PhD thesis proposal – PILOT project PEPR eNSEMBLE

Group key management in decentralized collaborative systems

Director of the thesis: Claudia-Lavinia Ignat, DR Inria, Inria centre of Lorraine University (team Loreley)
Co-supervisors of the thesis: Mathieu Turuani, CR Inria, Inria centre of Lorraine University (team PESTO) and Davide Frey, CRHC Inria, Inria centre at Rennes University (team WIDE)
Hosting lab: Inria Centre of the University of Lorraine, Nancy
Research team: Loreley

Context

In large-scale collaborative environments, groups of users frequently join and leave shared workspaces while interacting with shared documents, communication channels, or collaborative tools. In such dynamic groups, ensuring secure communication among participants is a critical challenge. In particular, the management of cryptographic group keys becomes complex when membership changes occur frequently.

When a participant leaves or is removed from a collaborative group, the confidentiality of the collaboration requires that this user should no longer have access to future communications or shared documents. Consequently, a new group key must be generated and distributed among the remaining members. In traditional approaches, this process requires several rounds of communication between participants to update and redistribute cryptographic material. In large and dynamic groups, these operations can introduce significant performance overhead, increase communication costs, and lead to temporary interruptions in the workflow of participants.

For many years, solutions for secure *n*-party group communication have faced a trade-off between scalability and security. Some protocols offered strong security guarantees but did not scale well to large groups, while others achieved scalability at the cost of weaker security guarantees.

The recent standardization of the **Messaging Layer Security (MLS) protocol** [1] addresses many of these challenges. MLS is designed to enable **secure, scalable, and efficient group communication**, supporting dynamic membership changes while ensuring strong security properties such as forward secrecy and post-compromise security. MLS relies on advanced group key agreement mechanisms that allow the cost of membership changes to scale logarithmically with the group size [2].

However, practical deployments of MLS rely on an additional component called the **Delivery Service (DS)**. The Delivery Service acts as an intermediary that coordinates message exchange between group members and ensures that group operations are

delivered in a consistent order. While the MLS protocol assumes that this service is **untrusted with respect to message confidentiality**, it nevertheless plays a critical role in maintaining group consistency and availability.

This centralized Delivery Service introduces potential **availability, reliability, and security risks**. A compromised or malicious Delivery Service could disrupt message ordering, block progress of the group, or create inconsistent views among participants. Furthermore, centralization raises concerns regarding scalability and resilience in large-scale collaborative environments.

Objectives

This PhD project aims to investigate the **security and resilience of the Delivery Service component in the MLS architecture**, with the objective of designing **a decentralized and Byzantine-resilient Delivery Service suitable for large-scale collaborative systems**.

First, we aim to **analyze the security limitations of the current centralized Delivery Service model** used in MLS deployments. Using both existing implementations and formal verification techniques, we will demonstrate that the centralized architecture can be vulnerable to several classes of attacks, including message ordering manipulation, consistency violations, and denial-of-service scenarios.

Second, we will design a **decentralized Delivery Service architecture** capable of coordinating message exchange among MLS clients without relying on a single trusted infrastructure. This architecture will aim to maintain the key consistency properties required by MLS while tolerating failures or malicious behavior of some participants.

In particular, we will focus on achieving **resilience against Byzantine faults**, where nodes in the system may behave arbitrarily or maliciously. Our goal is to develop a Delivery Service design that guarantees:

- consistent ordering of MLS messages,
- agreement among group members on the sequence of operations,
- robustness against malicious participants,
- scalability to large and dynamic groups.

Third, we will validate the proposed architecture through **formal verification and experimental evaluation**. Formal methods will be used to verify the correctness and security properties of the proposed protocol, while practical experiments will evaluate its performance and scalability in realistic collaborative scenarios.

Methodology

The research will be conducted in several stages.

Security Analysis of Existing MLS Delivery Services
Using symbolic verification tools such as ProVerif [3], we will analyze how the Delivery Service interacts with MLS clients and identify potential vulnerabilities related to message ordering, proposal handling, and commit validation.

We will also study several existing MLS implementations to understand how Delivery Service assumptions are implemented in practice and how inconsistencies may arise in real deployments.

Design of a Decentralized Delivery Service
Based on the vulnerabilities identified in the first phase, we will design a distributed Delivery Service architecture that removes the reliance on a centralized server.
Possible approaches include:

- peer-to-peer message dissemination,
- distributed ordering protocols,
- Byzantine fault-tolerant consensus mechanisms such as CAC [4],

The design will aim to preserve the security guarantees of MLS while improving resilience and availability.

Formal Verification of the Proposed Architecture
Once the decentralized architecture is designed, we will formally analyze its security properties using formal verification tools such as ProVerif.
The analysis will focus on verifying properties such as:

- epoch agreement [5],
- epoch-content consistency [5],
- resilience to Byzantine nodes.

Implementation and Experimental Evaluation
To demonstrate the practical applicability of the proposed solution, we will implement the decentralized Delivery Service and integrate it into real collaborative systems.

In particular, we plan to integrate our solution into the *MUTE* [6] peer-to-peer collaborative editor or collaborative tools from *La Suite Numérique*, such as *Docs*.
This integration will allow us to evaluate the system in realistic collaborative scenarios involving dynamic group membership and large number of participants.

Case Studies
An important application domain for secure group communication is healthcare, which is already being investigated by several PhD students and postdoctoral researchers within the PILOT project. In this domain, multidisciplinary teams collaborate around patients while handling highly sensitive medical data. Physicians, nurses, specialists, and external consultants frequently join or leave care teams, requiring secure mechanisms to update access rights to shared medical information. Group key management mechanisms such as those provided by the Messaging Layer Security (MLS) protocol can ensure that only authorized participants can access patient-related communications, while preventing former members from accessing future discussions. A decentralized MLS infrastructure would further improve resilience and trust when collaboration spans multiple hospitals or healthcare institutions, enabling secure inter-organizational medical collaboration. We will adapt our solution to some healthcare use cases already identified by other PhD students or postdocs of PILOT.

Collaboration aspects

In this project, the notion of *collaboration* is understood in a broad sense, encompassing human activities mediated by digital technologies that involve a group

of several participants. These collaborative activities may fulfill different functions, such as communication, information sharing, coordination of tasks, or collective decision-making. They can occur in synchronous settings, where participants interact in real time, or asynchronously, where contributions are made at different moments. Collaborative activities may also span different time scales, from short interactions lasting a few seconds to long-term collaborations extending over months or years. Furthermore, collaborative groups can vary greatly in size, ranging from small teams to communities involving hundreds or thousands of participants. Collaboration may also take place in different spatial configurations, including co-located, distributed, or hybrid environments. Supporting such diverse forms of collaboration raises significant challenges for the underlying communication infrastructure. In particular, collaborative systems must support dynamic group membership, where participants frequently join and leave, while ensuring the confidentiality and integrity of communications. Protocols such as Messaging Layer Security (MLS) provide scalable mechanisms for secure group key management, but rely on a Delivery Service to coordinate message exchange and maintain a consistent group state. This PhD aims to investigate the limitations of this centralized component and to design decentralized Delivery Service mechanisms that can support secure and resilient collaboration across the wide variety of collaborative contexts described above.

Expected results and impact

The expected results of this PhD project include:

- a comprehensive security analysis of the MLS Delivery Service model,
- the design of a decentralized and Byzantine-resilient Delivery Service architecture,
- formal verification of the proposed protocols,
- practical implementations integrated into collaborative platforms,
- empirical evaluation through deployment and user studies.
- adaptation of the solution to some healthcare use case

By addressing the limitations of centralized message coordination in MLS deployments, this research will contribute to the development of secure, scalable, and resilient collaboration infrastructures, which are essential for modern distributed work environments.

The results of the project will be released as open-source software and formal verification models, benefiting both the research community and developers building MLS-based applications. This will support the broader adoption of MLS in secure messaging and collaborative systems.

Integration into PILOT project:

This subject integrates into the PILOT axis on open technical frameworks for long-term collaboration as it contributes to building a sustainable and safe infrastructure for future forms of collaboration.

The selected PhD student will work closely with the other PILOT PhD students and postdocs on the adaptation of the solution to some healthcare use cases handling highly sensitive medical data.

The contributions of this PhD are complementary to the objectives of PEPR Cybersécurité, which promotes research on secure digital infrastructures and the protection of distributed systems and where team PESTO is actively involved. By combining formal verification, cryptographic protocol design, and experimental evaluation in real collaborative platforms, this PhD contributes to advancing secure communication technologies relevant to both PEPR eNSEMBLE and PEPR Cybersécurité.

The proposed PhD also has links with the TRUSTINCloudS project of the PEPR Cloud program, which focuses on strengthening the security of cloud infrastructures and protecting outsourced data in cloud environments and where team Loreley is involved. TRUSTINCloudS aims to develop new methodologies and tools to ensure the confidentiality, integrity, and availability of data, applications, and services deployed in the cloud. Collaborative platforms such as MUTE or tools from La Suite Numérique are typically deployed in cloud or distributed infrastructures. The results of this PhD complement the objectives of TRUSTINCloudS by providing secure communication and key management mechanisms that strengthen the protection of collaborative data hosted in cloud environments, contributing to the broader goal of building trusted and sovereign cloud-based services.

Bibliography:

[1] R. Barnes, B. Beurdouche, R. Robert, J. Millican, E. Omara, and K. Cohn-Gordon, “The Messaging Layer Security (MLS) Protocol,” RFC 9420, Jul. 2023.

[2] K. Bhargavan, R. Barnes, and E. Rescorla, “Treekem: asynchronous decentralized key management for large dynamic groups A protocol proposal for Messaging Layer Security (MLS),” Inria Paris, Tech. Rep., 2018.

[3] B. Blanchet, “Modeling and verifying security protocols with the applied pi calculus and Proverif,” Foundations and Trends in Privacy and Security, vol. 1, no. 1-2, pp. 1–135, 2016.

[4] Timothé Albouy, Davide Frey, Mathieu Gestin, Michel Raynal, François Taïani: Contention-Aware Cooperation. OPODIS 2025: 9:1-9:19

[5] Ludovic Paillat, Claudia-Lavinia Ignat, Davide Frey, Mathieu Turuani, and Amine Ismail. 2024. Discreet: distributed delivery service with context-aware cooperation. Annals of Telecommunications 80 (2024), 357–374.

[6] Matthieu Nicolas, Victorien Elvinger, Gérald Oster, Claudia-Lavinia Ignat, François Charoy: MUTE: A Peer-to-Peer Web-based Real-time Collaborative Editor. ECSCW Panels, Demos and Posters 2017