

Masterarbeit “Secure Multicast for Virtual Conferences”

Beginn: 1. Dezember 2003

Abgabe: 1. Juni 2004

Dieses Dokument gibt den Rahmen der Masterarbeit von Clemens Schroedter vor. Abweichungen oder Änderungen sind in gegenseitiger Absprache möglich.

Aufgabenstellung

A multicast protocol among a group of servers allows every server of the group to send data to all other servers, such that the *data packets* are being routed in an efficient way (for example, it avoids multiple transmissions of a packet over the same physical link). Multicast protocols are therefore particularly suitable for applications that multicast large amount of data, such as tele- or video- conferencing. A *secure* multicast protocol additionally provides sender authentication, and ensures that the multicast data remains hidden from any outsider of the group that may only observe the network traffic.

This master thesis consists of two parts. The goal of the first part is to implement a secure multicast protocol for a fixed group of servers by rendering a given multicast implementation secure. The solution must maintain the current way by which data packets are being routed; yet a public key infrastructure and insecure point-to-point communication channels may be used for setting up encryption and authentication keys. This setup of the multicast must be fully asynchronous and terminate for every server even if a fraction of servers crash. A technique for generating a secret group key can be found in [1], and a technique for efficient sender and message authentication for the multicast setting can be found in [2].

The goal of the second part is to implement a secure chat-room as an example application for a virtual conference based on secure multicast. The solution may extend the (insecure) implementation available from the distributed computing group. Furthermore, for establishing the public key infrastructure and the point-to-point communication links needed for setting up the underlying secure multicast, the solution may depend on a central server that provides the public keys and IP addresses of all servers involved in a secure chat.

Allgemeines

- Selbstständiges Arbeiten ist Voraussetzung.
- In der IBM Rueschlikon steht ein Arbeitsplatz zur Verfügung. Es besteht jedoch auch die Möglichkeit, zu Hause zu arbeiten.
- Es sind eine Zwischen- und eine Schlusspräsentation vorgesehen.
- Jeweils Ende Monat ist ein "Monthly Report" zu erstellen, welcher eine kurze Zusammenfassung, der Arbeit/Resultate eines Monats enthält.
- Der schriftliche Teil der Arbeit umfasst zwei Dokumente:
 - Einen Bericht (30 bis 50 Seiten, Sprache wählbar), welcher über die Arbeit und die Resultate Auskunft gibt. Dieser Bericht soll unter anderem auch eine kritische Beurteilung der eigenen Arbeit enthalten.
 - Einen Forschungsbericht (10 Seiten, in Englisch), welcher die Arbeit und die Resultate kompakter und unter einem wissenschaftlichen Gesichtspunkt darstellt.

Kontaktpersonen

- | | |
|----------------------|-------------------------|
| 1. Reto Strobl | rts@zurich.ibm.com |
| 2. Roger Wattenhofer | wattenhofer@inf.ethz.ch |

Literatur

[1] C. Cachin, R. Strobl, “Asynchronous Group Key Exchange with Failures”, manuscript

[2] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, "Multicast Security: A Taxonomy and Efficient Constructions", INFOCOMM99