Universidade do Minho
Mestrado Integrado em Engenharia Informática
Tecnologia de Segurança
Trabalho Prático 1

1 *- Instruções*

- O trabalho prático deverá ser feito em dupla;
- A submissão deverá ser feita por apenas um dos integrantes do grupo, exclusivamente, via *blackboard*;
- A entrega consiste em um ficheiro pdf que inclua toda a análise proposta neste enunciado;
- O prazo de submissão será 23h59 do dia **20/11/2020**

2 - *Objetivo*

Como membros da equipa de desenvolvimento de um serviço de identificação digital e móvel, vocês são responsáveis pela componente de projeto relacionada com a segurança da informação e infraestrutura de suporte. Para isso, numa primeira fase, é necessário que identifiquem todos os aspectos que representam riscos a este sistema.

Como objetivo principal, espera-se que a sua análise identifique e descreva potenciais incidentes de segurança aos quais o respetivo sistema poderá estar exposto quando em produção. Serão valorizados os trabalhos que apresentem, também, possíveis soluções ou alterações no projeto capazes de eliminar ou mitigar os riscos identificados.

É importante que esta análise seja detalhadamente documentada para posterior validação e orientação das demais equipas envolvidas no projeto. Além disso, procure fornecer para estas equipas uma avaliação sobre os aspectos mais críticos identificados na sua análise, indicando quais devem ser priorizados do ponto de vista da segurança global da informação e da infraestrutura do sistema.

Algumas das técnicas e artefactos que podem ser usados na sua análise incluem:

- Catalogação de vulnerabilidades e *exploits*;
- Catalogação de fraquezas típicas
- Modelação de ameaças:
  - Orientado aos ativos;
  - Orientado aos atacantes;
  - Orientado ao software.
- Análise de risco.

Vale ressaltar que sua análise não precisará se restringir à lista anterior e poderá adotar uma abordagem mista, recorrendo a diferentes técnicas complementares.

3 *- Descrição do sistema em desenvolvimento*

O sistema em desenvolvimento suportará um serviço de desmaterialização de documentos de identificação pessoal. Através dele, um cidadão poderá substituir um documento físico por um equivalente, digital (i.e., *mID*), armazenado em um *smartphone*. Por se tratar de dados pessoais sensíveis, tal sistema precisará garantir confiabilidade, materializada em soluções robustas de segurança em todos as entidades que o compõe.

A utilização deste documento de identificação em interacções cotidianas requer uma aplicação compatível (i.e., *leitor*). Através dela, um verificador (pessoa ou entidade a quem se faz prova de identidade) estabelece uma conexão com o dispositivo de um portador (pessoa que faz prova de identidade) por onde são pedidos e transmitidos atributos de identificação. Estes atributos são representados por estruturas de dados passíveis de verificação quanto a autenticidade e integridade por parte do leitor.

Abaixo são apresentados detalhes de cada entidade do sistema, suas principais funções, interações com demais entidades e requisitos de segurança. Note que por se tratar de em projeto em andamento, algumas entidades trazem maior detalhe técnico. Além disso, os requisitos de segurança aqui apresentados são genéricos, pelo que a sua análise será responsável pelo aperfeiçoamento desta dimensão do projeto.

Aplicação mID (aplicação do portador)

Corresponde a uma aplicação móvel para sistemas operativos Android e IOS. Esta aplicação armazena os dados de um documento de identificação e os elementos usados pela aplicação *leitor* para verificar a sua integridade e autenticidade.

Na primeira vez que o portador usa a aplicação, esta conecta-se com a infra-estrutura de uma entidade emissora de documentos (usando comunicação TCP/IP) para o download de todos os dados associados a este documento. Para isso, o cidadão autentica-se ao respectivo serviço por forma a iniciar a transferência do seu documento. Esta operação repete-se periodicamente para eventuais atualização de dados, neste caso, sem recorrer a uma autenticação explicita ao sistema. Em ambas as situações, é preciso garantir mecanismos robustos de autenticação, a confidencialidade e a integridade dos dados transferidos para o dispositivo do portador. Dados estes transferidos em formato *JSON - JavaScript Object Notation*.

Além disso, é igualmente relevante a garantia da integridade e autenticidade dos dados armazenados no dispositivo do portador.

Todas as operações que correspondem a uma prova de identidade, seja pela transferência de toda a informação de um documento armazenado ou de apenas um subconjunto deste, ocorre entre um dispositivo leitor e o dispositivo do portador. Estas operações podem assumir dois modos: (i) *off-line*, onde o dispositivo do portador transfere os atributos de identificação diretamente para o dispositivo leitor, assim como os dados necessários para a sua verificação; (ii) *on-line*, onde o dispositivo leitor transfere um token de autorização para que o verificador consulte diretamente a entidade emissora do documento, garantindo assim, dados mais recentes sobre o respetivo cidadão.

Em ambas as situações, o estabelecimento da comunicação é, sempre, iniciada pelo dispositivo do portador através de um *QR Code* contento toda a informação necessária

para que o dispositivo leitor o encontre e inicie a conexão, que pode usar uma das seguintes tecnologias: *BLE - Bluetooth Low Energy*; *NFC - Near Field Communication*; *WiFi-Aware*.

Uma vez estabelecido um canal entre os dispositivos, o verificador envia um pedido contendo os identificadores dos atributos desejados. A este pedido, o portador pode aceitar a transferência da sua totalidade, ou de apenas um subconjunto dos atributos solicitados. Toda esta comunicação é suportada por mensagens codificados no formato CBOR - *Concise Binary Object Representation*.

Assim como a comunicação com a entidade emissora, é preciso garantir que a interação entre o dispositivo do portador e o dispositivo leitor garante confidencialidade e integridade dos dados transmitidos. Um outro requisito relevante é permitir auditar as interações ocorridas com leitores, por exemplo, indicando os dados transmitidos para um leitor em particular e quando ocorreu.

Aplicação leitora (aplicação do verificador)

Assim como a *aplicação mID*, a aplicação leitora corresponde a uma aplicação móvel para sistemas operativos Android e IOS, ou qualquer outro dispositivo que suporte os 3 protocolos de comunicações e operações aqui definidos. Através desta aplicação, um verificador estabelece comunicação com o portador e solicita atributos suficientes para o identificar no âmbito de um serviço em particular. Por exemplo, para fazer prova de maioridade ou comprovar residência.

Esta aplicação precisa suportar todos os protocolos indicados para a *aplicação mID*. Além disso, cabe ao verificador decidir se a operação será em modo off-line ou em *modo on-line*. É necessário também que esta aplicação forneça os dados necessários para permitir auditoria das operações por parte do portador. Para isso, a própria aplicação ou seu utilizador devem ser autenticados.

No *modo on-line* de operação, é preciso garantir que a aplicação leitora não é capaz de alterar a lista de atributos autorizados pelo portador antes da consulta à infra-estrutura da entidade emissora.

Entidade emissora (backend do sistema)

Corresponde à entidade com poder de emitir e conferir autenticidade a um documento de identificação pessoal. No âmbito do serviço mID, esta entidade é também responsável por prover os mecanismos que garantem a autenticidade e integridade dos documentos digitais transmitidos tanto no *modo on-line*, quanto no *modo off-line*.

Como descrito nas secções anteriores, esta entidade comunica-se com a *aplicação mID* e com *aplicação leitora* via rede pública recorrendo a tecnologias suportadas pela arquitectura TCP/IP. Apesar de não intervir nas operações em *modo off-line*, é imperativo a garantia da disponibilidade dos serviços por ela oferecidos.

Esta componente do sistema está em fase de testes preliminares. Abaixo são listados detalhes sobre a infra-estrutura atual:

- Sistema operativo do servidor web: CentOS 7.8.2003
- Backend principal: Django v3.0
- Servidor web: UWSGI
- Base de dados principal: PostgreSQL 12.4
- Sistema operativo do serviço de gestão do sistema: Ubuntu 20.04
- Backend de gestão: Flask 1.0
- Servidor web: Gunicorn
- Base de dados de gestão: PostgreSQL 12.1 (a correr em um container Docker versão 19.03.6)

Os elementos da infra-estrutura listados acima poderão não ser suficientes para garantir todos os requisitos de segurança. Neste caso, indique possíveis novos elementos e justifique qual a sua função do ponto de vista destes requisitos ou outros que possa identificar na sua análise.