estga
universidade de aveiro
escola superior de tecnologia
e gestão de águeda

Projeto de Segurança Informática

Trabalho realizado por Grupo 10:

Tiago Rodrigues 84040

João Mendes 86093

Licenciatura em Tecnologias da Informação

1º Semestre

2018/2019

estga
universidade de aveiro
escola superior de tecnologia
e gestão de águeda

Índice

estga
universidade de aveiro
escola superior de tecnologia
e gestão de águeda

Resumo

O objetivo deste projeto é criar um programa que, depois de iniciado, durante o registo emita um pedido de licença (com as informações do utilizador e da máquina onde se encontra), esse pedido deverá ser autenticado e enviado de volta para o programa, que a partir desse momento, vai permitir ao utilizador utilizá-lo.

Estrutura do projeto

O projeto foi dividido em duas partes, *user* e *owner*, sendo o *user* o utilizador do programa e o *owner* o dono que irá emitir as licenças.

User

Classe	Tarefa
Criptografia	Este método está encarregue de criar uma chave simétrica com o algoritmo AES, encriptar e desencriptar com essa chave.
GenerateKeys	Este método cria um par de chaves publica/privada, escreve e lê de um ficheiro.
Identification	Este método inicializa o programa atribuindo-lhe um id e uma versão. Com os respetivos getters e setters
MachineInfo	Este método adquire as informações necessárias para a identificação da máquina, sendo estas o número da Bios e o UUID (identificador único universal), este método retorna também o Unix time
Main	Este método corre os métodos de todas as classes.
ReadKeys	Este método permite ler as chaves publica e privada, e também encriptar e desencriptar com as tais.
CartaoCidadao	Este método recolhe toda a informação relevante ao cartão do cidadão, tais como os providers, a chave publica o certificado,

Owner

Classe	Tarefa
GenerateKeys	Este método cria um par de chaves publica/privada, escreve e lê de um ficheiro.
Main	Este método corre os métodos de todas as classes.
VerifyRequest	Verifica o certificado e a assinatura.
SendAutentication	Envia encripta a informação e envia a autenticação para o programa.

Requisitos e Soluções

Requisito 1: Criação de um ficheiro com um pedido de licença que inclua a identificação do utilizador, dados sobre a plataforma para a execução da aplicação e dados sobre a aplicação.

Solução 1: Foi criado um ficheiro com as informações do utilizador que são recolhidas durante o registo, password e nome, são recolhidas as informações sobre a máquina (Bios Serial, UUID, Unix Time) onde o programa se encontra a ser executado, e foram recolhidas as informações sobre o id e versão do programa executado.

Requisito 2: Proteção (integridade, confidencialidade, autenticação, não repudiação) do pedido de licença.

Solução 2: Para o pedido de licença foi criada uma mensagem com toda a informação relevante ao pedido da licença, que foi encriptada utilizando uma chave simétrica, que em seguida foi encriptada com a chave publica do owner, e tudo isso foi assinado pelo CC (cartão do cidadão), além disso, no pedido também é enviado o certificado e uma versão não assinada da mensagem.

Requisito 3: Validação do pedido de licença.

Solução 3: Não foi implementada a validação do pedido de licença.

Requisito 4: Emissão da licença, com todos os dados que garantam que apenas uma aplicação legitima pode ser executada no sistema autorizado e pelo utilizador autorizado

Solução 4: Não foi implementada a emissão de licença.

Requisito 5: Proteção (integridade, confidencialidade, autenticação, não repudiação) da licença emitida.

Solução 5: Não foi implementada uma solução para a emissão de uma licença para o cliente.

Requisito 6: Validação do documento da licença.

Solução 6: Não foi implementada a validação do documento de licença

Requisito 7: Proteção contra execução da aplicação noutro sistema.

Solução 7: Durante o login é verificado se as especificações da máquina são iguais as aprovadas na licença do produto.

Requisito 8: Proteção contra a execução da aplicação por outro utilizador.

Solução 8: Durante o login são verificados o nome do utilizador a password e os dados do cartão do cidadão, a password é comparada com a hash da password aprovada durante o registo, é também comparado o certificado do cartão do cidadão com o aprovado durante o pedido de licença.

Requisito 9: Proteção contra a alteração da aplicação.

Solução 9: Sempre que possível os métodos e as variáveis foram criados como private ou protected, e tentamos isolar os métodos uns dos outros. É bastante difícil proteger uma aplicação java de ser alterada, a partir do momento em que se encontrar na máquina de outrem, pois o programa pode ser sempre descompilado, e mesmo com a encriptação do código os padrões no código de java são fáceis de detetar, podendo estes padrões serem alterados, mas poderia fazer com que a ligação a algumas bibliotecas ou API's deixassem de funcionar.

Problemas de implementação

Não conseguimos implementar a maioria das funcionalidades no lado do owner, receber e validar o pedido de licença e emitir o pedido de licença, o que levou a não podermos verificar se o pedido de licença é válido no utilizador pois não o conseguimos criar.

Conclusão

Com este trabalho aprofundámos os conhecimentos que tínhamos sobre vulnerabilidades, criptografia, gestão de chaves assimétricas, autenticação e canais de autenticação segura.

Infelizmente não foi possível concluir todos os requisitos da aplicação por dificuldades em aprender a trabalhar com as tecnologias e bibliotecas que nunca tínhamos utilizado anteriormente acabando por se tornar uma tarefa mais difícil do que esperado.