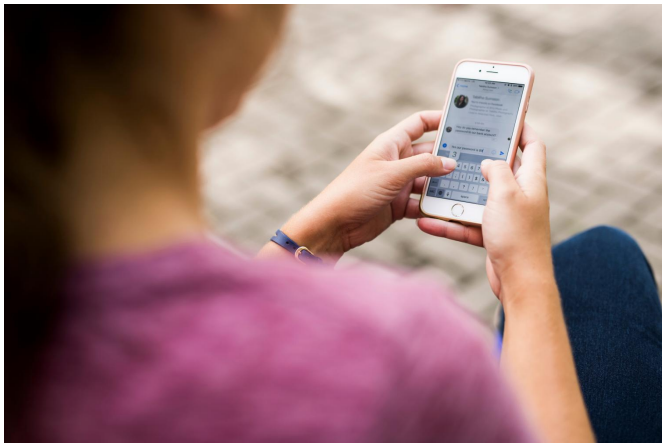
New study on popular messaging apps shows encrypting is easy but authenticating is hard

10 August 2017, by Andrea Christensenk.c. Miller



Researchers have learned that most users of popular messaging apps are leaving themselves exposed to hacking and fraud because they aren't using important security options. Credit: Nate Edwards/BYU

Researchers at Brigham Young University have learned that most users of popular messaging apps Facebook Messenger, What'sApp and Viber are leaving themselves exposed to fraud or other hacking because they don't know about or aren't using important security options.

"We wanted to understand how typical users are protecting their privacy," said BYU computer science Ph.D. student Elham Vaziripour, who led the recent study. Short answer: they're generally not.

Even though What'sApp and Viber encrypt messages by default, all three messaging apps also require what's called an authentication ceremony to ensure true security. But because most users are unaware of the ceremony and its importance, "it is possible that a malicious third party or man-in-the middle attacker can eavesdrop on their conversations," said Vaziripour, who was joined on the study by computer science professors Daniel Zappala and Kent Seamons and five other student researchers.

The authentication ceremony allows users to confirm the identify of their intended conversation partner, and makes sure no other person—even the company providing the messaging application—can intercept messages.

In the first phase of a two-phase experiment, the research team prompted study participants to share a credit card number with another participant. Participants were warned about potential threats and encouraged to make sure their messages were confidential. However, only 14 percent of users in this phase managed to successfully authenticate their recipient. Others opted for ad-hoc security measures like asking their partners for details about a shared experience.

In the second phase, participants were again asked to share a credit card number, but in this round researchers emphasized the importance of authentication ceremonies. With that prompting, 79 percent of users were able to successfully authenticate the other party.

Researchers have learned that most users of popular messaging apps are leaving themselves exposed to hacking and fraud because they aren't using important security options. Credit: Nate Edwards/BYU

Despite the drastic climb, however, researchers discovered another significant hurdle: participants averaged 11 minutes to authenticate their partners.

"Once we told people about the authentication ceremonies, most people could do it, but it was not simple, people were frustrated and it took them too long," Zappala said.

Because most people don't experience significant security problems, both professors agreed, it's hard to make a case for them investing the time and effort to understand and use security features that applications offer. But because there's always a risk in online communications, Seamons added, "we want to make it much easier to do and cut that time way down."

The ultimate goal? "If we can perform the authentication ceremony behind the scenes for users automatically or effortlessly, we can address these problems without necessitating user education," said Vaziripour.

This study is an extension of ongoing work on usable security in the two labs Seamons and Zappala run, funded in part by more than $1 million in recent grants from the National Science Foundation and Department of Homeland Security.

"Security researchers often build systems without finding out what people need and want," said Seamons. "The goal in our labs is to design technology that's simple and usable enough for anyone to use."

Provided by Brigham Young University