Universidade do Minho
Departamento de Informática
Criptografia e Segurança em Redes **2023/2024**

Trabalho Prático 2

Limite de submissão: 14/11/2023

1. Instruções

O trabalho deverá ser desenvolvido em grupo de três integrantes e submetido exclusivamente via *blackboard* na data indicada acima. Submissões por outro canal serão desconsideradas. A partir da data e hora indicados, o grupo terá um desconto de 10% da classificação por dia de atraso na entrega.

Um único membro do grupo deverá submeter uma pasta compactada contendo:

- Relatório com os detalhes sobre o desenvolvimento do trabalho, as decisões e escolhas do grupo, resultados e dificuldades enfrentadas;
- Todo o código desenvolvido devidamente comentado.

A avaliação deste trabalho levará em consideração apenas os artefactos submetidos pelo grupo. Portando, é importante garantir que o relatório possui o nível de detalhamento adequado para a avaliação do trabalho desenvolvido.

2. Descrição do trabalho

O objetivo do trabalho é desenvolver (usando uma linguagem de programação escolhida pelo grupo) um sistema de comunicação por mensagens de texto entre pares com diferentes níveis de garantia de segurança. O sistema deverá seguir uma arquitetura cliente-servidor, onde o servidor aceita conexão via *socket* em um endereço IP e porta conhecidos pelo cliente. Um esquema básico ilustrativo do serviço é apresentado na Figura 1, seguido pela descrição dos requisitos do trabalho prático.

Figura 1: Esquema básico do serviço de chat.

Após o estabelecimento de comunicação entre as duas entidades, o servidor deverá enviar uma lista de opções de comunicação com os diferentes tipos de garantia de segurança suportadas. Caso necessário, o cliente e o servidor iniciarão a troca dos

parâmetros exigidos pelo o mecanismo de segurança escolhido pelo cliente (*e.g.,* chaves, *seed*, *nonce*, etc) seguindo um protocolo (sequência de passos) definido pelo grupo.

Uma vez estabelecido um canal de comunicação seguro, a aplicação passará ao modo de *chat*, onde os utilizadores podem trocar mensagens via linha de comandos com as garantias de segurança abaixo descritas.

2.1 Modos de segurança

O serviço desenvolvido deverá suportar três modos de garantia de segurança:

A - **Integridade**: neste modo, o serviço garante a integridade das mensagens trocadas entre os utilizadores, mas não implementa um mecanismo de garantia da confidencialidade;

B - **Confidencialidade e Integridade**: neste modo, além da garantia da integridade das mensagens, o serviço deverá implementar um mecanismo para a garantia da confidencialidade suportado por uma cifra simétrica;

C - **Confidencialidade, Integridade e autenticidade**: no modo mais seguro, o serviço deverá suportar mecanismos que garantam a confidencialidade, a integridade e a autenticidade da origem da mensagem. Para isso, recorra a uma cifra de chave pública.

Para os três modos de operação, o grupo deverá escolher os mecanismos e algoritmos que julgarem mais adequados aos requisitos de segurança estabelecidos. As escolhas deverão ser devidamente justificadas no relatório do trabalho.

2.2 Demonstração

Para todos os modos de operação, o grupo deverá incluir nos resultados do trabalho (assim como no relatório) capturas de tráfego que demonstrem que o nível de proteção oferecido corresponde aos requisitos estabelecidos neste enunciado.