PHYS ORG

# Computer scientists address gap in messaging privacy

September 27 2017

Credit: University of Birmingham

Researchers have developed a solution to a longstanding problem in the field of end-to-end encryption, a technique that ensures that only sender and recipient can read a message.

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.

The new protocol, published in *IEEE Transactions on Information Forensics and Security*, forces attackers to leave evidence of any such activity and alerts users to take action.

Dr. Jiangshan Yu at the University of Luxembourg, Professor Mark Ryan at the University of Birmingham and Professor Cas Cremers at the University of Oxford, were motivated by the discovery of mass software vulnerabilities, such as the Heartbleed bug, that make the majority of devices vulnerable to compromise.

Dr Yu explained, "There are excellent end-to-end encryption services out there, but by definition they rely on your device itself remaining secure; once a device has been compromised there's little we can do. That's the problem we wanted to solve."

Following Edward Snowden's revelations about government mass surveillance, end-to-end encryption is now widely available through services such as Facebook's WhatsApp. The approach uses pairs of cryptographic 'keys' for the sender to encrypt and the recipient to decrypt messages; anyone wanting to read your messages has to first hack into your phone to steal your latest keys. The attacker then performs a 'Man-in-the-middle' (MITM) attack, for example by taking control of your WIFI router to intercept your messages, and uses the stolen keys to impersonate you.

Current encryption protocols such as Signal used by WhatsApp make the most of the fact that a MITM attacker can only intercept messages sent via the compromised network. For example, as soon as you send a message via 3G rather than the compromised WiFi the attacker will no longer be able to act as an intermediary. They will lose track of the keys and be locked out of the conversation.

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.

"There's no silver bullet in the field of end-to-end encryption", said Dr. Yu, "but we hope that our contribution can add an extra layer of security and help to level the playing field between users and attackers."

Professor Mark Ryan, from the School of Computer Science at the University of Birmingham, said, "Our Security and Privacy group tries to solve problems that are important to society. Given the prevalence of cyber-attacks on phones and laptops, we are proud of this work on detecting when encryption keys have become compromised. Next, we intend to apply for this work on detecting encryption key compromise to applications, for example in blockchain or in Internet-based voting."

## Example of solution in practice

To prepare for receiving a message, Robert's device certifies an encryption key, and publishes the certificate in the ledger. To send a message, Sally's device uses a cryptographic process to fetch and verify the certified encryption key from the ledger. She then uses it to send a message to Robert, who opens it with the corresponding decryption key.

If an attacker wants to impersonate Robert, they will need to put a forged key certificate in the ledger, persuading Sally's device to use a fake encryption key. However, the DECIM ledger supports efficient (for billions of users each sending thousands of messages) and automatic cryptographic proof generation and verification to ensure that the log cannot be tampered with. So, if Robert's device detects forged certificates, it is sure evidence of an attacker impersonating him. The log also records device activity, so if Robert sees a record for a device that he hasn't used recently it is again evidence of an attack.

**More information:** Jiangshan Yu et al. DECIM: Detecting Endpoint Compromise In Messaging, *IEEE Transactions on Information Forensics and Security* (2017). DOI: 10.1109/TIFS.2017.2738609

Provided by University of Birmingham

Citation: Computer scientists address gap in messaging privacy (2017, September 27) retrieved 20 April 2024 from https://phys.org/news/2017-09-scientists-gap-messaging-privacy.html