Doctoral Thesis

# SANGRIA Secure ANonymous GRoup InfrAstructuere

**Author(s):**
Weiler, Nathalie

**Publication Date:**
2002

**Permanent Link:**

https://doi.org/10.3929/ethz-a-004469302 →

Diss. ETH No. 14770

# SANGRIA
# Secure ANonymous GRoup InfrAstructure

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZÜRICH

for the degree of
Doctor of Technical Sciences

presented by

NATHALIE WEILER

Dipl. Informatik-Ing. ETH
born 2nd of June, 1973
citizen of Luxembourg

accepted on the recommendation of
Prof. Dr. Bernhard Plattner, examiner
Prof. Dr. Rüdiger Grimm, co-examiner

2002

# Abstract

SECURE group communication services promote the deployment of traditional and new multi-party applications in networks such as video conferencing or large scale distance education. Confidentiality and authenticity combined in an intelligent group communication service with good scalability properties and efficient employment of the network infrastructure meet the needs of users and providers. Future generation networks such as mobile ad hoc networks challenge the research community even more for a commitment both to preserve the privacy of the users and to secure the network infrastructure of the provider. While other approaches focus either on the establishment of traditional security services – i.e. confidentiality, integrity and availability – in groups or on the anonymisation of point-to-point communication, this thesis introduces a self-contained approach to guarantee privacy preservation in closed groups, an infrastructure for secure and anonymous group communication.

The work first introduces an application independent framework for secure group communication. This framework fills the gap between different single, isolated proposals and the complete multicast application. The devised engineering approach is demonstrated in two ways: (1) Three kind of applications, i.e. a single sender, multiple receiver broadcast scenario, a highly dynamic, decentralised game, and a small scale, many-to-many workflow application, rely on the framework to provide a secure multicast service managing the access, the technical aspects of the group membership, and the network service. (2) The newly proposed secure group management scheme called Semsomm can be compared in a fair and efficient way to other approaches in the literature by simply plugging the respective implementations into the framework.

In the second part, the design of Semsomm is detailed. The main strategy of Semsomm is twofolded. First,intermediate nodes of the multicast distribution tree are used as untrusted relaying nodes in order to overcome the need to re-key the entire group upon each membership change. Second, the traffic encryption key is periodically renewed and redistributed to legitimate group members, thus inhibiting any collusion attack. It is shown that Semsomm scales to very large groups while preserving perfect forward secrecy of the multicasted information, i.e. only actual members of the group can understand it, thanks to its multiple encryption method.

The third contribution of this thesis consists in the design and implementation of a secure and anonymous group infrastructure, in other words, only users who fulfil certain conditions are allowed to join the secure anonymous group, non-members of the group cannot understand the data, and the identity of a member cannot be disclosed to outsiders of the group. Additionally, the member may hide its identity to other group members. The designed infrastructure, the Secure ANonymous GRoup InfrAstructure (SANGRIA), builds on top of unicast anonymity and is extended with the needed secure multicast functionality. It is shown in the context of multimedia applications how this infrastructure can be used.

Finally, the implementations are evaluated and discussed. Semsomm proves to achieve the scalability and security goals claimed, esp. the swift execution of the join and leave operations are confirmed. On the other hand, the evaluation of the infrastructural costs for group anonymity shows promising results. The impact of anonymisation depends on the configuration of the anonymising network that must be traded for the desired resistance against attacks on anonymity.

# Zusammenfassung

SICHERE Gruppenkommunikationsdienste fördern die Verbreitung von traditionellen und neuen multi-party Netzwerkanwendungen wie z.B. Videokonferenzen oder Distance Education. Wenn man Sicherheitseigenschaften wie Vertraulichkeit und Authentizität kombiniert mit einem intelligenten Gruppenkommunikationsdienst, der gut skaliert und die Netzwerkinfrastruktur effizient nutzt, kann man dadurch die Anforderungen sowohl von den Benutzern als auch von den Providern erfüllen. Die Anforderung, dass die Privatsphäre der Benutzer geschützt und zugleich die Netzwerkinfrastruktur der Provider gesichert wird, wird durch Netze neuerer Generation, wie z.B. mobiler ad hoc Netze, noch verstärkt. Während viele Forschungsarbeiten sich entweder mit dem Problem beschäftigen, wie man Sicherheitsdienste – Vertraulichkeit, Integrität und Verfügbarkeit – für Gruppen erbringen kann, oder damit wie Punkt-zu-Punkt Kommunikation anonymisiert werden kann, wird in dieser Dissertation eine in sich abgeschlossene Lösung für die Wahrung der Privatsphäre in geschlossenen Gruppen, also eine Infrastruktur für sichere und anonyme Gruppenkommunikation, vorgeschlagen.

Diese Arbeit stellt zuerst ein anwendungsunabhängiges Framework für sichere Gruppenkommunikation vor. Dieses füllt die Lücke zwischen Einzellösungen und Multicast-Anwendungen. Der entwickelte Ansatz wird auf zwei Arten verifiziert: (1) Drei verschiedene Arten von Anwendungen, nämlich ein Broadcast Szenario mit einem Sender und vielen Empfängern, ein sehr dynamisches, dezentralisiertes Spiel und eine Workflow Anwendung mit wenigen aber sehr rege interagierenden Benutzern, beziehen vom Framework einen sicheren Multicast Dienst, welcher den Zugriff regelt, die Gruppenzugehörigkeit handhabt und den Netzwerkdienst bereitstellt. (2) Das in dieser Arbeit neu vorgeschlagene sichere Gruppenverwaltungssys-

tem namens Semsomm kann auf faire und effiziente Art und Weise mit anderen Systemen aus der Literatur verglichen werden, in dem jedes dieser Systeme im Framework abgebildet wird.

Der zweite Teil der Arbeit beschreibt das Design von Semsomm ausführlich. Semsomm verfolgt zwei Hauptstrategien. Erstens werden die inneren Knoten im Multicast Verteilungsbaum als nicht vertrauenswürdige Weiterleitungspunkte verwendet. So umgeht man die Notwendigkeit, jedes Mal wenn ein Mitglied die Gruppe verlässt oder ein Mitglied hinzukommt, die ganze Gruppe mit neuen Schlüsseln versorgen zu müssen. Zweitens wird der Datenschlüssel in regelmässigen Abständen ersetzt und so verteilt, dass nur berechtigte Gruppenmitglieder ihn erhalten. So wird eine erfolgreiche Attacke durch Zusammenschluss von Gegnern verhindert. Es wird weiterhin gezeigt, dass Semsomm dank seiner mehrfachen Verschlüsselungsmethodik für sehr grosse Gruppen skaliert ohne dass die Eigenschaft der perfect forward secrecy verletzt wird, d.h. nur berechtigte Mitglieder können die verteilten Daten sinnvoll interpretieren.

Der dritte Beitrag dieser Dissertation ist das Design und die Implementierung einer sicheren und anonymen Gruppeninfrastruktur, d.h. falls Benutzer die vorgegebenen Bedingungen erfüllen, um in der sicheren und anonymen Gruppe teilzunehmen, können Nichtmitglieder die Identifikationsparameter dieser Teilnehmer in dem benutzten Netzwerk nicht ermitteln. Die entworfene Infrastruktur, die Secure ANonymous GRoup InfrAstructure (SANGRIA), baut auf Methoden auf, die für Unicast Anonymität eingesetzt werden. Diese werden mit Multicast Funktionalität erweitert. Es wird weiterhin gezeigt, wie diese Infrastruktur für Multimedia Anwendungen einsetzt werden kann.

Schliesslich werden am Ende der Arbeit die Implementierungen ausgewertet und besprochen. Es wird gezeigt, dass Semsomm die geforderten Skalierungs- und Sicherheitziele erreicht, insbesondere die rasche Ausführung derJoin und Leave Operationen. Andererseits zeigt die Beurteilung der Infrastrukturkosten für sichere Gruppenanonymität vielversprechende Resultate. Die Auswirkungen der Anonymisierung hängen von den Konfigurationsparametern des verwendeten anonymisierenden Netzes ab, welches gegen den Widerstand gegen Attacken auf die Anonymität abgewogen werden muss.