Ciências ULisboa | Informática

di.ciencias.ulisboa.pt

/difcul

Segurança Informática

2023/2024

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 **mySNS**, onde o utilizador usa um servidor central para armazenar os **seus ficheiros** referentes a exames e prescrições médicas.

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 autenticados.
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*), separador por **;**

```
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.

O servidor, no início da sua execução, deve verificar se existe o ficheiro de *passwords* no sistema. Caso não exista, deve criar automaticamente o ficheiro com o utilizador com *username admin* e pedir a *password* para este utilizador.

B. Para aceder ao sistema **mySNS**, o cliente passará a necessitar de **receber** a opção -p que permite indicar a *password* (-p) do utilizador.

```
mySNS -a <serverAddress> -m <username do médico> -p <password> -u <username do utente> -sc {<filenames>}+
mySNS -a <serverAddress> -m <username do médico> -p <password> -u <username do utente> -sa {<filenames>}+
mySNS -a <serverAddress> -m <username do médico> -p <password> -u <username do utente> -se {<filenames>}+
myCloud -a <serverAddress> -u <username do utente> -p <password> -g {<filenames>}+
```

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

C. **Criação** de utilizadores

A opção -au será utilizada para criar utilizadores:

```
mySNS -a <serverAddress> -au <username> <password> <ficheiro com certificado>
```

onde

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

<ficheiro com certificado> identifica o ficheiro do certificado do utilizador a enviar para o servidor. Os alunos têm de criar uma diretoria no servidor para armazenar todos os certificados.

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

Exemplo:

```
mySNS -a 10.101.21.22 -au maria ut12?!WE maria.cert
```

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

Exemplo:

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

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 utilizador *admin*.

No início da sua execução, o servidor pede a password do admin e deve usar o 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 administrador do **mySNS** (utilizador que inicia a execução do servidor **mySNS**) 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.

Como referido anteriormente, caso não exista o ficheiro das passwords, o servidor deve criá-lo e de seguida, deve calcular o respetivo MAC.

O MAC será guardado num ficheiro utilizado apenas para este efeito.

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. Todas a opções do trabalho 1 devem ser estendidas do seguinte modo: caso seja necessário um certificado de um utilizador que não exista na keystore do utilizador que está a usar o cliente mySNS, o cliente mySNS deve pedir o certificado ao servidor e adicioná-lo à keystore do utilizador. Deste modo, não é necessário fazer os *imports* dos certificados previamente.

4 Avaliação

A avaliação dos projetos será feita segundo uma abordagem funcional, onde cada funcionalidade descrita no enunciado deve ser apresentada pelos alunos. Não serão consideradas funcionalidades incompletas ou valorizada qualquer implementação não funcional. **É obrigatório apresentarem os trabalhos em três máquinas distintas do laboratório (servidor e 2 clientes em máquinas separadas).** De preferência, devem utilizar o sistema operativo Linux.
Considere, por exemplo, o seguinte cenário.

Cada uma das opções/funcionalidades apresentadas será valorizada de acordo com a seguinte tabela.

Funcionalidade	Valorização	Validação
Gestão utilizadores		
Autentica corretamente utilizadores Adiciona utilizador admin, caso não exista Adiciona utilizadores (criar user) Verifica password Ficheiro de passwords com formato correto (texto e separador)	1.25 0.5	
Envia o certificado (enviar para o servidor e armazenar no servidor)	+0.5	
Usa corretamente o salt	+1	

Usa corretamente algoritmo de síntese	+1	
Apresenta mensagens de erro (utilizar existe, utilizador não existe/password incorrecta, …)	+0.25	
Algoritmo eficiente para procura de utilizadores	+0.25	
Funciona qualquer que seja o número de utilizadores	+0.25	
Adiciona utilizador apenas caso não exista	+0.25	
Apenas envia ficheiros para utilizadores existentes	+0.25	
Não usam algoritmos seguros	**Penalização** de 1 valor	
Preparação da apresentação para a avaliação e cumprimento do tempo	0.5	
MAC		
Calcula o MAC corretamente e valida-o corretamente	3	
Calcula um novo MAC em **todas** situações previstas (início, caso necessário, e sempre que há alterações)	+1	
Valida o MAC em **todas** as situações previstas (início e em todos os acessos)	+1	
Apresenta mensagens de erro (quando mac não existe, mac incorreto, …)	+0.25	
Funciona qualquer que seja a dimensão do ficheiro das passswords	+0.25	
Não usam algoritmos seguros	**Penalização** de 1 valor	
Preparação da apresentação para a avaliação e cumprimento do tempo	0.5	
Sockets seguros (TLS)		
TLS/SSL a funcionar	3	
Relatório		
Relatório (e entrega dentro do prazo)	1	
Extensão das opções do trabalho 1		
Import do certificado para a keystore do utilizador para 1 das opções (verifica que não tem, pede ao servidor e guarda na keystore)	2	
Import do certificado para a keystore do utilizador para cada uma das outras 3 opções	3x0.5	
Preparação da apresentação para a avaliação e cumprimento do tempo	0.5	

5 Entrega

Código:

Dia **28 de Abril**, até às 20:00 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 **28 de Abril**, até às 23:55 horas, no moodle.

No relatório devem ser apresentados e discutidos os seguintes aspetos:

- Os objetivos concretizados com êxito
- Os problemas encontrados
- Tabela de auto avaliação preenchida
- Análise crítica à segurança da aplicação criada, identificando 2 possíveis **fraquezas e melhorias** a incluir em versões futuras. Na análise crítica não devem foca-se nas limitações da vossa implementação, caso não tenham cumprido todos os requisitos. Deve considerar a aplicação final de acordo com os requisitos do trabalho.

O relatório deve ter no máximo 3 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.

6 Avaliação dos Trabalhos

A avaliação dos trabalhos e dos alunos será efetuada nas 2 últimas semanas de aulas.