SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Concurrent Group Operations on TreeKEM

Yugo Koyanagi * Masahiro Ishii * Keisuke Tanaka *

Keywords: Secure group messaging, Messaging Layer Security, TreeKEM, Post-Compromise Security, concurrent operations

Abstract

Due to the COVID-19 that has been spreading worldwide since the end of 2019, the use of video calling applications is increasing to prevent infection. What is needed for video calls is the technology to exchange video and audio in real time and securely. Therefore, research and development of Messaging Layer Security (MLS) [2] which is designed as secure layer for end-to-end encrypting messages in many groups has been more active. We analyze and discuss TreeKEM, the core protocol of MLS, with respect to its ability to handle concurrent group operations.

In this paper, we discuss concurrent and auxiliary operations in TreeKEM. Concurrent group operations are more likely to occur in video calls, where the movement of devices in a group (joining, leaving, etc.) is more active than in messaging. Hence, our study will be useful for implement TreeKEM more efficiently and securely.

Regarding the concurrent group operations of TreeKEM, Bhargavan et al [1] have shown five dangerous patterns in previous studies. In this paper, we discuss all patterns including them and show three main things.

First, we show that the processing order of operations should be $ADD \rightarrow UPDATE \rightarrow REMOVE$. Second, we show that Post-Compromise Security (PCS) protection after concurrent updates is possible for two devices with the same countermeasures as in previous studies, but does not work well for three or more devices, and then discuss countermeasures in those cases. Third, we showed the exceptional patterns for cases where auxiliary operations must be performed, or where concurrent group operations are not possible at all. Table 1 and the following enumaration outlines the problems and countermeasures for processing the concurrent execution of two devices. Those of three or more devices can be handled by a combination of these, except for (ii).

Table 1: The order of concurrent group operations and countermeasures to problems for two devices. '–' means that concurrent group operations cannot be performed properly in this processing order.

before \ after	ADD	$UPDATE$	$REMOVE$
ADD	(i)	(i)	(i)(iv)
$UPDATE$	–	(ii)	(ii)
$REMOVE$	–	–	(ii)(iii)

(i) Newly added device can't recognize other operations. Information needs to be complemented.

(ii) If a device is compromised, PCS can't be guaranteed. Further update is required.

(iii) Devices need to be removed collectively due to multiple factors, such as device compromise.

(iv) There are exceptional patterns where concurrent group operations cannot be processed.

References

[1] Karthikeyan Bhargavan, Richard Barnes and Eric Rescorla, "TreeKEM: Asynchronous Decentralized Key Management for Large Dynamic Groups," *Messaging Layer Security mailing list*, 2018.

[2] Richard Barnes, Benjamin Beurdouche, Raphael Robert, Jon Millican, Emad Omara and Katriel Cohn-Gordon, "draft-ietf-mls-protocol-12 - The Messaging Layer Security (MLS) Protocol," `https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/`, 10/11/2021, (Accessed on 12/01/2021).

* Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku Tokyo 152-8550 Japan