An Improved TreeKEM protocol with stronger PCS

2230407 Tomoko Otsuru

Secure Messaging protocols enable end-to-end secure communication over untrusted network and server infrastructure. They are used in major application services that provide secure message exchange between users, such as Signal, Facebook Messenger and etc.

TreeKEM is a continuous group key agreement (CGKA) protocol and is at the core of the Secure Group Messaging (SGM) protocol in the IETF MLS working group. Alwen et al. have first analyzed the security of TreeKEM and are followed by several papers. In Alwen et al., they have claimed that the original TreeKEM does not satisfy forward secrecy (FS) and proposed a modification that satisfies FS. Their modification is very simple: They have replaced the public-key encryption used in the original TreeKEM with updatable public-key encryption. As for PCS, Alwen et al. has claimed that the original TreeKEM is sound against the post-compromise attacks. However, their definition of PCS is not well deployed in the case of TreeKEM because it is defined in a general CGKA protocol. In TreeKEM, each user keeps plural secrets corresponding to each node in "the tree" of TreeKEM, a part of which is used to obtain the new group session key I. In Alwen's definition, the key compromise should always reveal the whole inner states of a compromised user. They do not consider "partial reveal". In our paper, we consider the node-by-node key compromise, which would be more suitable for TreeKEM. In addition, we introduce an extra key derived from the root secret. With this modification, we can significantly increase the case of key updates that the protocol can recover from compromise. In our protocol, even if an attacker obtains some private keys of nodes, it will no longer be able to obtain subsequent session keys if there is an update from users other than the specific ones.