**1Segurança de Redes e Sistemas de Computadores**

**2018/2019, 2º Sem.**

**Ficha de Implementação do Trabalho Prático nº 2**

**Aluno ou Grupo de Alunos**

|  |  |
| --- | --- |
| **Nº de Aluno** | **Nome Apelido** |
|  |  |
|  |  |

**Caracterização Geral da Implementação entregue.**

**Coloque X nas respetivas colunas e fases implementadas.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Fases Implementadas** | **SIM, comprovado funcionamento correto** | **NÃO implementado** | **Implementação parcial, mas o que foi implementado foi testado com funcionamento correto** | **Implementação parcial foi endereçada, mas não funciona corretamente** |
| **Só foi implementada a FASE 1** |  |  |  |  |
| **Foram implementadas as FASES 1 e 2** |  |  |  |  |

1. **Introdução e caracterização do trabalho desenvolvido, em relação aos aspetos da FASE 1**

**1.1 Colocar X nas colunas da seguinte TABELA de acordo com a sua implementação**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Tabela de caracterização da FASE 1: Implementação e completude do trabalho**  **Critérios de caracterização da solução e implementação entregue** | **A)** | **B)** | **C)** | **D)** | **E)** |
| **SIM** | **NÃO** | **Parcialmente, ou de forma incompleta** | **Funciona corretamente com comprovação experimental** | **Funciona incorretamente ou não funciona** |
| 1 | Foram implementados totalmente todos os requisitos da FASE 1, de acordo com as especificações inicialmente endereçadas pelo enunciado |  |  |  |  |  |
| 2 | Foi implementada a arquitetura e todos os módulos de acordo com o enunciado (nomeadamente: módulos/componentes: Client. FServ (Main Dispatcher, Authentication (Auth), AccessControl e Storage) |  |  |  |  |  |
| 3 | O cliente apenas interage diretamente com o Dispatcher, sendo este módulo a intermediar todas as interações com os restantes módulos |  |  |  |  |  |
| 4 | A interação entre todos os módulos está suportada e protegida com TLS, permitindo suporta TLSv1.1 ou TLSv1.2 e autenticação mútua |  |  |  |  |  |
| 5 | Todas as operações requeridas para a manipulação (gestão) de ficheiros para operação do cliente, de acordo com o sistema implementado, estão implementadas e executam corretamente |  |  |  |  |  |
| 6 | Foi implementado um protocolo de autenticação de clientes e suportam-se sessões de clientes com controlo de autenticação e validação de sessões |  |  |  |  |  |
| 7 | As operações que são realizadas pelo Dispatcher no módulo Access Control, permitem que o Access Control possa verificar que o pedido do Dispatcher está a ser feito em nome de um cliente (user) numa sessão autenticada, pois pode escrutinar a prova de autenticação do cliente que resultou da autenticação desse cliente pelo módulo de autenticação. |  |  |  |  |  |
| 8 | As operações que são realizadas pelo Dispatcher no módulo Storage permitem que Storage possa verificar que o pedido do Dispatcher está a ser feito em nome de um cliente numa sessão autenticada, pois pode escrutinar a prova de autenticação do cliente (user) que resultou da verificação de controlo de acesso para essa operação, pois pode escrutinar que tal foi verificado pelo módulo de controlo de acesso. |  |  |  |  |  |
| 9 | Os módulos de Storage, Controlo de Acesso e Autenticação não interagem diretamente, apenas interagindo diretamente com o Dispatcher |  |  |  |  |  |
| 10 | Os ficheiros armazenados no módulo de *storage* são sempre armazenados cifrados e possuem provas de autenticação com base em assinaturas digitais dos clientes que os mandaram armazenar. |  |  |  |  |  |
| 11 | A implementação suporta clientes concorrentes (com sessões concorrentes) |  |  |  |  |  |
| 12 | A interação cliente / Main Dispaher está baseada em sockets (sockets TLS), sendo as operações suportadas por mensagens |  |  |  |  |  |
| 13 | A interação cliente / Main Dispaher está baseada em REST |  |  |  |  |  |
| 14 | As interações TLS podem ser parametrizáveis em relação às ciphersuites TLS que se pretendam utilizar pois isso é suportado de forma configurável |  |  |  |  |  |
| 15 | Foi testado e comprova-se experimentalmente o funcionamento das seguintes parametrizações: TLS v1.1, TLSv1.2, autenticação do servidor ou mútua e as seguintes Ciphersuites, em todos os endpoints de todos os módulos da arquitetura, podendo serem usadas diferentes configurações nas interações entre os diferentes módulos.  TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 |  |  |  |  |  |
| 16 | Para se suportarem as configurações em 15., basta que se configurem os ficheiros de configuração nos diversos endpoints, podendo usar-se sempre as mesmas keystores ou trustedstores |  |  |  |  |  |
| 17 | No protocolo de autenticação implementado está a usar-se o méodo de Diffie-Hellman, no suporte de autenticação de clientes com base no módulo de autenticação |  |  |  |  |  |
| 18 | O FServ (Main Dispatcher) verifica ou valida as operações solicitadas pelo cliente com base em informação de autenticação validada na sessão, pois as operações são sempre solicitadas pelo cliente com envio de informação de validação de autenticação na sessão (sob a forma deverificadores - tokens ou cookies de sessão - que são obtidos pelo cliente na autenticação do mesmo e podem ser atestados na sua autenticidade e validade, seja pelo cliente, seja pelo Dispatcher |  |  |  |  |  |
| 19 | Existe controlo de validade da duração da prova de autenticação de clientes em sessão, havendo controlo dessa validade ou de expiração de provas de autenticação por parte do cliente e do Dispatcher |  |  |  |  |  |
| 20 | Após uma operação de logout, a única forma de um cliente usar o sistema é se voltar a realizar a operação de login e assim obter nova prova de autenticação, pois não é possível a reutilização de provas de autenticação de sessões anteriores, uma bez que estas são completamente descartadas no processamento da operação de logout |  |  |  |  |  |
| 21 | Quando o Fserv (Main Dispatcher) interage com o componentes Access Control para a verificação das permissões do cliente, o módulo Access Control pode comprovar por si mesmo a autenticidade do cliente na sessão para o qual se está a verificar as permissões |  |  |  |  |  |
| 22 | Quando o Fserv (Main Dispatcher) interage com os componente Storage para suportar as operações no repositório de armazenamento, o módulo Storage pode comprovar por si mesmo a autenticidade do cliente na sessão para o qual se estão a solicitar as operações |  |  |  |  |  |
| 23 | Na comprovação experimental da implementação, pode comprovar-se que todos os módulos podem executar de forma distribuída, podendo cada um deles executar em diferentes maquinas (físicas ou virtuais) |  |  |  |  |  |

* 1. **Aspetos de clarificação sobre critérios de 1 a 20 na tabela do ponto 1.1**

|  |  |
| --- | --- |
| **Inclua a justificação dos seguintes critérios de 1 a 15, só no caso dos critérios que tiver caracterizado como “C - Parcialmente, ou de forma incompleta” para os caracterizar.** | |
| Critério 1 |  |
| Critério 2 |  |
| Critério 3 |  |
| Critério 4 |  |
| Critério 5 |  |
| Critério 6 |  |
| Critério 7 |  |
| Critério 8 |  |
| Critério 9 |  |
| Critério 10 |  |
| Critério 11 |  |
| Critério 12 |  |
| Critério 13 |  |
| Critério 14 |  |
| Critério 15 |  |

|  |  |
| --- | --- |
| **Inclua a justificação dos seguintes critérios de 13 a 20, só no caso dos que tiver caracterizado com a opção “A – SIM”, de acordo com a correção e funcionamento na sua avaliação e teste experimental, ou como setup que pode ser comprovado em demonstração do seu trabalho** | |
| Critério 16 |  |
| Critério 17 |  |
| Critério 18 |  |
| Critério 19 |  |
| Critério 20 |  |
| Critério 21 |  |
| Critério 22 |  |
| Critério 23 |  |

* 1. **Colique a seguir uma listagem do conteúdo do ficheiro de configuração de um endpoint TLS (ficheiro de parametrização da versão de protocolo, *ciphersuites* e tipo de autenticação – unilateral ou mútua), tal como é suportado na implementação e configuração dos vários módulos da sua solução**
  2. **Coloque a seguir a listagem do conteúdo da keystore usada como trusted store do FServ (Dispatcher Module)** quando se está a usar autenticação mútua com o cliente

**Note que se trata da listagem obtida com keytool –list –keystore <keystore file>**

* 1. **Coloque a seguir a listagem do conteúdo da keystore usada como trusted store do FServ (Dispatcher Module)** quando se está a usar autenticação mútua com o cliente

**Note que se trata da listagem obtida com keytool –list –keystore <truststore file>**

* 1. **Coloque na seguinte tabela as passwords que protegem as keystores e trusted stores usadas por todos os módulos da solução (tal como submeteu a implementação), de modo a que possa ser comprovada a operação do seu trabalho**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Módulo** | **Keystore como cliente endpoint TLS** | **Keystore como servidor endpoint TLS** | **Truststore como cliente endpoint TLS** | **Truststore como servidor endpoint TLS** |
| **Cliente** |  | **NÃO APLICÁVEL** |  | **NÃO APLICÁVEL** |
| **FServ / Dispatcher** |  |  |  |  |
| **Auth** | **NÃO APLICÁVEL** |  | **NÃO APLICÁVEL** |  |
| **Access Contol** | **NÃO APLICÁVEL** |  | **NÃO APLICÁVEL** |  |
| **Storage** | **NÃO APLICÁVEL** |  | **NÃO APLICÁVEL** |  |

1. **Introdução e caracterização do trabalho desenvolvido, em relação à implementação da FASE 2**

**2.1 Colocar X nas colunas da seguinte tabela, de acordo com a sua implementação**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **FASE 2: Implementação e completude do trabalho em relação aos requisitos e possíveis opções de desenvolvimento**  **Critérios de caracterização da solução e implementação entregue (cobertura de requisitos da FASE 2)** | **A)** | **B)** | **C)** | **D)** | **E)** |
| **SIM** | **NÃO** | **Parcialmente, ou de forma incompleta** | **Funciona corretamente com comprovação experimental** | **Funciona incorretamente ou não funciona** |
| 1 | A minha solução da fase 2 permite o suporte de clientes concorrentes atuando em sessões autenticadas concorrentes |  |  |  |  |  |
| 2 | Foi implementado o suporte que permite que os ficheiros armazenados (através do módulo Storage) estejam guardados se acedidos estando sempre cifrados, com a privacidade assegurada face a ameaças de adversários do tipo “HbC – Honest But Curious”, que possam por exemplo monitorizar a memória ou o sistema de ficheiros na máquina que suporta o módulo/serviço de Storage |  |  |  |  |  |
| 3 | Para as garantias do ponto anterior (1) nenhuma chave de cifra usada para cifrar os ficheiros é exposta ou usada fora do controlo do cliente |  |  |  |  |  |
| 4 | No suporte anterior, estão ainda incluídas provas de integridade e autenticidade com assinaturas digitais dos ficheiros por parte dos respetivos clientes que os guardaram, podendo assim os clientes saber se os mesmos foram alterados ou forjados ilicitamente |  |  |  |  |  |
| 5 | O cliente pode usar diferentes chaves pata cifrar diferentes ficheiros que foram armazenados, controlando o cliente a chave que deve ser usada (bem como modo ou *padding* usado ) para efeitos de recuperar qualquer ficheiro que tenha sido armaenado |  |  |  |  |  |
| 6 | A minha solução possui mecanismos de mitigação de ataques por inferência que permitam a um adversário que atua no sistema de storage poder inferir sobre tipologias de ficheiros, inferência de conteúdos por interpretação do nome dos ficheiros ou inferência por vai do tamanho dos ficheiros |  |  |  |  |  |
| 7 | Para além de 5., a minha solução possui outros mecanismos de mitigação de possíveis ataques por inferência do que está armazenado ao nível do serviço disponibilizado pelo módulo de storage |  |  |  |  |  |
| 8 | A minha implementação foi enriquecida com proteção para alta disponibilidade garantindo que os ficheiros estão acessíveis mesmo quando um oponente apague ilicitamente um ou mais dos ficheiros cifrados que estão armazenados |  |  |  |  |  |
| 9 | A interoperabilidade entre todos os módulos (cliente e todos os o FServer na solução da fase 2) é toda suportada em sockets TLS e intercomunicação por invocações REST protegidas por TLS, autenticação mútua, suporte da versão do protocolo (TLS v1.1 ou TLS v1.2) bem como reforço de parametrização de *ciphersuites* para qualquer uma das anteriores versões TLS. |  |  |  |  |  |
| 10 | A interoperabilidade entre todos os módulos (cliente e todos os o FServer na solução da fase 2) é toda suportada em invocações REST/TLS em que a proteção TLS pode assegurar autenticação mútua, suporte da versão do protocolo (TLS v1.1 ou TLS v1.2) bem como reforço de parametrização de ciphersuites para qualquer uma das anteriores versões TLS |  |  |  |  |  |

* 1. **Aspetos de clarificação sobre critérios de 1 a 10 conforme a sua caracterização na tabela anterior**

|  |  |
| --- | --- |
| **Critério #** | **Inclua a justificação dos seguintes critérios só no caso de ter escolhido “C - Parcialmente, ou de forma incompleta”** |
| Critério 1 |  |
| Critério 2 |  |
| Critério 3 |  |
| Critério 4 |  |
| Critério 5 |  |

|  |  |
| --- | --- |
| **Critério #** | **Inclua a justificação ou argumentação dos seguintes critérios só no caso de ter escolhido “A – SIM”** |
| Critério 5 |  |
| Critério 7 |  |
| Critério 7 |  |
| Critério 8 |  |

|  |  |
| --- | --- |
| **Critério #** | **Inclua a justificação dos seguintes critérios só no caso de ter escolhido “C - Parcialmente, ou de forma incompleta”** |
| Critério 9 |  |
| Critério 10 |  |

**2.3 Colocar X nas seguintes colunas de critérios adicionais em relação aos critérios da tabela em 2.1.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **FASE 2: Implementação e completude do trabalho em relação aos requisitos e possíveis opções de desenvolvimento**  **Critérios de caracterização da solução e implementação entregue (cobertura de requisitos da FASE 2)** | **A)** | **B)** | **C)** | **D)** | **E)** |
| **SIM** | **NÃO** | **Parcialmente, ou de forma incompleta** | **Funciona corretamente com comprovação experimental** | **Funciona incorretamente ou não funciona** |
| 11 | A interoperabilidade entre todos os módulos (cliente e todos os o FServer na solução da fase 2) é suportada de forma diferente do indicado na tabela do ponto 2.1, em relação após pontos 9 e 10. No entanto a minha implementação garante proteção TLS assegurando autenticação mútua, suporte da versão do protocolo (TLS v1.1 ou TLS v1.2) bem como reforço de parametrização de ciphersuites para qualquer uma das anteriores versões TLS |  |  |  |  |  |
| 12 | A minha implementação, por concepção, poderia ser estendida de forma a usar um modelo de armazenamento com diversidade e uso de múltiplas clouds de armazenamento (*multi-cloud storage* ou s*torage nebula*), de modo a poder beneficiar das vantagens dos modelos e soluções *outsourced* de armazenamento em cloud, mas com garantias de controlo das propriedades de segurança, fiabilidade (tolerância a falhas devidas au *cloud-outages* bem como de proteção de eventuais práticas do tipo *cloud-vendpr-lock-in*, oferecendodisponibilidade permanente, por tolerância a indisponibilidade de alguma das *storage-clouds* que fossem usadas |  |  |  |  |  |
| 13 | A minha implementação, por desenho e por implementação pode permitir ser suportada num ambiente distribuído na Internet, em que os vários módulos podem ser suportados executando em diferentes máquinas. |  |  |  |  |  |
| 14 | Para efeitos de demonstração do ponto 13, foi verificado ou será possível demonstrar que é possível executar os diversos módulos em diferentes máquinas virtuais (usando virtualização VMware ou VirtualBOX) |  |  |  |  |  |
| 15 | Para efeitos de demonstração do ponto 13, a minha implementação possui os módulos implementados de forma a poderem executar como componentes/serviços docker, pelo que pode ser demonstrado esse *deployment* para demonstração do isolamento dos componentes e o seu possível suporte em máquinas distintas |  |  |  |  |  |
| 16 | Na minha solução, utilizo o suporte STUNNEL para suportar as comunicações protegidas por TLS, de acordo com o anteriormente caracterizado em 13, 14 ou 15. |  |  |  |  |  |

* 1. **Aspetos de clarificação sobre critérios de 11 a 16 conforme a sua caracterização na tabela anterior**

|  |  |
| --- | --- |
| **Critério #** | **Inclua a justificação ou argumentação dos seguintes critérios só no caso de ter escolhido “S - SIM”** |
| Critério 11 |  |
| Critério 12 |  |

|  |  |
| --- | --- |
| **Critério #** | **Inclua a justificação dos seguintes critérios só no caso de ter escolhido “C - Parcialmente, ou de forma incompleta”** |
| Critério 13 |  |
| Critério 14 |  |
| Critério 15 |  |
| Critério 16 |  |

* 1. **Adicione se entender quaisquer outros critérios relativos às suas opções de implementação, argumentáveis como aspetos de extensão, valorização ou diferenciação da sua implementação para que possam ser apreciados.**

Inclua e argumente sobre a implementação a que se referem