Twice the Fun: Adapting Unicast Privacy Notions for Group Communication

Christoph Cajanovic 1, Christiane Kuhn 2, Thorsten Strufe 3

1Karlsruhe Institute of Technology
2firstname.lastname@kit.edu

Kuhn et al. [5]: framework of formal privacy notions through indistinguishability games (IND-CPA-like):

\[ \Pi \rightarrow \{C, D\} \]

Scenario \( S_0 \): One or more communications defined by sender message, and receiver:

\[ A \xrightarrow{m} B \]

\[ B \xrightarrow{m} A \]

Challenge = \( (S_0, S_2) \)

How to Formalize Privacy Goals?

- Concrete Privacy notions are defined by properties
  - Specify which information may be disclosed
  - Disclosable information has to be identical in both scenarios

- Group-Message Unlinkability

Partial Hierarchy

Future Work

- Further privacy notions (e.g., membership-related)
- Protocol analysis

Acknowledgments & References

This work was supported by funding of the Helmholtz Association (HGF) through the Competence Center for Applied Security Technology (KASTEL).


Picture credit: The New York Times

Group with critical messages are blocked by the regime
Activist receiving critical messages faces persecution
Political activists (e.g., in Myanmar) require private and secure means of communication.

Motivation

Setting

Communication Format

Membership Management

New Notions

- To cover link between groups and messages
- See hierarchy on the left

Kuhne et al. [5]: framework of formal privacy notions through indistinguishability games (IND-CPA-like):

\[ \Pi \rightarrow \{C, D\} \]

Scenario \( S_0 \): One or more communications defined by sender message, and receiver:

\[ A \xrightarrow{m} B \]

\[ B \xrightarrow{m} A \]

Challenge = \( (S_0, S_2) \)

How to Formalize Privacy Goals?

- Concrete Privacy notions are defined by properties
  - Specify which information may be disclosed
  - Disclosable information has to be identical in both scenarios

- Group-Message Unlinkability

Partial Hierarchy

Future Work

- Further privacy notions (e.g., membership-related)
- Protocol analysis

Acknowledgments & References

This work was supported by funding of the Helmholtz Association (HGF) through the Competence Center for Applied Security Technology (KASTEL).