Deniability in MLS

Sofía Celi
Cloudflare

IETF110

Context

- Deniability could be a desirable privacy property, which several messaging protocols provide.
- There is an increase on providing this property.

- Deniable authentication is a property by which it cannot be proven that a message has been authored by anyone in a conversation, as anyone could have potentially authored that message.

Authentication in MLS

- Group members can verify a message originated from a member of the group they belong to. This form of authentication is implicit.

- Group members can verify a message originated from a particular member of the group. This form of authentication is explicit. This authentication is guaranteed by a digital signature on each message using the sender's public signature key. This key is advertised on the Credential inside the KeyPackage object in the leaves of the tree.

The ideas

- A weak form of deniability is preserved for implicit authentication: someone from the group sent a message, but it is not possible to know who sent it from that group.
- A version of offline deniability can be achieved for explicit authentication if the private key corresponding to the advertised signature key from the KeyPackage object is revealed: anyone with access to that key can create arbitrary messages with it, and no one can attest that a particular user is the author of a message.

Security/Privacy/Practical considerations

- When to reveal these keys: the two-generals problem
- Will revealing these keys diminish authentication?
- Which kind of deniability is this? Post-compromise deniability?
- What happens with messages that arrive late after the key has been revealed or rotated?
- Signature keys must be per device

- Draft location: https://github.com/claucece/draft-celi-mls-deniability/blob/main/draft-celi-mls-deniability.md

Thank you!