TRABALHO PRÁTICO 2 *Tecnologias de Segurança*

TECHNICAL REPORT

Ivo Miguel Alves Ribeiro
Mestrado em Engenharia Informática
Universidade do Minho
Pg53886
pg53886@alunos.uminho.pt

Henrique Ribeiro Fernandes
Mestrado Integrado em Engenharia Informática
Universidade do Minho
A95323
a95323@alunos.uminho.pt

17 de abril de 2024

ABSTRACT

Este trabalho prático tem como objetivo principal uma análise que identifique e descreva potenciais incidentes de segurança aos quais um *sistema de suporte a interoperabilidade segura de dados médicos*, que está a ser desenvolvido, pode estar exposto quando em produção.

Para uma análise mais detalhada e documentada iremos versar-nos sobre detalhes que achamos que não foram bem documentados neste enunciado, tentando apresentar uma possível solução, bem como apresentar algumas vulnerabilidades e fraquezas dos sistemas usados nas entidades presentes.

Keywords potenciais incidentes de segurança · vulnerabilidades e fraquezas

1 Introdução

O presente relatório propõe uma abordagem abrangente na avaliação de um *sistema de suporte a interoperabilidade segura de dados médicos* que está a ser desenvolvido quanto à segurança da informação e infraestrutura. Para tal iremos separar a nossa análise em duas fases, sendo a primeira uma breve análise à descrição do sistema proposto no enunciado e, posteriormente, uma análise mais detalhada às entidades presentes no sistema, onde iremos tirar partido de técnicas como *Catalogação de fraquezas típicas, Modelação de ameaças orientado ao software* e ainda *Análise de risco*, com o objetivo final de descobrir potenciais vulnerabilidades, problemas e fraquezas aos quais as componentes do sistema podem estar expostas.

O sistema apresentado no enunciado é composto por uma *aplicação paciente* que, assim como o nome indica, é a interface do lado do paciente e que tem como objetivo permitir ao paciente autorizar o(s) atributo(s) que pretende que o médico consulte durante a sua consulta. Uma *aplicação médica* onde o médico, quando numa consulta, lista os atributos médicos aos quais pretende ter acesso, sendo essa informação transferida ao paciente por via de uma comunicação *TCP/IP*, após a autorização do paciente é estabelecida uma comunicação segura entre as unidades de saúde que detém os atributos referidos nas suas *bases de dados* e a *base de dados* da unidade de saúde onde o medico esta a exercer, todo este processo é certificado pela *autoridade certificadora*. Esta ponte entre a aplicação médica e as *base de dados das unidades de saúde* é uma outra entidade do nosso sistema chamada *broker*, que tem como objetivo mapear a informação presente nas diversas bases de dados e informar, aquando um pedido a localização dessa informação. Todo este processo é apenas autorizado quando certificado por uma outra entidade do nosso sistema, a *autoridade certificadora*.

2 Análise à descrição do sistema em desenvolvimento

Analisando atentamente a descrição do sistema, bem como o papel de cada uma das entidades que nele interagem, consideramos que existem alguns pontos neste enunciado que, ou não estão bem documentados e explícitos, ou talvez tenham sido ignorados. Porém, consideramos que é relevante alertar para a sua importância, uma vez que podem por em causa a segurança da informação, bem como a integridade e fiabilidade do sistema.

Posto isto, achamos que a descrição de como a comunicação entre a *aplicação medica - aplicação paciente - broker* é realizada pode apresentar problemas nesse aspeto. É descrito que a aplicação médica estabelece uma ligação por um canal seguro com a *aplicação paciente* e envia um pedido com uma lista de atributos médicos sobre o paciente aos quais pretende ter acesso. O paciente autoriza ou nega o acesso aos atributos listados, quais os atributos dessa lista pretende solicitar, enviando um *token* de autorização e o seu certificado digital. Esta organização levanta algumas preocupações quanto à integridade do paciente uma vez que, e apesar de ser descrito que o paciente pode personalizar a quais atributos, dos listados pelo médico, pretende efetivamente conceder o acesso e até mesmo que a *aplicação médica* não armazena qualquer tipo de informação, a verdade é que, do lado da *aplicação médica*, está presente toda a informação necessária para saber qualquer atributo sobre o paciente, uma vez que tendo acesso ao *token* de autenticação válido e ao certificado digital do mesmo, a informação sobre a lista de atributos médicos a ser acessada pode ser manipulada após a comunicação com o paciente e antes da comunicação com o *broker*, permitindo o acesso a atributos que o paciente não autorizou.

Visto isto achamos relevante tomar em consideração este fator e descrever mais detalhadamente este processo de comunicação. Para isso, referimos de seguida duas possíveis modificações ao enunciado do projeto que têm como objetivo oferecer uma maior segurança, fiabilidade e autenticidade ao paciente quando usa este serviço.

Uma possibilidade seria adicionar, em caso de autorização do acesso a uma lista de atributos, uma comunicação entre aplicação paciente e *broker*, onde os dados do cliente como *token* de autorização e certificado digital são enviados, bem como uma cópia da lista dos atributos que autorizou. Desta forma, o *broker* iria validar, através da *autoridade certificadora* os certificados tanto do médico, como da unidade de saúde onde o médico está a atuar, enviados pela *aplicação médica* como os certificados e *token* de autenticação do paciente enviados pela aplicação medica, assim como comparar a lista de atributos enviada por ambas as aplicações garantindo que não há elevação dos privilégios. Uma outra possibilidade seria a de implementar um método onde o *token* de autenticação gerado pelo paciente tivesse uma validade temporal de uma sessão e que, de alguma maneira, validasse a lista de atributos médicos autorizados pelo paciente. Assim, quando esta informação chega ao *broker* este consegue garantir que o *token* enviado corresponde à lista de atributos médicos identificados.

Como resultado de uma atenta análise, decidimos realçar um outro fator que é descrito como principal método de comunicação entre as entidades e para o qual deixamos alguns alertas. Apesar de um canal seguro ser muito melhor do que não ter nenhum tipo de cuidado na transferência destes dados, pode estar sempre presente o fator *man in the middle attack* por mais seguro que seja o canal estabelecido, e, como os dados presentes nesta comunicação são dados de algum interesse, ainda mais suscetível se torna o nosso sistema a este tipo de ataques, o que faz do canal seguro não suficiente quando falamos de dados com alguma necessidade de sigilo e importância da integridade e autenticidade. Para tal, uma ótima opção para mitigar este problema seria a do uso de encriptação ponto a ponto em conjunto com o canal seguro. Esta solução seria facilmente implementada, uma vez que temos acesso a uma autoridade certificadora e a certificados digitais que facilitam, e muito, este processo.

Por fim notamos que não é identificado como e quando é que um médico deixa de ter acesso, na sua aplicação, aos dados do paciente, sendo enunciado apenas o facto de a aplicação médica não guardar qualquer tipo de informação do paciente. Apesar de essa informação ser relevante, achamos que falta definir como deve terminar a sessão de uma consulta a um paciente. Uma possível solução para isso seria a de aproveitar o canal seguro estabelecido com a aplicação médica no inicio da mesma e implementar um método onde o encerramento desse mesmo canal culminava no descartar de todos os dados em *cache* na aplicação médica referentes à consulta em questão.

3 Análise à descrição das entidades

3.1 Aplicação do paciente

Os requisitos definidos no ponto 4.1 referente à descrição da aplicação do paciente podem levantar riscos associados à sua implementação, no caso é descrito que o paciente, na sua primeira vez de uso da aplicação, conecta-se com a autoridade certificadora usando uma comunicação *TCP/IP* para o download dos dados e certificado digital, que esta operação é repetida periodicamente para eventuais atualizações desses dados e que estas atualizações já não necessitam de recorrer a autenticação no sistema.

3.1.1 Análise de risco geral

Esta metodologia, segundo uma análise de risco, revela uma série de preocupações, uma vez que a comunicação com a *autoridade certificadora* é um dos principais fatores do nosso serviço e daí não ser de todo ideal que esta seja realizada sob protocolos de transporte de dados que não ofereçam qualquer tipo de segurança quando a integridade e autenticidade dos mesmos. Assim, a primeira sugestão seria modificar esta comunicação para uma comunicação em canal segura segundo protocolos de transporte seguros e preferencialmente associados a mecanismos de encriptação que garantissem os pontos acima discutidos. Para além disso, a autenticação do paciente deve ser feita periodicamente, preferencialmente a cada início de sessão na aplicação e essa autenticação pode, aí sim, estabelecer uma comunicação com a *autoridade certificadora*, validando assim os certificados do utilizador a cada sessão.

Além disso, está referenciado o facto de os dados serem transferidos em formato *JSON*. O formato em questão é bastante rico e ajuda na identificação e organização dos dados, daí considerarmos o formato como ideal para os mesmos, porém, para uma maior segurança do sistema, achamos que um sistema de encriptação desses mesmos dados seria uma ótima opção, vez que do lado do cliente temos o certificado e a sua chave privada não seria um método difícil de implementar. Assim, segundo esta metodologia, podemos ainda aproveitar que os dados já se encontram encriptados e garantir que uma cópia (dos dados encriptados) seja armazenada no dispositivo do portador, garantindo uma integridade e autenticidade dos mesmos sempre que desencriptados, bem como uma maior segurança quando armazenados.

3.1.2 Modelação de ameaças orientado ao software

3.1.2.1 Spoofing

Os ataques de *Spoofing* geralmente ocorrem quando os dados são falsificados para que uma entidade se faça passar com sucesso por outra, visando obter vantagens ilegítimas sobre a vítima. Nesse contexto, uma entidade maliciosa disfarça-se como uma fonte confiável para tentar obter informações confidenciais que outra entidade compartilha, acreditando serem seguras.

Fraqueza: Armazenamento das credencias do portador de forma não segura.

Ameaça: Uma das ameaças associadas a ataques de *Spoofing* existe quando uma entidade maliciosa consegue obter os dados privados de autenticação do portador da aplicação, visto estas estarem armazenadas no sistema sem estarem cifradas. Isto pode acontecer, caso a password ou o certificado digital seja armazenada em *plaintext* ou facilmente identificada descobrindo padrões. Desta forma, a entidade maliciosa consegue aceder à conta do portador, permitido que esta entidade consiga realizar operações e funcionalidades em nome do portador, ou seja, consegue-se fazer passar pelo portador e enganar as restantes entidades como o leitor e a emissora.

Forma de Mitigação: Esta ameaça pode ser provocada por dados privados de autenticação de um portador não estarem armazenadas de forma segura, mas pode ser resolvida através da implementação de mecanismos de encriptação de forma segura, onde as passwords e os certificados digitais são gerados utilizando algoritmos de PBKDFs (Password-based Key Derivation Functions) que derivam uma *hash* de uma password, utilizando uma função pseudo-aleatória, sendo essa a *hash* armazenada no sistema. Segundo o que é recomendado para o armazenamento de passwords, não se deve utilizar funções de *hash* simples, pois estas podem ser alvo de ataques de dicionário onde um atacante consegue descobrir padrões entre as passwords mais utilizadas por utilizadores e a password que pretende obter. Com a utilização de PBKDFs que a partir da password e de *salt* pseudo-aleatório derivam uma *hash* sempre diferente, isto é, passwords iguais derivam *hash's* diferentes. Assim, para se obter a password e necessário ter acesso ao valor do *salt*, acrescentando uma camada extra de segurança. Desta forma, torna-se dificil para um atacante descobrir qual a password que o portador usa para autenticação reduzindo o perigo de entidades maliciosas acederem aos dados privados do portador e conseguirem obter os mesmos diretos na aplicação que este.

Análise de Risco Esta fraqueza esta prevista ser mitigada, pois está expressa nos requisitos a necessidade de garantir mecanismos robustos de autenticação, a confidencialidade e a integridade dos seus dados e certificado. Desta forma o risco associado a esta fraqueza é baixo. Já o impacto desta fraqueza é alto visto que a informações medicas de uma pessoa São bastante sensíveis:

- RISCO: 1
- IMPACTO: 5
- CRITICIDADE: 1 + 5 = 6

Fraqueza: Falta de Autenticação para Atualizações de Dados

Ameaça: A ameaça mais iminente decorrente dessa fraqueza é o *Spoofing* de identidade. Nesse tipo de ataque, um indivíduo mal-intencionado pode falsificar informações de identificação ou aproveitar-se da falta de autenticação para se passar por outro usuário legítimo. Isso pode resultar em acessos não autorizados as contas de utilizadores.

Forma de Mitigação: Esta ameaça pode ser resolvida com novas autenticações quando há atualização de dados ou certificados.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos a necessidade de utilizar uma autenticação robusta. Desta forma o risco associado a esta fraqueza é médio-alto, já o impacto desta fraqueza é médio-alto visto que a realização de operações de acesso a dados sensıveis pode trazer grande impacto. Desta forma temos:

- RISCO: 4
- IMPACTO: 4
- CRITICIDADE: 4 + 4 = 8

3.1.2.2 Tampering

Tampering refere-se à alteração de dados em disco, em uma rede ou na memória, violando a propriedade de integridade. As vítimas comuns desse tipo de ataque incluem repositórios de dados, fluxos de dados e processos.

Fraqueza: Transferência de dados não cifrados.

Ameaças A ameaça nesse contexto é a possibilidade de que os dados transferidos entre a aplicação do paciente e aplicação medica possam ser alterados ou manipulados por terceiros não autorizados.

Forma de Mitigação Para mitigar a vulnerabilidade da transferência de dados não cifrados entre entidades do sistema, é essencial implementar medidas de segurança robustas. Isso inclui o uso de criptografia para proteger a confidencialidade das informações e a adoção de certificados digitais para autenticar as partes envolvidas. Além disso, tecnologias seguras de comunicação, como SSL/TLS, devem ser empregadas para estabelecer canais seguros. Mecanismos de validação de integridade, como hashes, garantem a integridade dos dados transmitidos.

Análise de Risco Esta fraqueza está prevista nos requisitos pelo que apresenta um risco baixo. Quanto ao seu impacto este é baixo pelo facto de poder causar problemas no funcionamento do sistema do paciente e do medico.

- RISCO: 1
- IMPACTO: 1
- CRITICIDADE: 1 + 1 = 2

3.1.2.3 Repudiation

Repúdio é o ato de recusar a autoria de algo que ocorreu, violando a propriedade de não-repúdio. As vítimas comuns desse tipo de ataque incluem processos e pessoas.

Fraqueza: O paciente negar ter realizado determinadas interações com a *aplicação médica*.

Ameaça: A ameaça é a potencial negação de autoria por parte do paciente em relação às interações realizadas com a *aplicação médica*. Isso pode levar a disputas legais, falta de confiança no sistema e dificuldades na prestação de cuidados médicos adequados, pois a integridade das transações e dos registos pode ser questionada.

Forma de Mitigação: Para mitigar essa vulnerabilidade, é essencial implementar um sistema de registo e auditoria robusto que registe todas as interações entre o paciente, a *aplicação médica* e a autoridade certificadora. Esses registos devem ser armazenados de forma segura e acessíveis para verificação posterior. Isso fornecerá evidências sólidas em caso de disputas de repúdio, ajudando a garantir a contabilidade e a transparência do sistema.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos a necessidade de utilizar uma autenticação robusta. Desta forma o risco associado a esta fraqueza é médio-alto. Já o impacto desta fraqueza é médio, visto que o não-repúdio pode trazer problemas jurídicos para as unidades de saúde. Desta forma temos:

- RISCO: 4
- IMPACTO: 2
- CRITICIDADE: 4 + 2 = 6

3.1.2.4 Information disclosure

Divulgação de Informações é o ato de compartilhar informações com uma entidade não autorizada a ter acesso a elas, violando a propriedade de confidencialidade.

Fraqueza: Transmissão de dados não cifrados.

Ameaça: Um dos principais riscos relacionados aos ataques de divulgação de informações é quando o canal de comunicação entre as partes permite que dados sejam acessados por terceiros não autorizados. Isso pode resultar no *leak* de informações sensíveis, como certificados de autenticação e dados médicos pessoais.

Forma de Mitigação: Esta ameaça pode ser causada quando os dados enviados para a aplicação médica não são cifrados pela *aplicação do paciente*, mas pode ser mitigada pelo uso de cifras robustas e algoritmos de troca de chaves. Isso permite que a *aplicação do paciente* e a entidade de destino concordem numa chave para decifrar a comunicação de forma segura. O AES-256 no modo Galois Counter e o algoritmo Elliptic Curve Diffie-Hellman (ECDH) são exemplos de cifras e algoritmos de troca de chaves que podem ser utilizados. Essas medidas garantem uma transferência segura de dados, sem comprometer a segurança da comunicação, por meio de cifras e algoritmos de geração de chaves considerados robustos e seguros.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos. Desta forma o risco associado a esta fraqueza é alto, já o impacto desta fraqueza é médio-alto visto que o *leak* de dados sensíveis nas transferências de dados médicos são bastante sensíveis. Desta forma temos:

- RISCO: 4
- IMPACTO: 4
- CRITICIDADE: 4 + 4 = 8

3.1.2.5 DoS

Negação de Serviço (DoS) envolve a absorção de recursos necessários para fornecer um serviço, violando a propriedade de disponibilidade.

Os ataques de *Denial of Service* são realizados de forma a tornar os recursos de um sistema indisponíveis para os seus utilizadores. Normalmente os alvos típicos deste tipo de ataques São servidores, pois há necessidade de estes estarem sempre disponıveis para que os utilizadores consigam aceder a informação nele contida. No caso da *aplicação do paciente*, este tipo de ataques não seria preocupante pois uma aplicação não é geralmente alvo destes ataques visto que não há necessidade da *aplicação do paciente* estar sempre disponível para obtenção de informação. Estes ataques são geralmente direcionados para entidades como o *broker*, pois há necessidade de este estar sempre disponível para comunicar com as entidades do sistema. Assim, estes ataques não são aplicados à entidade em questão.

3.1.2.6 Elevation of privilege

Elevação de Privilégio (EoP) refere-se à permissão concedida a uma entidade para realizar algo para o qual não está autorizada, violando a propriedade de autorização.

Na aplicação do paciente, a elevação de privilégio não representa uma preocupação significativa. Isto deve-se ao facto de que o sistema é projetado para garantir que os utilizadores, incluindo o próprio paciente, tenham apenas acesso aos recursos e funcionalidades para os quais estão autorizados. Como resultado, não há a possibilidade de um usuário ganhar acesso a privilégios além do que foi definido para sua conta.

3.1.3 Catalogação de fraquezas típicas:

BLE - Bluetooth Low Energy

- Ataques de Man-in-the-Middle: Utilizadores maliciosos podem intercetar comunicações entre dispositivos *BLE*, comprometendo a confidencialidade e integridade dos dados.
- Risco de DoS (Denial of Service): Assim como outros protocolos de comunicação sem fio, o *BLE* está sujeito a ataques de negação de serviço *(DoS)*, nos quais um atacante pode sobrecarregar um dispositivo *BLE* com solicitações ou tráfego malicioso, impedindo seu funcionamento normal.

NFC - Near Field Communication

- Skimming: Atacantes podem intercetar comunicações NFC para roubar informações sensíveis dos pacientes.
- Relay Attacks: Atacantes podem usar dispositivos intermediários para estender o alcance de comunicações NFC, permitindo ataques de *relay*.

Quanto à *aplicação do paciente* são estes os detalhes que achamos relevante analisa e tentamos oferecer uma solução ou indicação de uma possível modificação ao sistema, de modo a melhorar e garantir uma maior autenticidade e integridade dos dados do cliente.

3.2 Aplicação médica

3.2.1 Análise de risco geral

Como referido na primeira análise a descrição do sistema, defendemos que os dados de cliente, apesar de ser descrito que não são armazenados, não devem sequer ser passados à *aplicação médica*, de modo a garantir que alguém nesta posição possa tirar partido dos mesmo obtendo informação não autorizada pelo paciente. As técnicas de como mitigar este problema já foram referidas acima mas, de modo sucinto, ou optamos por uma conexão extra entre o cliente e o *broker* para validar a ação da *aplicação médica* de solicitar os dados as demais unidades médicas através do *broker*, ou então o *token* gerado pelo cliente conter informações acerca dos atributos que foram aceites pelo paciente para serem observadas pelo médico em questão.

3.2.2 Modelação de ameaças orientado ao software

3.2.2.1 Spoofing

Fraqueza: Falta de autenticação dos médicos.

Ameaças A ameaça neste cenário reside na possibilidade de *spoofing*, onde um indivíduo mal-intencionado pode fazer-se passar por um médico legítimo por meio da *aplicação médica*. Isso pode ocorrer devido à falta de autenticação adequada do médico e à possibilidade de falsificação de certificados de autenticidade.

Forma de Mitigação Uma abordagem eficaz de mitigação é garantir que o médico faça *login* e valide o seu certificado, bem como o certificado da unidade de saúde a cada consulta realizada por meio da *aplicação médica*. Isto adiciona uma camada adicional de segurança, pois confirma a identidade do médico e a autenticidade da unidade de saúde antes de cada consulta.

Análise de Risco Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos a necessidade de utilizar uma autenticação robusta. Desta forma o risco associado a esta fraqueza é média-alta, já o impacto desta fraqueza é média visto que o não repudio pode trazer problemas em relação aos pacientes. Desta forma temos:

- RISCO: 4
- IMPACTO: 4
- CRITICIDADE: 4 + 4 = 8

3.2.2.2 Tampering

Fraqueza: Falta de proteção na lista de pedidos do utilizador.

Ameaças: A principal ameaça associada a esse problema de *tampering* é a possibilidade de um médico, após obter o *token* do utilizador, manipular o conteúdo da lista de pedidos na *aplicação médica*. Isto pode resultar na obtenção de informações do paciente não autorizadas, comprometendo a privacidade mesmo, afetando a qualidade do atendimento médico prestado.

Forma de Mitigação: Uma abordagem eficaz para mitigar o problema da elevação de privilégio seria estabelecer um fluxo direto de comunicação entre a aplicação do paciente e o *broker*, sem a necessidade de intermediários, como a *aplicação médica*.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos. Desta forma o risco associado a esta fraqueza é média-alta, já o impacto desta fraqueza também é média-alta visto que este fraqueza ameaça dados sensíveis dos utilizadores. Desta forma temos:

- RISCO: 4
- IMPACTO: 4
- CRITICIDADE: 4 + 4 = 8

3.2.2.3 Repudiation

Fraqueza: A falta de registos de auditoria torna possível o repúdio, dificultando a responsabilização e rastreamento de ações maliciosas.

Ameaças: Sem o armazenamento de *logs* num sistema de registo de eventos, torna-se impossível auditar as operações que ocorreram entre as entidades. Como resultado, em caso de um ataque, não será possível identificar o autor, pois não haverá registos das atividades realizadas no sistema.

Forma de Mitigação: Para mitigar essa vulnerabilidade, é essencial implementar um sistema de registo e auditoria robusto que registe todas as interações da aplicação medica. Esses registos devem ser armazenados de forma segura e acessíveis para verificação posterior. Isso fornecerá evidências sólidas em caso de disputas de repúdio, ajudando a garantir a contabilidade e a transparência do sistema.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos a necessidade de utilizar uma autenticação robusta. Desta forma, o risco associado a esta fraqueza é médio-alto, já o impacto desta fraqueza é médio visto que o não repudio pode trazer problemas para as unidades de saúde. Desta forma temos:

- RISCO: 4
- IMPACTO: 2
- CRITICIDADE: 4 + 2 = 6

3.2.2.4 Information disclosure

Na *aplicação médica*, não há armazenamento de informações do titular no dispositivo do médico. A função principal da aplicação é solicitar e transmitir apenas os atributos necessários para o atendimento específico, sem reter os dados em si. Desta forma, as informações enviadas pela *aplicação médica* ao *broker* consistem apenas nos atributos requeridos, sem divulgar os detalhes completos dos dados do titular. Essa abordagem garante que não há *information disclosure*, uma vez que a aplicação médica atua apenas como uma intermediária na transmissão dos atributos necessários para a prestação de cuidados de saúde, sem armazenar ou divulgar informações pessoais do titular.

3.2.2.5 DoS

Os ataques de *Denial of Service* são realizados de forma a tornar os recursos de um sistema indisponíveis para os seus utilizadores. Normalmente os alvos típicos deste tipo de ataques são servidores, pois há necessidade de estes estarem sempre disponıveis para que os utilizadores consigam aceder a informação nele contida. No caso da *aplicação médica*, este tipo de ataques não seria preocupante pois uma aplicação não é geralmente alvo destes ataques, visto que não há necessidade da *aplicação médica* estar sempre disponível para obtenção de informação. Estes ataques são geralmente direcionados para entidades como o *broker*, pois há necessidade de este estar sempre disponível para comunicar com as entidades do sistema. Assim, estes ataques não são aplicados a entidade em questão.

3.2.2.6 Elevation of privilege

Fraqueza: Médicos acederem a informações de pacientes sem as devidas permissões.

Ameaças: A elevação de privilégio neste cenário ocorre quando um médico, após obter o *token* do utilizador, conseguir manipular o conteúdo da lista de pedidos. Isto concede acesso a informações sensíveis que ele não deveria ter, comprometendo a confidencialidade dos dados do paciente e potencialmente violando regulamentos de privacidade. .
Forma de Mitigação: Uma abordagem eficaz para mitigar o problema da elevação de privilégio seria estabelecer um fluxo direto de comunicação entre a aplicação do paciente e o *broker*, sem a necessidade de intermediários, como a *aplicação médica*.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos. Desta forma o risco associado a esta fraqueza é médio-alto, já o impacto desta fraqueza é médio-alto visto que se trata de informações sensíveis. Desta forma temos:

- RISCO: 4
- IMPACTO: 4
- CRITICIDADE: 4 + 4 = 8

Gostaríamos ainda a de evidenciar que ambas as *aplicações paciente e medico*, por serem desenvolvidas para *Andoid* e *IOS* podem apresentar as suas **fraquezas típicas**.

3.2.3 Catalogação de fraquezas típicas:

Android

- Malware e Aplicações Maliciosas: O modelo de permissões granulares do *Android* pode ser mal interpretado pelos utilizadores, levando-os a conceder permissões excessivas a aplicações maliciosas. A natureza aberta da plataforma *Android* pode resultar em maior exposição a *malware*, aplicações maliciosas e ataques de *phishing*.

IOS

- *Phishing* e Ataques de Engenharia Social: Assim como em ambiente *android* os utilizadores do *IOS* podem ser alvos de *phishing* e ataques de engenharia social, levando-os a divulgar informações pessoais ou instalar aplicações maliciosos que comprometam a aplicação medica.
- *Jailbreaking*: O processo de *jailbreaking* pode comprometer a segurança do dispositivo *iOS*, permitindo a instalação de aplicações não autorizadas e acesso ao sistema de arquivos do dispositivo.

3.3 Broker

3.3.1 Análise de risco geral

O *broker*, por ser o intermediário responsável pelo mapeamento da localização dos dados pelas diversas unidades de saúde, é uma entidade da qual necessitamos garantir a disponibilidade a tempo integral de uso do sistema, isto é, devemos garantir que, caso haja uma falha neste componente os dados nele presentes (nomeadamente o mapeamento da localização das dos dados presentes nas diversas unidades de saúde), não sejam perdidos, ou, de certa maneira, garantir que a recuperação ou remapemaneto dessa informação não seja um processo de todo demorado. Isto de modo a garantir relançar este serviço sem que haja uma falha do sistema por um período de tempo longo e indeterminado. Caso a solução de armazenar a informação sobre o mapeamento for a escolhida para mitigar o problema acima referido, devemos ter ainda especial atenção à forma como os armazenamos. Para além disso, devemos garantir que essa informação seja encriptada e esteja fora do alcance de qualquer possível atacante. Além disso, a autenticação mútua é de facto desejável pois permite garantir a identidade e autenticidade das partes envolvidas, mas a sua implementação incorreta pode levar a ataques de *Spoofing* ou falsificação de identidade, por isso um alerta para essa possibilidade.

3.3.2 Modelação de ameaças orientado ao software

3.3.2.1 Spoofing

Fraqueza: Falta de mecanismos robustos de verificação do *broker*.

Ameaça: Uma ameaça significativa associada a essa situação é o potencial comprometimento da integridade e segurança dos dados. Se um médico atacante conseguir passar-se por um *broker*, pode enviar solicitações ilícitas às unidades de saúde. Essas solicitações podem incluir acesso não autorizado a informações confidenciais do paciente ou manipulação de pedidos de atributos para benefício próprio, comprometendo a precisão e a confiabilidade das informações transmitidas. Isto não apenas viola a privacidade dos pacientes, mas também pode resultar em decisões médicas erradas ou prejudiciais.

Forma de Mitigação: Uma abordagem sugerida para mitigar esse risco seria a implementação de técnicas de autenticação mútua, como a troca de certificados digitais assinados por uma autoridade de certificação confiável. Isto desde logo garantiria que tanto o *broker* quanto as unidades de saúde se autenticassem durante o processo de comunicação, reduzindo assim a possibilidade de *spoofing* por parte de entidades maliciosas.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois nos requisitos só pede para garantir integridade entre comunicações mas não nos seus dados. Desta forma o risco associado a esta fraqueza é médio-alto. Já o impacto desta fraqueza é alto visto que informações sensíveis de pacientes podem ser reveladas.

- RISCO: 4
- IMPACTO: 5
- CRITICIDADE: 4 + 5 = 9

3.3.2.2 Tampering

Fraqueza: Modificação do mapa entre grupos de atributos

Ameaça: A ameaça principal é a manipulação indevida do mapa mantido pelo *broker*. Isto pode ocorrer quando um atacante consegue acesso não autorizado ao sistema do *broker* e altera o mapeamento entre os grupos de atributos dos titulares e das unidades de saúde correspondentes. Como resultado, o *broker* pode direcionar incorretamente os pedidos de atributos ou fornecer informações imprecisas às entidades solicitantes.

Forma de Mitigação: Para mitigar as modificações individuais no mapa de atributos mantido pelo *broker*, é crucial implementar um sistema de controle de acesso detalhado. A utilização de técnicas avançadas de criptografia para proteger os dados do mapa de atributos em repouso e em trânsito é essencial para garantir a segurança e a privacidade dos dados. Adicionalmente, devemos garantir a implementação de assinaturas digitais para cada entrada no mapa, permitindo verificar a autenticidade e integridade dos dados. Quanto à exigência de autenticação mútua entre o *broker* e as entidades, devemos garantir a identidade das partes envolvidas na troca de informações para salvaguardar o repúdio.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois nos requisitos só pede para garantir integridade entre comunicações mas não nos seus dados. Desta forma o risco associado a esta fraqueza é médio-alto, já o impacto desta fraqueza é baixo visto que o serviço fica a não funcionar apropriadamente:

- RISCO: 4
- IMPACTO: 1
- CRITICIDADE: 4 + 1 = 5

3.3.2.3 Repudiation

Fraqueza: A falta de registos de auditoria torna possível o repúdio, garantindo a responsabilidade dos autores sobre as ações por eles cometidas e o fácil rastreio de ações maliciosas.

Ameaças: Sem o armazenamento de *logs* em um sistema de registo de eventos, torna-se impossível auditar as operações que ocorreram entre as entidades. Como resultado, em caso de um ataque, não será possível identificar o autor, pois não haverá registos das atividades realizadas no sistema.

Forma de Mitigação: Para mitigar essa vulnerabilidade, é essencial implementar um sistema de registo e auditoria robusto que registe todas as interações de um *broker*. Tais registos devem ser armazenados de forma segura e acessível para verificação posterior. Isso fornecerá evidências sólidas em caso de disputas de repúdio, ajudando a garantir a confiabilidade e a transparência do sistema.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos a necessidade de utilizar uma autenticação robusta. Desta forma o risco associado a esta fraqueza é médio-alto, já o impacto desta fraqueza é médio visto que o não repúdio pode trazer problemas para as unidades de saúde. Assim, temos:

- RISCO: 4
- IMPACTO: 2
- CRITICIDADE: 4 + 2 = 6

3.3.2.4 Information disclosure

Devido à natureza do *broker*, que atua como um intermediário entre as unidades de saúde e os titulares dos dados, não há preocupação com *Information Disclosure*. Isto ocorre porque o *broker* não armazena os valores dos atributos na sua base de dados, apenas mantém um mapa que associa grupos de atributos aos respetivos titulares e unidades de saúde. Portanto, não há risco de divulgação não autorizada de informações, uma vez que o *broker* não retém os dados sensíveis dos utilizadores.

3.3.2.5 DoS

Fraqueza: Falta de controlo da quantidade de pedidos de dados.

Ameaças: Um atacante pode inundar o sistema com uma quantidade excessiva de solicitações, sobrecarregando o sistema o que o impede de atender às necessidades dos demais utilizadores. Além disso, a chegada dessas solicitações em grande quantidade pode aumentar significativamente o consumo de recursos de rede, resultando numa redução drástica no fluxo de comunicação com outras entidades e, consequentemente, diminuindo a disponibilidade do sistema.

Forma de mitigação: Limitar a quantidade de pedidos com sobre os quais o sistema está a realizar operações.

Análise de risco: Esta fraqueza não está prevista nos requisitos pelo que apresenta um risco médio-alto. Quanto ao seu impacto este é alto pelo facto de impossibilitar o funcionamento do sistema.

- RISCO: 4
- IMPACTO: 5
- CRITICIDADE: 4 + 5 = 9

3.3.2.6 Elevation of privilege

No *broker*, a elevação de privilégio não representa uma preocupação significativa. Isto deve-se ao facto de que o sistema é projetado para garantir que o sistema tenha apenas acesso aos recursos e funcionalidades para os quais estão autorizados. Como resultado, não há a possibilidade de um *broker* ganhar acesso a privilégios além do que foi definido.

3.3.3 Catalogação de fraquezas típicas:

Ubuntu Server

- Vulnerabilidades de Kernel: Vulnerabilidades no *Kernel* do *Linux* podem permitir a execução de código arbitrário ou escalonamento de privilégios.
- Falhas de Configuração: Configurações inadequadas de permissões de arquivos, *firewalls* e serviços podem levar a falhas de segurança.
- Falhas de Atualização: A não atualização resulta em não aplicar *patches* de segurança que deixam o sistema vulnerável a ataques conhecidos.

Apache Tomcat

- Injeção de Código: Vulnerabilidades como injeção de *SQL ou XSS* podem permitir a execução de código malicioso no servidor.
- Perda de Informações: Configurações inadequadas de segurança podem resultar no vazamento de informações sensíveis.
- Exposição de Diretorias: Falhas de configuração podem expor diretorias sensíveis ou arquivos de configuração.

PostgreSQL

- Injeção de SQL: Falhas de segurança que permitem a execução de instruções SQL não autorizadas.
- Acesso Não Autorizado: Falhas na autenticação ou permissões inadequadas podem permitir acesso não autorizado aos dados.
- Ataques de Negação de Serviço (DoS): A sobrecarga do servidor por ataque de entidades maliciosas pode levar à negação do serviço a utilizadores legítimos.

OpenSSL

- Vulnerabilidades de Criptografia: Vulnerabilidades na implementação de algoritmos criptográficos podem comprometer a segurança das comunicações.
- Ataques de Protocolo: Protocolos de segurança, como *TLS/SSL*, apresenta vulnerabilidades que podem ser exploradas permitindo ataques como interceção ou manipulação de dados.
- Ataques de Buffer Overflow: Falhas na validação de entradas podem resultar num corrompimento do *buffer* e execução de código arbitrário.

Django

- Vulnerabilidades de Injeção de Código: Vulnerabilidades que permitem a injeção e execução de código arbitrário no servidor.
- Falhas de Autenticação e Autorização: Erros na implementação de autenticação e autorização podem resultar em acesso não autorizado a recursos.
- Exposição de Dados Sensíveis: Configurações inadequadas podem expor dados sensíveis, como chaves de API ou dados privados como passwords.

3.4 Base de dados das unidade de saúde

Como descrito no enunciado, os sistemas internos das unidades de saúde estão fora do escopo do projeto. Contudo, deixamos apenas alguns apelos às entidades que os irão desenvolver sobre alguns problemas comuns com os protocolos descritos.

3.4.1 Análise de risco geral

Embora o protocolo de segurança *FHIR* seja um padrão robusto que promove a interoperabilidade entre sistemas de informação que segue um conjunto de padrões para troca de informações de saúde eletrónicas entre sistemas de saúde, não nos podemos esquecer que devemos sempre aliar esses padrões com outras praticas necessárias para garantir a segurança e integridade dos dados transmitidos, como por exemplo comunicações associadas a *TLS (Transport Layer Security)* bem definidas, encriptação ponto a ponto na troca de informações e ainda métodos que permitam garantir a autenticidade dos autores em comunicação.

Quando à questão de utilizar um esquema *JSON* para a partilha de dados, pode ser seguro se implementado corretamente. No entanto, é importante garantir que não haja vulnerabilidades de injeção de código (como ataques de *JSON injection*) e que a validação dos dados seja rigorosa para evitar a manipulação maliciosa. Preferencialmente esses dados devem fazer-se acompanhar de certificados digitais que garantem a sua autoria.

O uso de certificados digitais X.509 é uma prática comum para autenticação e segurança de comunicação. No entanto, a gestão inadequada dos certificados, como a não renovação periódica dos mesmo e, em casos mais extremos, a não revogação de certificados comprometidos, pode comprometer a autenticidade das partes envolvidas. Assim como no *boker*, caso seja implementado um esquema de autenticação mútua devemos ter muita atenção e garantir uma correta implementação desse esquema.

3.5 Autoridade certificadora

Assim como as bases de dados acima descritas, a autoridade certificadora também é um serviço externo, contudo, deixamos um alerta para potenciais falhas de segurança que possam surgir com a utilização das técnicas mencionadas no enunciado.

3.5.1 Análise de risco

Se o método de emissão de certificados usar *CSR (Certificate Signing Request)*, é fundamental garantir que os processos de geração, envio e armazenamento das solicitações de assinatura de certificado sejam seguros e preferencialmente associados um registo de auditoria. A proteção adequada das chaves privadas associadas aos *CSR* é crucial para evitar a emissão indevida de certificados. Se as chaves privadas forem comprometidas, um atacante pode solicitar certificados fraudulentos em nome das entidades legítimas.

A comunicação com entidades externas via *API REST* requer medidas de segurança adequadas, como autenticação robusta e registada, controlo de acesso e se possivel encriptação ponto a ponto na troca de dados. A implementação inadequada da autenticação ou autorização na *API* pode expor o sistema a ataques de usurpação de identidade *(spoofing)* ou acessos não autorizados.

Assim como referido acima quando abordamos o assunto do uso de certificados digitais X.509 uma pratica comum para garantir a validade dos mesmos é disponibilização da lista de certificados revogados através do *OCSP*. No entanto, é importante garantir que esse serviço seja protegido contra ataques de negação de serviço *(DoS)* e que os tempos de resposta sejam adequados para evitar atrasos na validação dos certificados.

3.5.2 Modelação de ameaças orientado ao software

3.5.2.1 Spoofing

Não há preocupações com *spoofing* neste contexto. A autoridade certificadora é uma entidade confiável e bem estabelecida, externa ao sistema em desenvolvimento. Ela segue métodos robustos, como o *Certificate Signing Request (CSR)*, para emitir certificados. Portanto, não há risco de falsificação de identidade ou ataques de *spoofing* na emissão ou associação de certificados.

3.5.2.2 Tampering

No contexto da autoridade certificadora, o risco de alteração ou manipulação de dados (*tampering*) é igualmente inexistente. Como a autoridade certificadora não mantém registos ou informações sensíveis no seu sistema, não há dados que possam ser alvo de alteração maliciosa.

3.5.2.3 Repudiation

Fraqueza: A falta de registos de auditoria torna possível o repúdio, dificultando a responsabilização e rastreamento de ações maliciosas.

Ameaças: Sem o armazenamento de *logs* num sistema de registo de eventos, torna-se impossível auditar as operações que ocorreram entre as entidades. Como resultado, em caso de ataque, não será possível identificar o autor, pois não haverá registos das atividades realizadas no sistema.

Forma de Mitigação: Para mitigar essa vulnerabilidade, é essencial implementar um sistema de registo e auditoria robusto que registe todas as interações da autoridade certificadora. Esses registos devem ser armazenados de forma segura e acessíveis para verificação posterior, o que fornecerá evidências sólidas em caso de disputas de repúdio, ajudando a garantir a contabilidade e a transparência do sistema.

Análise de Risco: Não está previsto no enunciado a mitigação desse problema, pois não é expressa nos requisitos a necessidade de utilizar uma autenticação robusta. Desta forma o risco associado a esta fraqueza é médio-alto, já o impacto desta fraqueza é baixo visto que os problemas de não repudio não traz problemas significativos ao sistema. Desta forma temos:

- RISCO: 4
- IMPACTO: 1
- CRITICIDADE: 4 + 1 = 5

3.5.2.4 Information disclosure

No contexto da autoridade certificadora, a divulgação não autorizada de informações é inexistente devido à natureza das suas operações. Como uma entidade confiável externa ao sistema, a autoridade certificadora não retém informações confidenciais ou sensíveis nos seus registos. Portanto, não há dados armazenados que possam ser expostos ou comprometidos. Assim, o risco de divulgação não autorizada de informações, conhecido como *Information Disclosure*, é efetivamente eliminado neste cenário.

3.5.2.5 DoS

Fraqueza: Falta de controlo da quantidade de pedidos de dados.

Ameaças: Um adversário pode inundar o sistema com uma quantidade excessiva de solicitações, sobrecarregando o sistema e impedindo-o de atender às necessidades dos demais utilizadores. Além disso, a chegada dessas solicitações em grande quantidade pode aumentar significativamente o consumo de recursos de rede, resultando numa redução drástica no fluxo de comunicação com outras entidades e, consequentemente, diminuindo a disponibilidade do sistema.

Forma de mitigação: Limitar a quantidade de pedidos com sobre os quais o sistema está a realizar operações.

Análise de risco: Esta fraqueza não está prevista nos requisitos, pelo que apresenta um risco médio-alto. Quanto ao seu impacto este é alto pelo facto de impossibilitar o funcionamento do sistema.

- RISCO: 4
- IMPACTO: 5
- CRITICIDADE: 4 + 5 = 9

3.5.2.6 Elevation of privilege

No contexto da autoridade certificadora, a elevação de privilégio (EoP) não representa uma preocupação relevante. Isto deve-se ao facto de a autoridade certificadora operar com um nível elevado de confiança e autoridade, estando fora do escopo do sistema em desenvolvimento. Como tal, não há a possibilidade de indivíduos ganharem privilégios não autorizados dentro do sistema por meio da autoridade certificadora. Assim, a elevação de privilégio não é uma ameaça significativa neste cenário.

3.6 Comunicação entre entidades

3.6.1 Análise de risco geral

Quanto à comunicação entre as entidades, não encontramos nenhum possível risco, a não ser os pontos que identificamos acima. Realçamos a sua importância, bem com uma conexão segura e sempre que possível garantir que os dados partilhados sejam encriptados e autenticados na comunicação ponto a ponto de modo a garantir a autenticidade, integridade e confidencialidade pretendida pelo sistema.

3.6.2 Modelação de ameaças orientado ao software

3.6.2.1 Spoofing

Fraqueza: Man-in-the-middle.

Ameaças: Um possível problema de "man-in-the-middle"surge quando um atacante interceta e manipula as comunicações entre as entidades do sistema. Isso pode permitir que o atacante obtenha acesso não autorizado aos dados transmitidos, altere seu conteúdo ou até mesmo injete dados maliciosos na comunicação, comprometendo assim a confidencialidade, integridade e autenticidade das informações trocadas.

Forma de Mitigação: Para mitigar o problema de "man-in-the-middle"na comunicação entre as entidades do sistema, é essencial implementar medidas de segurança robustas. Isto inclui a adoção de criptografia de ponta a ponta para proteger os dados durante a transmissão, garantindo que apenas as partes autorizadas possam ter acesso. Além disso, é importante estabelecer certificados digitais e autenticação mútua entre as entidades para verificar suas identidades e garantir a integridade da comunicação. O uso de chaves de sessão seguras e renováveis ajuda a dificultar a interceção dos dados por parte de terceiros.

Análise de Risco Esta fraqueza está prevista nos requisitos pelo que apresenta um risco baixo. Quanto ao seu impacto este é alto pelo facto de impossibilitar o funcionamento do sistema ou então a entrega de dados médicos alterados, levando a má qualidade de serviço médico para os pacientes ou o roubo de dados confidenciais.

- RISCO: 1
- IMPACTO: 6
- CRITICIDADE: 1 + 6 = 7

3.6.2.2 Tampering

Fraqueza: Transferência de dados não cifrados.

Ameaças: A ameaça neste contexto é a possibilidade de que os dados transferidos entre as entidades do sistema possam ser alterados ou manipulados por terceiros não autorizados. Isto pode levar a consequências graves, como a violação da integridade dos dados.

Forma de Mitigação: Para mitigar a vulnerabilidade da transferência de dados não cifrados entre entidades do sistema, é essencial implementar medidas de segurança robustas. Isto inclui o uso de criptografia para proteger a confidencialidade das informações e a adoção de certificados digitais para autenticar as partes envolvidas. Além disso, tecnologias seguras de comunicação, como SSL/TLS, devem ser utilizadas para estabelecer canais seguros. Ainda, mecanismos de validação de integridade, como *hash's*, garantem a integridade dos dados transmitidos.

Análise de Risco: Esta fraqueza está prevista nos requisitos pelo que apresenta um risco baixo. Quanto ao seu impacto este é alto pelo facto de impossibilitar o funcionamento do sistema ou então pela entrega de dados médicos alterados, levando a má qualidade de serviço médico para os pacientes.

- RISCO: 1
- IMPACTO: 5
- CRITICIDADE: 1 + 5 = 6

3.6.2.3 Repudiation

Fraqueza: Transferência de dados não assinados entre o portador e as entidades.

Ameaças: A principal ameaça associada aos ataques de repudiação reside na incapacidade da aplicação do portador rastrear atividades ilegais originadas a partir dele. Isto torna difícil para o recetor ou emissor identificar o autor do ataque. Como resultado, um atacante pode enviar dados maliciosos para o recetor ou emissor através do portador, sem que essas entidades tenham conhecimento de que os dados foram enviados por uma entidade maliciosa.

Forma de Mitigação: Esta ameaça pode surgir quando dados são enviados para o recetor ou emissor sem serem devidamente assinados pelo portador. No entanto, é possível mitigá-la por meio do uso de assinaturas digitais, que certificam os dados transferidos entre as entidades. As assinaturas digitais utilizam certificados digitais acessíveis pelas entidades do sistema para obter a chave pública da assinatura, permitindo assim a confirmação da identidade da entidade que enviou os dados. Este método possibilita que as entidades rastreiem tanto atividades legais quanto ilegais, identificando as respetivas entidades responsáveis por essas ações.

Análise de Risco: Esta fraqueza está prevista nos requisitos pelo que apresenta um risco baixo. Quanto ao seu impacto este é médio-alto pelo facto de impossibilitar a responsabilização por um possível ataque.

- RISCO: 1
- IMPACTO: 4
- CRITICIDADE: 1 + 4 = 5

3.6.2.4 Information disclosure

Fraqueza: Transmissão de dados não cifrados

Ameaça: Um dos principais riscos relacionados aos ataques de divulgação de informações é quando o canal de comunicação entre as partes permite que dados sejam acessados por terceiros não autorizados. Isto pode resultar na fuga de informações sensíveis, como certificados de autenticação e dados médicos de pacientes.

Forma de Mitigação: Esta ameaça pode ser causada quando os dados enviados para a *aplicação médica* ou para uma unidade de saúde não são cifrados, mas pode ser mitigada pelo uso de cifras robustas e algoritmos de troca de chaves. Isto permite que as entidades concordem numa chave para decifrar a comunicação de forma segura. O AES-256 no modo *Galois Counter* e o algoritmo *Elliptic Curve Diffie-Hellman* (ECDH) são exemplos de cifras e algoritmos de troca de chaves que podem ser utilizados. Estas medidas garantem uma transferência segura de dados, sem comprometer a segurança da comunicação, por meio de cifras e algoritmos de geração de chaves considerados robustos e seguros.

Análise de Risco: Esta fraqueza está prevista ser mitigada, pois é expressa nos requisitos. Desta forma o risco associado a esta fraqueza é baixo, já o impacto desta fraqueza é alto visto que o *leak* de dados nas transferências de dados médicos são bastante sensíveis. Desta forma temos:

- RISCO: 1
- IMPACTO: 5
- CRITICIDADE: 1 + 5 = 6

3.6.2.5 DoS

Não faz sentido considerar ataques de negação de serviço distribuído (DDoS) nesta situação, uma vez que estamos a lidar com a comunicação entre entidades do sistema, e não com uma máquina ou servidor específico que possa ser alvo desse tipo de ataque. Em vez disso, o foco deve ser na garantia da confidencialidade, integridade e autenticidade das comunicações entre as diversas partes envolvidas no sistema.

3.6.2.6 Elevation of privilege

Embora a comunicação entre as entidades do sistema deva garantir a confidencialidade, integridade e autenticidade das partes envolvidas, a elevação de privilégios não representa preocupação significativa. Isto deve-se ao facto de que as comunicações em si não são entidades, logo, não têm permissões .

4 Conclusão

Em suma, e com base numa análise a praticamente todos os detalhes deste serviço descrito no enunciado, podemos concluir que existem ainda alguns pontos que devem ser de facto revistos e trabalhados antes de o colocarmos em ambiente de produção. Como equipa de responsáveis pela componente de projeto relacionada com a segurança da informação e infraestrutura, defendemos e destacamos neste relatório os pontos críticos e importantes para a garantia de um serviço que oferece autenticidade, integridade e confiabilidade a todas as entidades envolvidas.