Universidade do Minho

Mestrado em Engenharia Informática

Tecnologia de Segurança

Trabalho Prático 2

1 - Instruções

- O trabalho prático deverá ser feito em grupo;
- 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 **08/04/2024.**

2 - Objetivo

Como membros da equipa de desenvolvimento de um *sistema de suporte a interoperabilidade segura de dados médicos*, vocês são responsáveis pela componente de projeto relacionada com a segurança da informação e infraestrutura. Para isso, numa primeira fase, é necessário que identifiquem todos os aspetos que representam riscos a esse 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 a análise seja detalhadamente documentada para posterior validação e orientação das demais equipas envolvidas no projeto. Além disso, procure fornecer uma avaliação sobre os aspetos 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 está restrita aos itens da lista anterior e poderá adotar uma abordagem mista, recorrendo a diferentes técnicas complementares.

3 - Descrição do sistema em desenvolvimento

O sistema em desenvolvimento tem como objetivo principal permitir a portabilidade de dados médicos entre unidades de saúde (*e.g.,* hospitais, clínicas, centros de saúde, etc) de forma segura e respeitando a privacidade do titular dos dados. O sistema é composto por cinco entidades principais, nomeadamente, *aplicação do paciente, aplicação médica, broker, base de dados da unidade de saúde* e *autoridade certificadora*.

O funcionamento básico do sistema consistem em:

- Unidades de saúde publicam no *broker* a lista de identificadores de atributos médicos dos pacientes que mantém em suas bases de dados. Note que o valor dos atributos não são partilhados com o *broker*.

- Durante uma consulta médica, o profissional de saúde usa a *aplicação médica* para estabelecer um canal seguro com a *aplicação do paciente*. Uma vez estabelecida a comunicação entre as aplicações, o profissional envia um pedido com a lista de atributos médicos aos quais pretende ter acesso.
- O titular dos dados (i.e., paciente) recebe na sua aplicação uma notificação com a lista de atributos solicitados e tem a opção de autorizar ou negar o acesso à totalidade dos dados solicitados. No primeiro caso, a *aplicação do paciente* envia para a *aplicação médica* um *token* de autorização com validade temporal e o *certificado digital* do titular dos dados.
- A *aplicação médica* envia um pedido para *broker* contendo o *token* de autorização, os *certificados digitais* do paciente e da unidade de saúde autorizada a consultar os dados.
- O broker envia o mesmo pedido acrescentado do seu próprio *certificado digital* para as unidades de saúde que possuem informações para a lista de atributos solicitados.
- As unidades de saúde que possuem os dados estabelecem um canal seguro com a unidade de saúde solicitante por onde os dados são enviados diretamente.
- A *autoridade certificadora é* responsável por todos os *certificados digitais* e controla a respetiva infraestrutura de chave pública.

4 - Descrição das entidades

Abaixo, são apresentadas algumas das características e requisitos das entidades do sistema. Note que a descrição não é exaustiva e pode estar incompleta. Assim, sempre que necessário, consulte o seu cliente (*i.e.,* professor da componente prática) para esclarecer os detalhes que julgue relevantes para a análise de segurança do sistema.

4.1 - Aplicação do paciente

Corresponde a uma aplica móvel para sistemas operativos Android e IOS. Esta aplicação armazena dados pessoais de identificação e o certificado digital do titular dos dados.

Na primeira vez que o titular usa a aplicação, esta conecta-se com a autoridade certificadora (usando comunicação TCP/IP) para o download dos seus dados e certificado digital. Para isso, o titular autentica-se ao respetivo serviço por forma a iniciar a transferência dos seus dados. Esta operação repete-se periodicamente para eventuais atualização de dados ou certificados, 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 titular. 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.

O estabelecimento da comunicação entre a aplicação do paciente e a aplicação médica é, sempre, iniciada pelo dispositivo do portador através de um *QR Code* contento toda a informação necessária para que o dispositivo com a aplicação médica 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 seguro entre os dispositivos, a comunicação é suportada por mensagens codificadas no formato JSON.

Assim como a comunicação com a autoridade certificadora, é preciso garantir que a interação entre o dispositivo do médico e o dispositivo do titular garante confidencialidade e integridade dos dados transmitidos. Um outro requisito relevante é permitir auditar as interações ocorridas com aplicações médicas, por exemplo, indicando os atributos autorizados para uma unidade de saúde em particular e quando ocorreu.

4.2 - Aplicação médica

Assim como a aplicação do paciente, a aplicação médica corresponde a uma aplicação móvel para sistemas operativos Android e IOS, ou qualquer outro dispositivo que suporte os protocolos de comunicações e operações aqui definidos. Através desta aplicação, um agente de saúde estabelece comunicação com o titular dos dados e solicita atributos necessários para o atendimento em particular.

Apesar de o processo de pedido de atributos ser controlado por essa aplicação, os dados do titular não deverão ser armazenados no respetivo dispositivo. Ou seja, os dados enviados por uma unidade de saúde deverão ser armazenados na base de dados da unidade de saúde para a qual o profissional está a

prestar o atendimento ao titular. Assim, é preciso que o pedido enviado pela aplicação médica ao broker contenha os mecanismos que permitam associá-lo com a unidade de saúde para a qual os dados serão enviados.

4.3 - Broker

Corresponde à entidade responsável por mediar o pedido de atributos entre uma unidade de saúde que solicita dados de um titular e aquelas que possuem dos respetivos dados em seus sistemas. Note que o *broker* não mantém os valores dos atributos em sua base de dados. O seu sistema mantém apenas um mapa entre grupos de atributos de um respetivo titular e as unidades de saúde que possuem os respetivos valores.

A comunicação entre o *broker* e todas as entidades com as quais interagem deve garantir confidencialidade, integridade e autenticidade das partes envolvidas. Desejavelmente, as entidades devem usar um esquema que suporte autenticação mútua.

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

- Sistema operativo do servidor: Ubuntu Server 20.04.6 LTS
- Servidor web: Apache Tomcat 10.0.27
- Base de dados: PostgreSQL 14.11
- Biblioteca de comunicação segura: OpenSSL 3.0.13
- Backend de gestão: Django 5.0.3

4.4 - Base de dados das unidade de saúde

Os sistemas internos das unidades de saúde estão fora do escopo do projeto. Assim, para que sejam integrados na solução em desenvolvimento, deverão suportar protocolos que garantem a interoperabilidade com o sistema. Nomeadamente:

- O modelo de dados usados no mecanismo de portabilidade deve seguir a norma técnica FHIR[1]
- Os dados partilhados devem usar, como base, o esquema JSON
- Assim como as demais entidades, o sistema deve suportar o uso de certificados digitais X.509

Além disso, a comunicação entre unidades de saúde deve garantir confidencialidade, integridade e autenticidade das partes envolvidas. Desejavelmente, as entidades devem usar um esquema que suporte autenticação mútua.

4.6 - Autoridade certificadora

A autoridade certificadora corresponde a uma entidade confiável externa ao sistema desenvolvido. Assim, será necessário que o processo de emissão e associação de certificados com as diferentes entidades do sistema tenha em consideração a possibilidade de mecanismos heterogéneos (*i.e.,* diferentes API, múltiplos mecanismos de autenticação). Dois aspetos da Autoridade Certificadora que podem ser relevantes são:

- A emissão de certificados usa o método *Certificate Signing Request* (CSR)
- Atualmente, a comunicação com entidades externas é feita por uma API REST
- A Autoridade Certificadora disponibiliza a lista de certificados revogados através de um serviço *Online Certificate Status Protocol* (OCSP)

4.7 - Comunicação entre entidades

Considerando a potencial heterogeneidade das tecnologias usadas para conectar as diferentes entidades do sistema, é necessário garantir que toda as comunicações garantam a confidencialidade, integridade e autenticidade das partes envolvidas.

[1] https://fhir.org/