In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

WhatsUpp with Sender Keys? Analysis, Improvements, and Security Proofs

By

Mr. David Balbás

IMDEA Software Institute & Universidad Politécnica de Madrid, Spain

Date : 11 December 2023 (Monday)
Time : 10:00am – 11:00am
Venue : Rm 801, Ho Sin Hang Engineering Building, CUHK

Abstract

Developing end-to-end encrypted instant messaging solutions for group conversations is an ongoing challenge that has garnered significant attention from practitioners and academics alike. Notably, industry-leading messaging apps such as WhatsApp and Signal Messenger have adopted the Sender Keys protocol, where each group member shares their own symmetric encryption key with others. Despite its widespread adoption, Sender Keys has never been formally analysed in the cryptographic literature, raising the following natural question:

What can be proven about the security of the Sender Keys protocol, and how can we practically mitigate its shortcomings?

In addressing this question, we conduct the first formal analysis of the Sender Keys protocol, and prove its security in a somewhat weak model. In particular, we observe shortcomings on the security of group membership, forward security guarantees for authentication, and sub-optimal recovery from compromise. Towards improving security and efficiency, we propose a series of modifications to Sender Keys. We combine these refinements into a new protocol that we call Sender Keys+, which may be of interest both in theory and practice. The full paper is available at (https://ia.cr/2023/1385)

Biography

David Balbás is a third-year PhD student at IMDEA Software Institute (Madrid, Spain) advised by Prof. Dario Fiore. He is broadly interested in theoretical and practical aspects of cryptography and computer security. His research focuses on verifiable computation, cryptographic primitives with advanced functionalities, and secure group messaging. Before joining IMDEA, he carried out his MSc Thesis at EPFL (Switzerland) advised by Prof. Serge Vaudenay. Previously, he was a Cryptography Engineer at BERTEN.

**** ALL ARE WELCOME ****

Host: Prof. Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8474)