Research offers solution to encrypted messages being hacked before sending or after receipt

July 19 2022

Credit: CC0 Public Domain

Message applications must do more to keep user data safe from undetected malware or over-the-shoulder eavesdropping that bypasses encryption before a message has been sent, according to researchers

from the University of Surrey.

To combat this issue of close location hacking, researchers from Surrey's School of Computer Sciences have created a new end-to-end encryption mechanism called Secure Node End-2-End Encryption (SNE2EE) that protects users' communications at a far higher level than currently experienced on popular applications.

Current messaging applications encrypt the data transfer from one device to another, but not the typed or received message on either end.

Dr. Sotiris Moschoyiannis at the University of Surrey says, "When an unencrypted message is received, there is no confidence that the received message will be read by the intended recipient. The SNE2EE offers a 4-level privacy protection approach, using a combination of software and hardware with multi-factor authentication and biometric data tools and an overlay screen or application used to ultimately decrypt the message.

"Work still needs to be done to ensure the offered solutions are user-friendly and efficiently integrated to popular message applications to make them highly secure."

The research was conducted in partnership with De Montfort University and Yale University, with the SNE2EE solution made freely available for other researchers in order to further extend its functionality and blend with other privacy or security mechanisms.

Provided by University of Surrey

https://techxplore.com/news/2022-07-solution-encrypted-messages-hacked-receipt.html