LEI: Segurança Informática e nas Organizações 2019-2020

Projeto 3: Autenticação

Entrega: 13 de Dezembro, 23:59

Objetivos

- Planeamento da autenticação das comunicações
- Autenticação por desafio resposta
- Autenticação com chaves assimétricas
- Utilização de certificados X.509
- Controlo de acesso

1 Descrição

Este trabalho visa explorar os conceitos relacionados com o estabelecimento de uma sessão segura entre dois interlocutores. Explora conceitos relacionados com a autenticação dos intervenientes na comunicação e o controlo de acesso dos clientes.

2 Preparação

Deve-se considerar como base o código utilizado para o projeto 2. Este código deve implementar um cliente e um servidor usando um protocolo seguro próprio baseado em mensagens JSON, sobre sockets TCP/IP. Por questões de simplicidade e de capacidade de análise das mensagens usando aplicações como a Wireshark, todas as mensagens transmitidas serão codificadas para texto (ex. usando base64), o que se mantém neste trabalho.

Se os alunos não possuirem uma versão funcional do projeto 2, deve-se considerar o código base, fornecido pelos docentes.

3 Trabalho a realizar

O projeto consiste no desenho e implementação de um protocolo que permita a comunicação segura entre dois pontos, com autenticação mútua. Pretende-se que seja possível trocar um ficheiro entre o cliente e o servidor usando o protocolo, caso o servidor considere que o utilizador tem essas permissões. O utente pode-se autenticar com senhas diretas ou com o cartão de cidadão. O servidor deverá conseguir provar a sua identidade, evintando-se ataques de MiTM ou impersonação.

O trabalho a realizar considera o planeamento, desenho, implementação e validação do protocolo. A avaliação irá focar-se em cada um dos pontos a seguir descritos, que também constituem os objetivos principais do trabalho.

1. Desenho de um protocolo (planeamento e descrição) para a autenticação de utentes através de um mecanismo de desafio resposta. Pode-se considerar a existência de uma ferramenta para aprovisionamento dos clientes do lado do servidor. Ou seja: não é necessário considerar o registo online dos clientes. (0.2 pontos)
2. Desenho de um mecanismo para controlo de acesso, que permita indicar explicitamente se um utente pode ou não transferir ficheiros. (0.2 pontos)
3. Desenho de um protocolo (planeamento e descrição) para a autenticação de utentes através do cartão de cidadão. (0.2 pontos)
4. Desenho de um protocolo (planeamento e descrição) para a autenticação do servidor utilizando certificados X.509. (0.2 pontos)
5. Implementação do protocolo para autenticação de utentes através da apresentação de senhas. (0.5 pontos)
6. Implementação do mecanismo para controlo de acesso. (0.2 pontos)
7. Implementação do protocolo para autenticação de utentes através do cartão de cidadão. (0.5 pontos)
8. Implementação do protocolo para autenticação do servidor através de certificados X.509. (0.5 pontos)

Os alunos poderão igualmente adicionar outros mecanismos que confiram maior segurança ao sistema, sendo estes avaliados como um bónus até 0.5 valores.

A entrega deverá consistir nas chaves, certificados, ficheiros de listas de utentes ou credenciais, necessárias à operação, o código desenvolvido e um relatório. O relatório deverá descrever o protocolo e demonstrar o funcionamento de cada uma das 4 funcionalidade (ex. execução mais capturas de

ecrã).

4 Notas

Considera-se que os trabalhos são realizados por 2 alunos e que o documento final submetido é de sua autoria. A utilização de recursos existentes na Internet ou partilhado com outros colegas leva à anulação imediata do trabalho.

Podem e devem ser utilizadas bibliotecas criptográficas como a `Cryptography.io` ou o `PyKCS11`. Podem também ser utilizadas outras bibliotecas, desde que forneçam apenas suporte à implementação dos mecanismos propostos.