Ciências ULisboa | Informática

di.ciencias.ulisboa.pt
/difcul

Segurança Informática

2022/2023

Trabalho 2

1 Objetivos

Esta fase do trabalho estende a anterior, possibilitando aos alunos experimentarem diversos mecanismos de segurança, tais como: MACs, comunicação com um protocolo seguro (TLS – Transport Layer Security) e gestão básica de certificados.

A envolvente do trabalho continua a ser a mesma, ou seja, a concretização de um sistema **simplificado** de armazenamento de ficheiros, designado por **myCloud**, onde o utilizador usa um servidor central para armazenar os **seus ficheiros**.

2 Modelo de adversário

Iremos assumir no trabalho que existe um adversário que pretende comprometer o correto funcionamento do sistema. O adversário terá um conjunto de capacidades que poderão ser empregues na realização das suas ações maliciosas. Torna-se assim necessário dotar o sistema dos mecanismos de proteção que lhe possibilitem manter um funcionamento correto ainda que se encontre sob ataque.

Vamos assumir que o adversário tem as seguintes capacidades:

- Acesso à rede: tendo o adversário acesso à rede, poderá escutar os pacotes trocados entre o cliente e o servidor. Potencialmente, também poderá tentar corromper, alterar, introduzir, e reproduzir mensagens de forma a enganar quer o cliente quer o servidor.

- Controlar um ou mais utilizadores: o adversário controla uma (ou mais) conta(s) de utilizadores do sistema. Através desta(s) conta(s), ele poderia tentar aceder a ficheiros para os quais não tem permissões ou corromper ficheiros com informação de outros utilizadores.

- Acesso à máquina onde o servidor é executado, em modo de leitura: o adversário tem acesso em modo de leitura aos ficheiros armazenados no servidor. Com esse acesso, ele pode potencialmente observar informação que eventualmente seria confidencial.

Em seguida indicam-se e discutem-se as proteções que devem ser adicionadas ao sistema.

3 Alterações a adicionar ao sistema

Nesta fase, os alunos devem usar a mesma arquitetura da 1ª fase. Adicionalmente, o sistema deve ser estendido para poder ser usado por vários utilizadores.
De seguida são descritas as alterações a adicionar ao sistema.

A. **Gestão utilizadores** no sistema – ficheiro de *passwords*

O servidor mantém um ficheiro (designado por *users*) com os utilizadores do sistema e respetivas informações. Este ficheiro deve **ser um ficheiro de texto**. Cada linha tem um *username* e a respetiva password (com o *salt*):

```
admin;ut4Ic9BfJNfFL2fJ+4IXGQ==;yn9ZU+vkUK/mtt+vuRU7az3yb4vWEPmoyXXRaI8nxIc=
maria;w9CfDqX9Li5krpdJZgg/Qh;A46KPmM+bClnR5D8URnVAzG9heNbvxop5eQq1leAcuk=
alice;dbqPTW49yNLmOJK4RC;MAOgRGmbTqpwNdI5yIjZJICRG7CvKlRNOozCKx0QsyY=
```

Com este objetivo, o servidor passará a identificar o utilizador e irá distinguir quem acede aos ficheiros.

B. Para aceder ao sistema **myCloud**, o cliente passará a necessitar de **receber** a opção -u e -p que permitem indicar o *username* (-u) e a *password* (-p).

   Exemplo (o mesmo se aplica às outras opções):

   myCloud -a <serverAddress> -u <username> -p <password> **-c {<filenames>}+**

   O sistema deve assumir que a *keystore* do utilizador está guardada no ficheiro ***username***.*keystore*, onde *username* corresponde ao *username* do utilizador.

   As passwords serão dadas na linha de comandos para simplificar o trabalho.

C. **Criação** de utilizadores

   A opção -au será utilizada para criar utilizadores:

   myCloud -a <serverAddress> -au <username> <password> <certificado>

   onde

   <username> e <password> correspondem ao *username* e à *password* do novo utilizador.

   Caso seja introduzido um *username* já existente, deve ser devolvida uma mensagem de erro e o programa deve terminar.

   O campo <certificado> representa o ficheiro .cer correspondente ao certificado gerado para o utilizador.

   Exemplo:

   myCloud -a 10.101.21.22 -au maria ut12?!WE maria.cer

   O ficheiro correspondente ao certificado da maria (maria.cer) pode ser obtido através do keytool.

   Exemplo:

   keytool -export -keystore maria.keystore -alias maria -file maria.cer

   Os ficheiros .cer devem ser guardados numa diretoria própria destinada apenas a guardar os certificados dos utilizadores.

   Com a criação de um novo utilizador, será criada também uma diretoria para esse utilizador no servidor, onde deverão ser guardados os ficheiros do utilizador.

D. O servidor deve proteger a **confidencialidade das *passwords***. Com este objetivo, as passwords devem ser armazenadas utilizando mecanismos baseados em algoritmos de sínteses e *salts*. O ficheiro das *passwords* deve manter o formato indicado em A.

E. O servidor deve proteger a **integridade do ficheiro das passwords**. Para tal, o ficheiro deve ser protegido com um MAC. O cálculo deste MAC utiliza uma chave simétrica calculada a partir da *password* do MAC.

   No início da sua execução, o servidor pede a password do MAC para verificar a integridade do ficheiro das passwords. Se o MAC estiver errado, o servidor deve imprimir um aviso e terminar imediatamente a sua execução. Se não há MAC a proteger o ficheiro, o servidor deve imprimir um aviso e perguntar ao utilizador do **myCloud** (utilizador que inicia a execução do servidor **myCloud**) se pretende calcular o MAC. O MAC deve **ser verificado em todos os restantes acessos ao ficheiro de passwords e atualizado caso o ficheiro seja alterado**.

Caso não exista o ficheiro das passwords, o MAC não é verificado.

O MAC pode ser guardado num ficheiro utilizado apenas para este efeito, designado por exemplo passwords.mac

F. Na comunicação entre o cliente e o servidor pretende-se garantir a **autenticidade do servidor** (um atacante não deve ser capaz de fingir ser o servidor e assim obter a password de um utilizador) e a **confidencialidade** da comunicação entre cliente e servidor (um atacante não deve ser capaz de escutar a comunicação). Para este efeito, devem ser usados **canais seguros** (protocolo TLS/SSL). Este protocolo permite verificar a identidade do servidor utilizando chaves assimétricas.

G. O sistema deve permitir enviar ficheiros para o servidor para outros utilizadores. Para tal pode ser usada a opção -d:

myCloud -a <serverAddress> -u <username> -p <password> -d <username de destinatário> **-c {<filenames>}+**

no seguinte exemplo:

myCloud -a 10.101.21.22 -u maria -p ut12?!WE -d alice **-c aa.pdf bb.txt**

são colocados na diretoria da alice no servidor os seguintes ficheiros

aa.pdf.cifrado.maria

aa.pdf.chave_secreta.maria – chave secreta usada para cifrar o aa.pdf e cifrada com a chave pública da alice

bb.txt.cifrado.maria

bb.txt.chave_secreta.maria – chave secreta usada para cifrar o bb.txt e cifrada com a chave pública da alice

A maria pode ter previamente o certificado da alice. Caso não o tenha, terá de o pedir ao servidor.

Caso a opção -d seja omitida, ao nome dos ficheiros deve ser também adicionado o *username* do próprio utilizador. Aplica-se a mesma alteração às opções *-s* e *-e*.

myCloud -a <serverAddress> -u <username> -p <password> -d <username de destinatário> **-s {<filenames>}+**

no seguinte exemplo:

myCloud -a 10.101.21.22 -u maria -p ut12?!WE -d alice **-s aa.pdf bb.txt**

são colocados na diretoria da alice no servidor os seguintes ficheiros

aa.pdf.assinado.maria

aa.pdf.assinatura.maria – assinatura feita pela maria

bb.txt.assinado.maria

bb.txt.assinatura.maria – assinatura feita pela maria

Na opção -g, a alice pode ter o certificado da maria para poder validar a assinatura. Caso não o tenha, terá de o pedir ao servidor.

No seguinte exemplo, o seu funcionamento é semelhante aos anteriores.

myCloud -a <serverAddress> -u <username> -p <password> -d <username de destinatário> **-e {<filenames>}+**

Considerando o seguinte exemplo:

myCloud -a <serverAddress> -u <username> -p <password> **-g {<filenames>}+**

a opção -g terá de ser alterada em conformidade com as alterações anteriores. Em particular, para validar a assinatura, é necessário ter em conta quem efetuou a assinatura (através do nome do ficheiro).

Caso o utilizador não tenha o certificado do assinante, o utilizador deve pedir ao servidor o respetivo certificado. No caso do servidor não ter o certificado, o utilizador deve ser avisado sobre a impossibilidade de se verificar a assinatura.

4 Entrega

Código:
Dia **14 de Maio**, até às 23:55 horas. O código do trabalho deve ser entregue na página da disciplina. Os alunos deverão submeter o código do trabalho num ficheiro zip e um readme (txt) sobre como executar o trabalho.

Relatório:
Dia **15 de Maio**, até às 9:30 horas, no moodle.

No relatório devem ser apresentados e discutidos os seguintes aspetos:

- Os objetivos concretizados com êxito
- Os problemas encontrados.
- A segurança da aplicação criada, identificando possíveis **fraquezas e melhorias** a incluir em versões futuras.

O relatório deve ter no máximo 5 páginas.

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.

5 Avaliação dos Trabalhos

A avaliação dos trabalhos e dos alunos será efetuada nas 2 últimas semanas de aulas.
A avaliação será composta por 2 momentos:

1) Avaliação do trabalho
2) Avaliação de cada um dos elementos do grupo. Neste momento, os alunos terão de fazer alterações aos trabalhos entregues demonstrando os seus conhecimentos sobre estes trabalhos.