits 0-9 from a previous session, and then reorder the recorded snippets to create any code the attacker wants to compromise a future session. Instead, he recommends the use of phonetically distinct words.

Saxena's group is cognizant to the fact that certain speech impediments may make it difficult for the transcription approach to work well. The easiest solution might be to outsource the task of announcing the code from the leader with the potential impediment to another participant without the impediment.

"More work can be conducted to design specific-word dictionaries that may work with certain known speech impediments when transcribing," Saxena said. He also noted that, although Zoom's proposal mentioned the possibility of using certificate transparency, this approach is not widely used yet and it cannot actually detect the presence of any attacks in real time.

**More information:** Meeting Security Code Validation: github.com/zoom/zoom-e2e-white … -Code-Validation.pdf

Provided by University of Alabama at Birmingham