UNIVERSITY OF BIRMINGHAM

Powered by: IN-PART

A New Method for End-to-End Encryption

A technique to ensure that only senders and recipients read messages by forcing attackers to leave evidence of any such activity.

Please note, header image is purely illustrative. Source: Tumisu, pixabay, CC0.

Seeking

Development partner, Commercial partner

About **University of Birmingham**

At the University of Birmingham our research leads to new inventions and fuels innovation and business growth.

Background

With current end-to-end encryption, if an attacker compromises a recipient's device, they can then put themselves in a position to intercept, read and alter all future communications without sender or recipient ever knowing. Effective end-to-end encryption services have already been developed, but by definition they rely on a device itself remaining secure; once a device has been compromised there's little that the user can do.

Tech Overview

Researchers at the University of Birmingham, in collaboration with the University of Luxembourg and University of Oxford, have developed a technique that ensures that only sender and recipient can read a message. The new protocol forces attackers to leave evidence of any such activity and alerts users to take action.

The solution, called DECIM (Detecting Endpoint Compromise in Messaging), addresses the question of what to do when the attacker is in a position to intercept all of your messages on a long-term basis. Both your Internet Service Provider and messaging service operator are in such positions – all your messages pass through their servers – so that if they obtained your keys, they would never be locked out of a conversation, and you would never know. With DECIM, the recipient's device automatically certifies new key pairs, storing the certificates in a tamper-resistant public ledger.

The team undertook a formal security analysis using a symbolic protocol verification tool, the 'Tamarin prover', which runs millions of possible attack situations, verifying DECIM's capabilities. This is a rare step for a messaging protocol, and the same analysis for other protocols revealed several security flaws.

The researchers are now looking at ways to detect encryption key compromise for applications, for example in blockchain or in Internet-based voting.

Further Details:

The paper presenting the protocol, 'DECIM: Detecting Endpoint Compromise in Messaging', was published in the IEEE Transactions on Information Forensics and Security, the leading peer-reviewed journal in the field of computer security and cryptography - DOI 10.1109/TIFS.2017.2738609.

Applications

This technology will be of interest to software developers, ISPs, sectors such as banking, government, NHS, large corporates especially where people travel – anywhere that people are connecting outside of known and verifiable secure places.

Opportunity

The university is seeking partners for further development and commercialisation.