Deniability in a group chat setting

Sofía Celi
The context

- Secure communication: encrypt and sign a message?
- Deniability in a two party conversation
- Ian Goldberg, Nikita Borisov, Erik Brewer: Off-the-record messaging
- Mimic casual conversations:
  - Deny having said something to anyone outside the conversation
  - Deny having said a message
  - Deny their participation in a conversation
- Other protocols emerged: Signal, Olm, etc.
- Serves only two participants
- New communication approach: group chat
Deniability

“Anyone could take or have taken part in a private conversation, but that person can plausibly deny ever having done so”.

Properties*

- Confidentiality
- Integrity
- Authentication (entity authentication and origin authentication)
- Participant Consistency
- Destination Validation
- Forward secrecy
- Backwards secrecy (Post-Compromise Secrecy)
- Anonymity Preserving
- Speaker Consistency
- Causality Preserving
- Global Transcript

Deniability properties*

- Message unlinkability
- Message repudiation
- Trust Equality
- Subgroup messaging
- Computational equality
- Contractible membership
- Expandable membership

Additional properties*

- No additional service
- Multi-device Support
- Out-of-Order Resilience and Dropped Message Resilience

New deniability properties

- Message deniability
- Participation deniability
- Online deniability
- Offline deniability

“A protocol is strongly deniable if transcripts provide no evidence even if long-term key material is compromised (offline deniability) and no outsider can obtain evidence even if an insider interactively colludes with them (online deniability).”

What work has been done?

- Bian, Seker and Topaloglu proposed a method for extending OTR for group conversation: *Off-the-Record Instant Messaging for Group Conversation*.
- Goldberg, Van Gundy, Ustaoglu and Chen proposed *Multi-party Off-the-Record Messaging*
- Liu, Vasserman, and Hopper proposed an improved group OTR (GOTR): *Improved group off-the-record messaging*
- Moxie Marlinspike et al: Signal group chat
- eQualit.ie: (n+1)sec group chat
- Schliep, Vasserman, and Hopper: *Consistent Synchronous Group Off-The-Record Messaging with SYM-GOTR*
- Matrix’s *Megolm*
Limitations

- No clear definitions of which properties are provided or want to be provided
- Comparison work by Schliep, Vasserman, and Hopper: Consistent Synchronous Group Off-The-Record Messaging with SYM-GOTR
- No inclusion of the ‘new’ definitions of deniability
References


• Dimitry, (2010). *Introducing (n+1)sec – A protocol for distributed multiparty chat encryption*. eQualitie. Available at: https://equalit.ie/introducing-n1sec-a-protocol-for-distributed-multiparty-chat-encryption/


• *Megolm group ratchet*. Matrix. Available at: https://git.matrix.org/git/olm/about/docs/megolm.rst
Thanks!

Sofía Celi
@cherenkov_d