Segurança de Redes e Sistemas de Computadores
(Networks and Computer Systems Security)
2023/2024, 1st Semester

Project Assignment #1: Mandatory Frequency valuation

Project title: A Secure Multicast Protocol for a Peer-Group Messaging System

Abstract

The goal of this project assignment is the design, implementation, and experimental validation of a solution to support a Secure Multicast Protocol to support a Peer-Group Messaging System as the demonstration application. The solution must be designed to address a generic model for a secure communication protocol supporting a secure UDP transport over IP Multicasting, to b used as a secure communication channel used by distributed peers or principals. The project assignment and its requirements can be addressed in different phases, where the solution will be refined and improved in their security arguments, including security properties and security parameterizations. The successive phases can reuse the goals from the previous phase, given the possibility to address the requirements step by step or phase by phase.

1. **Introduction, required materials and technology**

The development of the work assignment will require the use of cryptographic primitives and algorithms, namely symmetric cryptography and related secure parameterizations for operation modes and padding, secure hash functions, secure message authentication constructions (namely HMACs) and digital signatures using asymmetric cryptography and related secure constructions and parameterizations. The implementation is proposed to be addressed using Java and the enabled cryptography from Java Cryptographic Architecture (JCA) and Java Cryptographic Extensions (JCE), to address the requirements in the successive phases.
For the development an initial implementation in Java of an Insecure Multicast Messaging System is provided. This is the bse to start the implementation for Phase 1 requirements.

It is relevant for the project the knowledge and practical observations in Labs and the initial provided materials:

- http://vps726303.ovh.net/srsc2324/, see Labs (Lab 1, 2 and 3 materials) and see also WAs, Project Assignment 1 and provided initial materials (source code). See the file README to know how to use the provided materials for the project leveraging base.
- See, particularly, the file TODO (in provided materials) for the requirements and expected achievements for each development phase

2. Goals

The main goal for the project assignment is the design, implementation and the validation demonstration and related experimental observations of a Secure Peer-Group Multicast Chat-Messaging System, where users exchange messages (data and control messages, in the context of a secure messaging system. In the core of this goal, the idea is the implementation of a secure group-oriented communication channel, on top of an UDP transport layer supported by IP Multicasting, designed in a way that the solution could be used or adapted to any other application that need to be supported by IP Multicasting. The secure communication channel will be designed as a secure channel abstraction to support the communication protocol for the messaging system.

The following figure 1 represents the communication stack for the non-protected system and for the required security solution:

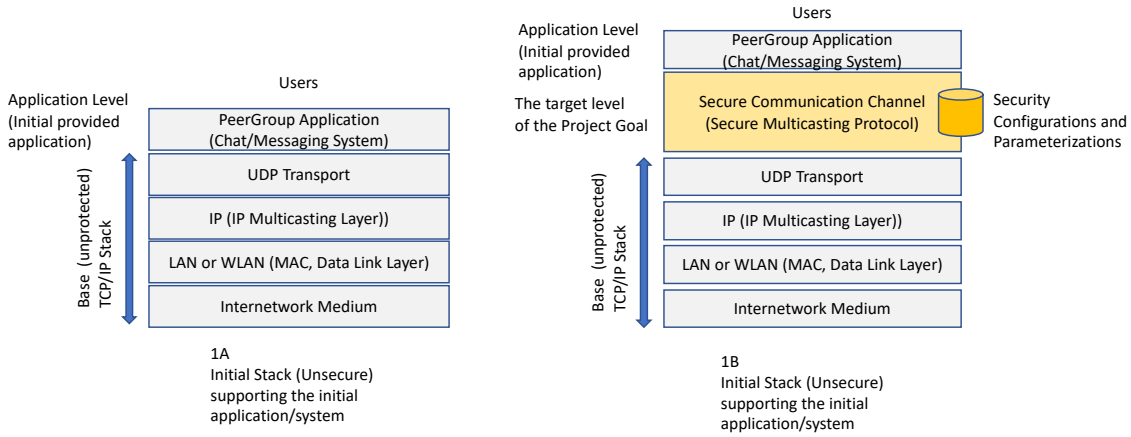

Fig.1 Communication Support Stack in TCP/IP:

1A – Unsecure Stack

1B – Secure Stack as addressed by the Project goal and requirements

Following the representation in figure 1, the solution must provide a secure datagram (connectionless) communication abstraction supported by UDP over IP Multicasting (independently of physical or MAC / Data Link layers)

The goal and requirements to build the targeted solution will be addressed in the following phases. These phases are suggested to be developed in sequence as a possible interesting methodology (but the development can follow a different approach – for example trying to arrive with one-shot development to the requirements of all phases). Each phase is described in its requirements, as defined in the TODO file (see the provided materials).

3. **Development Phases**

   For the detailed specifications of the presented phases, see the file TODO in the provided materials for the project assignment, including the configurations and parameterizations of the used cryptography for each phase

   In summary, the successive phases and their specific goals are represented in the following table

Phase	Goal	Characterization of the solution	Limitation	Score
1	Base implementation of the secure protocol / secure group communication channel	Base format and parts for encapsulation of the Secure Grout Messaging Protocol Only uses Symmetric Crypto + Secure Hashing + HMACs	Static and rigid configurations with pre-shared cryptographic parameterizations in endpoints	Correct, perfectly supported implementation and complete requirements and quality: Until 12/20
2	Phase 2 implementation of the secure protocol / secure group communication channel	Base format and parts for encapsulation of the Secure Grout Messaging Protocol (as in Phase 1) Can use variations of Symmetric Crypto + Secure Hashing + HMACs parameterizations	Static but flexible configurations with pre-shared cryptographic parameterizations in endpoints	Correct, perfectly supported implementation and complete requirements and quality: Until 14/20
3	Phase 3 Extended implementation of the Phase 2 protocol for group communication channel	All support for Phase 2, with additional use of Digital Signatures to provide initial Peer-Authentication guarantees	Static but flexible configurations with pre-shared cryptographic parameterizations for all the required cryptographic constructions in endpoints	Correct, perfectly supported implementation and complete requirements and quality: Until 18/20
4	Phase 4 Extended implementation of the Phase 3 protocol for group communication channel	All support for Phase 3, with additional use of Digital Signatures to provide initial Peer-Authentication guarantees	No static configurations but flexibility for each endpoint to express what is used to protect sent messages, allowing for the receivers to process dynamically by the receiver endpoints Minimal required configurations or no configurations at all	Correct, perfectly supported implementation and complete requirements and quality + high lights of the proposed and implemented solution: 19/20 or 20/20

4. **Evaluation factors**

   In each phase, the criteria for the evaluation involve:

   - The compliance and completeness of the requirements for each phase: 40%
   - The correctness of the implementation and evaluation running the Chat-Messaging system supported by the implemented secure protocol in each phase: 40%
   - The modularity and quality of the provided solution: 7,5%
   - The optimization and factorization of the solution (comparing with the initial provided materials) – Differences in Number of Lines of Code in the comparison with the initial materials (classes/java code): 7,5%
   - The appreciation of the solution and its potential as a generic solution that can be used by other applications using UDP/IP-Multicasting, that can be adapted to use the provided solution: 5%

5. **Project delivery**

   - The project must be submitted for evaluation in the period 14/OCT/23 to 24/OCT/23
   - Submission will be done by GOOGLE FORM
   - The form will be ready and open for submissions after 14/OCT/23 00h00 until 24/OCT/23, 23h59
   - For the submission you must answer the required questions in the Submission Form
   - The URL for the form will be sent via a CLIP message in 14/OCT/23 when the form is ready
   - For delivery, the implementation must be in a Github repository, that must be shared with: **henriquejoaolopesdomingos**
   - In the submission form you will be asked to include (mandatory) the URL of the GitHub repository with the implementation
   - The deadline for delivery is 24/OCT/23, 23h59m
   - All submitted forms will be processed on 25/OCT/2023 and ll the implementations will be downloaded and cloned for verification and subsequent evaluation on 25/OCT/2023