Ciências ULisboa | Informática

di.ciencias.ulisboa.pt

/difcul

Segurança Informática

2022/2023

Trabalho 1

1 Objectivos

A componente de avaliação contínua da disciplina de Segurança Informática pretende familiarizar os alunos com alguns dos problemas envolvidos na programação de aplicações distribuídas seguras, nomeadamente a gestão de chaves criptográficas, a geração de sínteses seguras, cifras e assinaturas digitais, e a utilização de canais seguros à base do protocolo TLS. O trabalho será realizado utilizando a linguagem de programação Java e a API de segurança do Java.

A primeira fase do trabalho tem como objetivo fundamental a construção de uma aplicação distribuída. O trabalho consiste na concretização de um sistema **simplificado** de armazenamento de ficheiros, designado por **myCloud**, onde o utilizador usa um servidor central para armazenar os **seus ficheiros**.

Na segunda fase do trabalho serão adicionadas outras funcionalidades que permitirão que vários utilizadores usem o mesmo servidor e partilhem ficheiros entre si. E finalmente na terceira fase do trabalho serão configurados mecanismos de segurança ao nível do servidor: *firewall* e detecção de intrusões.

2 Arquitectura do Sistema

O trabalho consiste no desenvolvimento de dois programas:

- O servidor *myCloudServer*, e
- A aplicação cliente *myCloud* que acede ao servidor via *sockets* TCP.

A aplicação é distribuída de forma que o servidor fica numa máquina e o utilizador pode usar clientes em máquinas diferentes na Internet.

3 Funcionalidades

O sistema tem os seguintes requisitos:

1. O servidor recebe na linha de comandos a seguinte informação:
   - Porto (TCP) para aceitar ligações de clientes.
2. O cliente pode ser utilizado com as seguintes opções na linha de comandos:

   myCloud -a <serverAddress> **-c {<filenames>}+**

   myCloud -a <serverAddress> **-s {<filenames>}+**

   myCloud -a <serverAddress> **-e {<filenames>}+**

   myCloud -a <serverAddress> **-g {<filenames>}+**

   Em que:

   - -a <serverAddress>

   identifica o servidor (*hostname* ou endereço IP e porto; por exemplo 127.0.0.1:23456).

   - -c {<filames>}+

   o cliente cifra um ou mais ficheiros e envia-os para o servidor. Caso algum dos ficheiros já exista no servidor ou caso algum dos ficheiros não exista localmente, apresenta uma mensagem de erro ao utilizador e continua para os seguintes ficheiros. O cliente usa **cifras híbridas**. Assim, a chave usada

para cifrar cada ficheiro deve ser cifrada no cliente e enviada para o servidor. Cada uma destas chaves pode ser guardada num ficheiro cujo nome deve ser o nome do ficheiro original com extensão chave_secreta. Os ficheiros cifrados são guardados no servidor com extensão cifrado.

Por exemplo:

myCloud -a 127.0.0.1:23456 -c trab1.pdf aulas.doc

envia para o servidor os ficheiros cifrados e armazena-os no servidor nos ficheiros trab1.pdf.cifrado e aulas.doc.cifrado e

envia para o servidor as chaves cifradas e armazena-as nos ficheiros trab1.pdf.chave_secreta e aulas.doc.chave_secreta.

- -s {<filenames>}+

o cliente assina um ou mais ficheiros e envia-os para o servidor. Caso algum dos ficheiros já exista no servidor ou caso algum dos ficheiros não exista localmente, apresenta uma mensagem de erro ao utilizador e continua para os seguintes. As assinaturas devem ser guardadas separadamente em ficheiros com extensão assinatura. Os ficheiros assinados são guardados no servidor com extensão assinado.

Por exemplo:

myCloud -a 127.0.0.1:23456 -s trab1.pdf aulas.doc

envia para o servidor os ficheiros trab1.pdf e aulas.doc e armazena-os no servidor nos ficheiros trab1.pdf.assinado e aulas.doc.assinado e

e envia para o servidor as assinaturas e armazena-as nos ficheiros trab1.pdf.assinatura e aulas.doc.assinatura.

- -e {<filenames>}+

o cliente assina e cifra um ou mais ficheiros e envia-os para o servidor. Caso algum dos ficheiros já exista no servidor ou caso algum dos ficheiros não exista localmente, apresenta uma mensagem de erro ao utilizador e continua para os seguintes. O cliente usa **envelopes seguros (para simplificar o trabalho, os alunos não precisam de cifrar a assinatura)**. Os ficheiros são guardados no servidor com extensão seguro.

Por exemplo:

myCloud -a 127.0.0.1:23456 -e trab1.pdf aulas.doc

envia para o servidor os ficheiros trab1.pdf e aulas.doc cifrados e armazena-os no servidor nos ficheiros trab1.pdf.seguro e aulas.doc.seguro e

envia as assinaturas – idêntico à opção -s

envia as chaves – idêntico à opção -c

- -g {<filenames>}+

o cliente recebe um ou mais ficheiros. Caso algum dos ficheiros já exista localmente ou caso algum dos ficheiros não exista no servidor, apresenta uma mensagem de erro ao utilizador e continua para os seguintes.

O cliente decifra os ficheiros que tenham sido cifrados.

O cliente verifica a assinatura dos ficheiros que tenham sido assinados.

Sugere-se que esta opção seja realizada incrementalmente, à medida que sejam realizadas as outras opções. Ou seja, quando a opção -c for realizada, sugere-se que seja realizada a parte da opção -g que trata os ficheiros cifrados.

Toda criptografia assimétrica no trabalho deve usar RSA com chaves de 2048 bits. A criptografia simétrica deve ser efetuada com AES e chaves de 128 bits.

Os utilizadores do myCloud devem ter um par de chaves na keystore designada por keystore.??Cloud, onde ?? corresponde ao alias do utilizador. Por exemplo, a keystore do utilizador com alias Manuel será designada por keystore.ManuelCloud. As keystores devem ser criada previamente através do comando keytool.

4 Relatório

O relatório será preenchido no moodle**.**

5 Entrega

Código:

Dia **26 de Março**, até às 20:00 horas. O código do trabalho deve ser entregue da seguinte forma:

- Os grupos devem inscrever-se atempadamente de acordo com as regras afixadas para o efeito, na página da disciplina.
- Na página da disciplina submeter o código do trabalho num ficheiro zip e um readme (txt) sobre como executar o trabalho.

Relatório:

Dia **26 de Março**, até as 23:55 horas, no moodle.

Não serão aceites trabalhos por email nem por qualquer outro meio não definido nesta secção. Se não se verificar algum destes requisitos o trabalho é considerado não entregue.