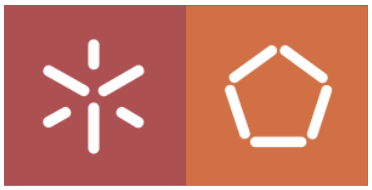


Universidade do Minho
Escola de Engenharia

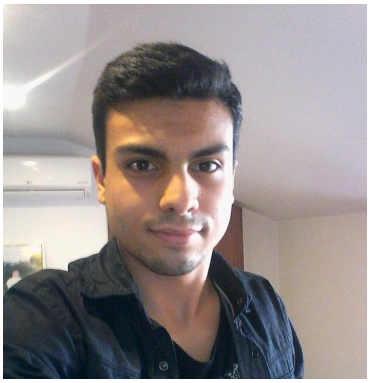
Universidade do Minho
Mestrado Integrado em Engenharia Informática

Tecnologia de Segurança

Trabalho prático 1

23 Novembro 2020

Ana Margarida Campos
(A85166)



Nuno Pereira
(PG42846)

Contents

List of Figures

Introdução

1.1 Contextualização

O presente relatório foi elaborado no âmbito do primeiro Trabalho Prático da Unidade Curricular de Tecnologia de Segurança, que se insere no 1º semestre do 4º ano do Mestrado Integrado em Engenharia Informática (1º ano MEI).

1.2 Objetivos e Trabalho Proposto

Para este trabalho foi proposto a análise de um sistema que suporta um serviço de desmaterialização de documentos de identificação pessoal. A análise consiste em enunciar aspetos que representam riscos para a segurança do sistema bem como possíveis soluções ou alterações capazes de eliminar os mesmos. Para tal é necessário recorrer a algumas técnicas estudadas nas aulas que incluem nomeadamente exploração de vulnerabilidades e *exploits*, modelação de ameaças e análise de riscos.

1.3 Estrutura do Relatório

Inicialmente é apresentada uma descrição geral do sistema em questão. Na secção seguinte, encontra-se detalhadamente descrito o modelo de ameaças onde é apresentado um *Data Flow Diagram* (DFD) do sistema em geral, a análise STRIDE das diversas entidades que o constituem e soluções para as fraquezas encontradas. Na secção seguinte é feita uma análise de risco onde são catalogadas vulnerabilidades já existentes . Por último é feita uma conclusão sobre o trabalho realizado.

Descrição Geral do Sistema

O sistema a analisar para este trabalho prático consiste num sistema que suporta um serviço de desmaterialização de documentos de identificação pessoal, ou seja, um cidadão poderá ter acesso aos seus documentos, como carta de condução, cartão de cidadão e outros, a partir do seu *smartphone*.

Neste sistema existem dois tipos de utilizadores: o portador e o verificador. O portador representa um mero cidadão que possui a aplicação com os seus dados no telemóvel. O verificador representa uma pessoa ou entidade que faz prova de identidade (por exemplo um agente da autoridade).

O estabelecimento da comunicação entre ambos é incializado através de um *QR Code* e cabe ao verificador decidir se as operações vão ser no modo *on-line* ou *off-line*. Estes dois modos diferem no sentido que no modo *off-line* o dispositivo do portador transfere os dados diretamente para o dispositivo do verificador, enquanto que, no modo *on-line* o verificador consulta diretamente a entidade emissora do documento, entidade esta que confere a autenticidade de um documento de identificação pessoal. Antes da transmissão, o portador pode aceitar a transferência da sua totalidade, ou de apenas um subconjunto dos atributos solicitados pelo verificador.

Threat Modelling

De maneira a analisar detalhadamente o sistem descrito na secção anterior e as suas particularidades descritas no enunciado do trabalho, é de seguida apresentado o modelo de ameaças do sistema (*Threat Modelling*).

O modelo de ameaças tem como principal objetivo analisar o que pode estar errado com o sistema a nível de segurança, ou seja, descobrir as possíveis vulnerabilidades e fraquezas do mesmo. De forma a incializar esta análise foi incialmente elaborado um *Data Flow Diagram* (DFD) do sistema em geral seguida da análise **STRIDE** de todas as entidades do sistema e possíveis soluções para a resolução dos problemas.

3.1 *Data Flow Diagram*

O *Data Flow Diagram* apresentado de seguida tem como entidades externas o Portador e o Verificador e como processos os dispositvos de ambos e a entidade emissora. As setas representam o fluxo dos dados.

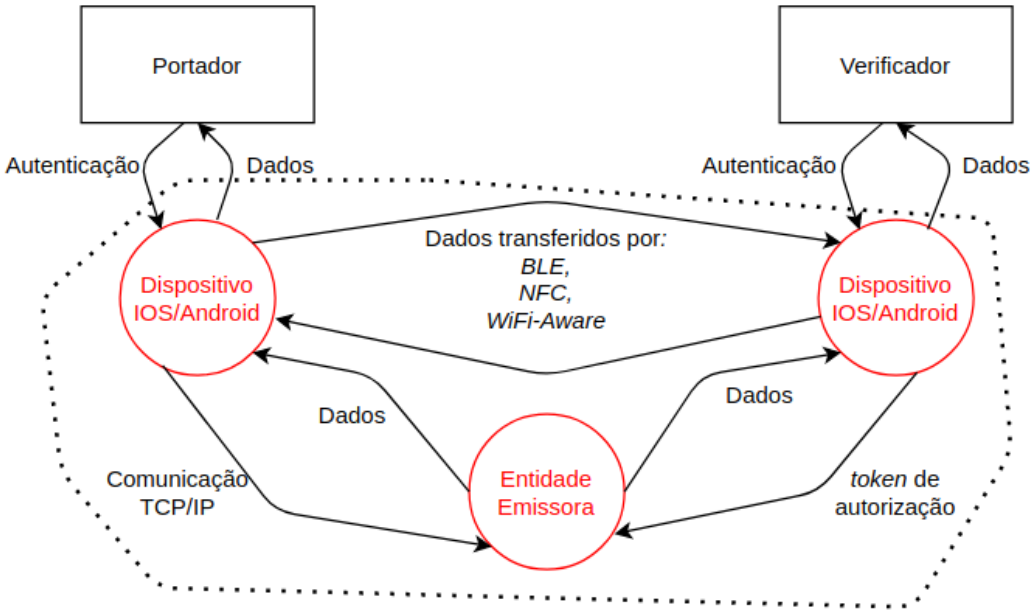


Figure 3.1: Data-Flow diagram

3.2 Análise STRIDE

A análise **STRIDE** consiste na análise de potenciais ameaças baseadas nos seguintes pontos:

- **Spoofing:** refere-se ao ato de se impersonar um utilizador roubando a sua identidade;
- **Tampering:** consiste na modificação não autorizada ou maliciosa de dados ou processos de um sistema;
- **Repudiation:** habilidade de recusar ter feito uma determinada ação ou que um certo evento ocorreu;
- **Information Disclosure:** divulgação de informações para entidades não autorizadas;
- **Denial of Service:** colocar ou sistema ou rede indisponível para os utilizadores;
- **Elevation of Privilege:** permitir que uma entidade tenha privilégios que não deveria ter.

De seguida é feita esta análise para todas as entidades do sistema.

3.2.1 Portador

Como dito anteriormente, a entidade Portador corresponde a um cidadão que possui a aplicação *mID* no seu dispositivo Android ou IOS. A análise STRIDE desta entidade centra-se nos

seguintes pontos:

Spoofing:

Um atacante pode tentar autenticar-se com os dados de um Portador através de por exemplo *brute force*.
Uma maneira de resolver esta vulnerabilidade seria através de uma autenticação correta ao sistema, ou seja, a criação de um módulo com o intuito de acrescentar uma camada de segurança. Isto pode passar por implementação de *tokens* de autorização, *cookies*, etc.

Tampering:

Um Portador com intenções maliciosas após a primeira conexão com a entidade emissora ou após atualizações do sistema, recebe os seus dados em formato *JSON*. Estes dados podem ser acedidos através de, por exemplo, *root* no telemóvel (isto permite ter acesso a todos os ficheiros do sistema). O Portador poderá manipular os ficheiros e alterar esses mesmos dados colocando dados falsos nos documentos. Se o Verificado decidir fazer a comunicação em modo *off-line*, onde os dados são transferidos diretamente para o dispositivo do leitor, ou seja, sem consultar a entidade emissora do documento, o Portador terá sucesso no seu ataque. Uma maneira de controlar este problema seria a cifragem dos dados que são transferidos para o dispositivo do Portador. Isto seria possível usando por exempo o formato *JEF - JSON Encryption Format*, onde são usados algoritmos criptográficos para a cifragem de todos os dados pertinentes. Assim, o utilizador não conseguiria perceber de que dados se tratavam nem proceder à sua alterção.

Repudiation:

Caso o Portador leve a cabo o *Tampering* descrito em cima poderá depois, quando for interrogado por um Verificador, negar que alterou os seus dados. A solução existente é a mesma que a dita no *Tampering* desta entidade, ou seja, encriptação dos dados.

Elevation of Privilege:

Se o caso de Spoofing anteriormente especificado nesta entidade for levado a cabo, então o atacante passa a ter acesso à conta do Portador onde se encontram os diversos documentos do mesmo. Isto significa que ele passa a ter acesso elevado aos dados de outra pessoa e, portanto, ocorre elevação de privilégio. A solução passa por ter um sistema de autenticação seguro.

3.2.2 Verificador

O Verificador é uma entidade externa que, como dito anteriormente, faz prova de entidade. Este possui a aplicação leitora instalada no seu dispositivo Android ou IOS. A análise STRIDE desta entidade é a seguinte:

Spoofing:

Um atacante pode tentar autenticar-se com os dados de um Verificador através de por exemplo *brute force*.
Uma maneira de resolver esta vulnerabilidade seria através de uma autenticação correta ao sistema, ou seja, a criação de um módulo com o intuito de acrescentar uma camada de segurança.

Isto pode passar por implementação de *tokens* de autorização, *cookies*, etc.

Elevation of Privilege:

Se o caso de Spoofing anteriormente especificado nesta entidade for levado a cabo, então o atacante passa a ter acesso à conta do Verificador. Isto significa que ele passa a ter acesso elevado aos dados de outra pessoa e, portanto, ocorre elevação de privilégio. A solução passa por ter um sistema de autenticação seguro.

3.2.3 Dispositivo IOS/Android

A entidade Dispositivo IOS/Android consiste no dispositivo usado por ambas as entidades externas, no entanto as duas entidades possuem aplicações diferentes: aplicação *mID* para o Portador e aplicação leitora para o Verificador. É importante destacar como são armazenados e transferidos os dados em ambas as aplicações. Na aplicação do Portador, o *download* inicial de todos os documentos associados ao cidadão é feito através do uso da comunicação TCP/IP. Esta operação também acontece para atualização de dados, neste caso, não ocorre autenticação explicita ao sistema. Estes documentos são provenientes da entidade emissora e são transferidos para o dispositivo em formato *JSON*. A comunicação entre os dispositivos do Portador e do Verificador é assegurada através de um *QR Code* e a conexão é estabelecida a partir de 3 possíveis tecnologias: *BLE - Bluetooth Low Energy, NFC - Near Field Communication e WiFi-Aware*. Toda a comunicação é suportada por mensagens no formato *CBOR - Concise Binary Object Representation*. A análise STRIDE desta entidade centra-se nos seguintes pontos:

Spoofing:

Pode ocorrer um *IP-Spoofing* quando o IP original é trocado pelo do atacante, permitindo ao mesmo obter informações sobre os documentos do Portador. Uma solução seria ter acesso a uma *IP blacklist*, onde estão registados endereços que estão envolvidos em ataques e bloquear esses mesmos endereços.

Outra forma de ocorrer spoofing pode ser através de uma vulnerabilidade do *BLE- Bluetooth Low Energy*, isto porque os *advertising packets* são sempre transmitidos por texto-limpo o que permite a um atacante impersonar o dispositivo através da clonagem dos *advertising packets* e do seu endereço MAC. Uma forma para resolver esta fraqueza seria a cifragem e posterior decifragem dos *advertising packets* através de por exemplo o algoritmo CCM-AES.

Os dispositivos móveis estão configurados para executar comandos recebidos de *NFC tags* automaticamente. Com isto, um atacante pode fazer-se passar por uma das pessoas a receber informação, comprometendo a *tag* com uma maliciosa. Uma medida para evitar esta fraqueza seria a colocação de um PIN de segurança antes da troca de informação por ambos os dispositivos.

No caso de ser utilizada a comunicação *WiFi-Aware* e caso seja executado o *tampering* indicado a baixo, um atacante facilmente efetua o spoffing podendo impersonar uma das partes envolvidas.

Repudiation

Se a comunicação entre os dispositivos for realizada a partir de *Wi-Fi Aware*, o utilizador desconhece a verdadeira identidade do atancante pelo que não o pode acusar de qualquer ação efetuada.

Tampering:

Como a comunicação entre o dispositivo do Portador e a Entidade Emissora occorre via TCP/IP, um atacante poderá intercetar esta comunicação, ler os pacotes enviados e alterar a respetiva informação.
Uma possível solução seria cifrar os dados na sua transição de maneira a que o atacante não conseguisse retirar ou modificar informações sobre os mesmos. Para tal poderia ser usado o protocolo *TLS- Transport Layer Security* que assegura a segurança da comunicação TCP/IP. Este protocolo é um protocolo criptográfico que nos dá segurança durante toda a comunicação.

A comunicação entre ambos os dispositivos (do Portador e do Verificador) pode ocorrer através de *BLE- Bluetooth Low Energy*. Um dos principais ataques ao *BLE* consiste no ataque *man-in-the-middle*. Neste ataque um dispositivo desconhecido finge ser central e periférico ao mesmo tempo e engana os outros dispositivos da rede de maneira a que se conectem a ele. Isto pode se tornar num problema grave pois o dispositivo estranho pode injetar dados falsos no fluxo, modificar os documentos do Portador e causar o mau funcionamento do sistema. Uma solução para este problema consiste no *Out of Band Pairing Method* (OOB). Este método permite que alguns pacotes de dados, como por exemplo as chaves que vão ser trocadas por ambos os dispositivos, sejam tranferidos por um meio diferente e mais seguro (por exemplo NFC dado que é mais difícil de atacar).

Se a comunicação entre ambos os dispositivos for através de *NFC - Near Field Communication*, apesar do cenário de modificação dos dados ser muito complicado pode vir a acontecer. A maneira mais comum de interferir na troca de dados e de os modificar consiste em usar *jammer RFID*, um dispositivo de radiofrequência. De forma a solucionar esta fraqueza, era necessário a implementação de algo que medisse a força das frequências de modo a escolher qual o dispositivo mais próximo e , portanto, o dispositivo correto para a comunicação.

Como dito anteriormente a comunicação entre os dispositvos é suportada por mensagens no formato CBOR. Este formato é um formato de serialização de dados binários baseado em JSON. Um atacante poderá intercetar a comunicação e modificar os dados contidos nas mensagens. Uma solução seria utilizar o CBOR mas encriptado. Para tal existe o formato COSE-*CBOR Object Signing and Encryption*. Este formato encripta os dados que são transmitidos entre os dispositivos.

A comunicação entre os dispositivos pode ocorrer através de *Wi-Fi Aware*. Um dos ataques que também pode acontecer neste tipo de comunicações é o ataque *man-in-the-midele*. Este, permite a interceção e modificação dos ficheiros transmitidos e possivelmente, transmissão de ficheiros maliciosos. Uma das formas de evitar este ataque será usar a camada de encriptação *TLS*, já que o *Wi-Fi Aware* usa o protocolo TCP/UDP

Uma vez que nas atualizações de dados não existe uma autenticação explicita ao sistema, um atacante pode intercetar a comunicação e ver dados sensíveis. Uma solução consiste em haver

sempre uma autenticação ao sistema.

Information Disclosure:

A comunicação entre o dispositivo do Portador e a Entidade Emissora ocorre via TCP/IP. Um atacante poderá intercetar esta comunicação e ler os pacotes enviados. Uma possível solução seria, como dito anteriormente, o uso do protocolo TLS- *Transport Layer Security.*

Como dito anteriormente, no *BLE- Bluetooth Low Energy* o facto dos *advertising packets* serem transmitidos por texto-limpo permitem a um atacante impersonar um dispositivo. Isto ao acontecer faz com que o atacante tenha acesso a informações do dispositivo como mensagens, calendário e outras aplicações. Uma solução seria a cifragem dos *advertising packets.*

Se a comunicação entre o Portador e o Verificador for feita a partir de *NFC*, poderá ocorrer um caso de Information Disclosure se um atacante decidir gravar a comunicação entre os dispositivos a partir de uma antena. Apesar desta comunicação ter de ser feita com os dispositivos muito próximos, não invalida que um ataque destes ocorra. O principal método para evitar este acontecimente consiste no uso de um canal seguro que utilize criptografia ou então, a troca de informação deve ocorrer longe de antenas de comunicação.

Uma vez que as mensagens transmitidas entre os dispostivos utilizam o formato CBOR, podem ser intercetadas por um atacante. Este pode fazer a descodificação do binário para JSON e retirar informações sobre as comunicações. Uma forma de evitar esta fraqueza seria utilizar o formato, já especificado anteriormente, denominado COSE.

Denial of Service:

O facto da primeira conexão do Portador com a Entidade Emissora ser por TCP/IP permite a um atacante levar a cabo um tipo de *Denail of Service* denominado de *SYN Flood attack.* Numa conexão normal, para cada pacote TCP SYN recebido é enviado como resposta um pacote TCP ACK. Num *SYN Flood attack* um atacante envia um fluxo contínuo de pacotes TCP SYN o que coloca o sistema muito sobrecarregado e sem conseguir responder a possíveis solicitações. Esta vulnerabilidade pode ser evitada recorrendo a *firewalls* que consigam distinguir pacotes normais de pacotes de *flooding*

As comunicações a partir da tecnologia *BLE* são projetadas para cada dispositivo apenas se conectar com um outro dispositivo de cada vez. Ao bombardear o dispositivo com solicitações de conexão, um atacante pode impedir que o Portador e o Verificador troquem os dados pertinentes pois estraga a conexão. Para evitar este problema é importante o uso de uma *firewall* de modo a bloquear os atacantes de prosseguirem com o ataque.

No *Wi-Fi Aware*, um ataque *DoS* é bem sucedido se o ator mal intencionado dessincronizar as sequências dos canais dos seus alvos, impedindo assim, as comunicações com outros dispositivos com a mesma tecnologia.

Elevation of Privilege:

Conforme mencionado previamente no *Information Disclosure*, se o atancante conseguir impersonar o dispositivo, fica com permissões elevadas sobre o dispositivo que está a ser atacado. Uma solução seria a pessoa que está a ser atacada verificar com quem está a fazer o emparelhamento.

3.2.4 Entidade Emissora

A Entidade Emissora corresponde à entidade que possui o poder de emitir e conferir autenticidade a um documento de identificação pessoal. É também esta entidade que garante a autenticidade e integridade dos documentos quando são transferidos. Esta conecta-se com os dispositivos das entidades externas a partir de tecnologias que suportam TCP/IP. Esta entidade suporta dois sistemas operativos, dois *backend*, dois servidores *Web* e duas bases de dados.

Spoofing:

Uma vez que são utilizadas tecnologias que suportam TCP/IP, pode ocorrer um *IP-Spoofing*. Neste caso o IP original é trocado pelo de um atacante, permitindo ao mesmo obter informações sobre os documentos. Como dito anteriormente, uma possível solução seria ter acesso a uma *IP blacklist*, onde estão registados endereços que estão envolvidos em ataques e bloquear esses mesmos endereços.

Tampering:

Como a Entidade Emissora se liga com as entidades externas a partir de TCP/IP, um atacante poderá intercetar esta comunicação, ler os pacotes enviados e alterar a respetiva informação. Uma possível solução seria cifrar os dados na sua transição de maneira a que o atacante não conseguisse retirar ou modificar informações sobre os mesmos. Para tal poderia ser usado o protocolo *TLS- Transport Layer Security.*

É sempre necessário ter cuidados no que toca a base de dados pois um atacante pode modificar os dados nela presentes. Para tal convém ter mecanismos de segurança associados tais como, por exemplo, redundância dos dados, isto é, os dados estarem disponibilizados em vários locais.

No que toca a *Backend*, é fundamental ter cuidados a nível de segurança pois um atacante pode conseguir modificar, extrair ou mesmo eliminar partes do código que sejam imprescindíveis. Um solução será recorrer a ferramentas que analisem o código à procura de anormalidades.

Repudiation:

Caso um atacante tenha acesso aos ficheiros de *logs*, pode apagar ou truncar estes ficheiros para esconder o seu ataque. Depois pode negar que o fez. Uma forma de mitigar este acontecimento é recorrer a *audit log.* Isto faz com que cada vez que exista uma mudança no sistema, esta mudança seja documentada no *audit log.*

Information Disclosure:

A comunicação ao ser feita por TCP/IP permite a um atacante intercetar a rede e ler os pacotes enviados. Uma possível solução seria, como dito anteriormente, o uso do protocolo TLS- *Transport Layer Security*.

No que toca a bases de dados, caso um atacante tenha acesso às mesmas pode retirar informações importantes. Uma maneira de prevenir isto seria através da cifragem dos dados que são considerados pertinentes (como *passwords*, documentos importantes, etc.).

Denial of Service:

O facto das conexões serem via TCP/IP permite a um atacante levar a cabo um tipo de *Denail of Service* denominado de *SYN Flood attack*. Esta vulnerabilidade pode ser evitada recorrendo a *firewalls* que consigam distinguir pacotes normais de pacotes de *flooding*

Elevation of Privilege:

Um atancante tendo acesso ao código poderá modificar os dados e executar ações em modo de administrador. Para evitar esta situação é necessário que haja mecanismos de autorização apropriados que impençam a alteração dos dados, tais como o príncipio de privilégios mínimos, por exemplo, correr o servidor como utilizador não *root*.

Análise de Risco

Uma análise de Risco consiste na verificação dos pontos críticos que possam aparecer num determinado sistema. Em termos de segurança, qualquer sistema deve respeitar as propriedades para obter uma comunicação segura. São estas:

- **Confidencialidade:** garante que apenas as pessoas com os privilégios corretos têm acesso;
- **Autenticação:** é necessário a confirmação da identidade antes de qualquer comunicação;
- **Integridade:** consiste em garantir autenticidade da informação, ou seja, que os dados se mantenham iguais, não sendo alterados;
- **Não-Repúdio:** evidências que impeçam intervenientes de negar comunicação;
- **Acesso e Disponibilidade:** serviços devem estar acessíveis e com disponibilidade para os seus utilizadores.

De maneira a que um sistema respeite estas propriedades devem ser corrigidas as vulnerabilidades apresentadas anteriormente na análise STRIDE, nomeadamente as que implicam uma falha de segurança muito grave no sistema. Conforme o estudo feito previamente e em jeito de aprofundamento, as fraquezas que já possuem histórico de serem exploradas são:

Tampering no *BLE*: Existem várias ocorrências de erros na segurança que permitiram a modificação dos dados a partir da interseção da comunicação *BLE* entre dispositivos. Falando de uma bastante grave em específico, um atancante que possui acesso físico ao cartão da *BrilliantTS FUZE* consegue desbloquear o cartão, extrair o número do cartão e modificar dados via *BLE* uma vez que não é necessária nenhuma autenticação.

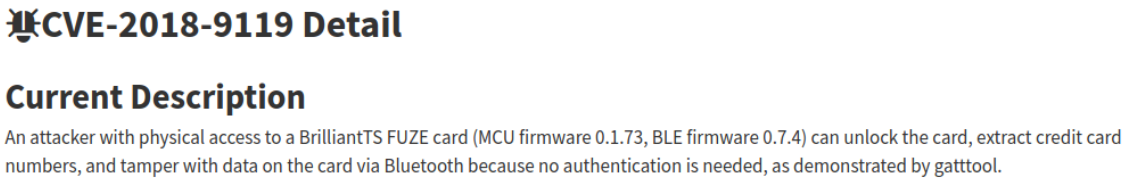


Figure 4.1: CVE-2018-9119

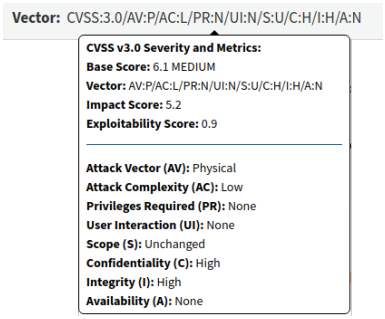


Figure 4.2: CVSS da vulnerabilidade CVE-2018-9119

Information Disclosure no *NFC*: Como é possível verificar na figura seguinte, há várias vulnerabilidades associadas à divulgação de informações a entidades não autorizadas a partir do *NFC*.

CVE-2020-0349	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139188779
CVE-2020-0348	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139188582
CVE-2020-0335	In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-122361504
CVE-2020-0334	In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147995915
CVE-2020-0326	In NFC, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-146453119
CVE-2020-0325	In NFC, there is a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145079309
CVE-2020-0319	In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137868765
CVE-2020-0300	In NFC, there is a possible out of bounds read due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148736216
CVE-2020-0282	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure. System execution privileges, a Firmware compromise, and User interaction are needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-144506224
CVE-2020-0281	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure. System execution privileges, a Firmware compromise, and User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137857778
CVE-2020-0268	In NFC, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148294643
CVE-2020-0158	In nfc_ncif_proc_t3t_polling_ntf of nfc_ncif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141547128

Figure 4.3: Information Disclosure *NFC*

Uma fraqueza em particular é o CVE-2020-0349. Este consiste na não existência de verificação do tamanho da informação. Isto pode levar a uma divulgação de informações que se encontram no armazenamento do dispositivo, neste caso, nos dispositivos com a versão *Android* 11.

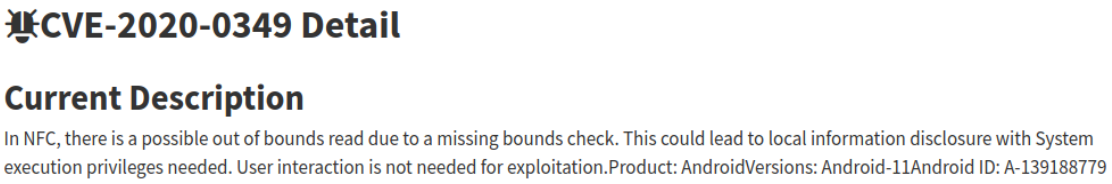


Figure 4.4: CVE-2020-0349

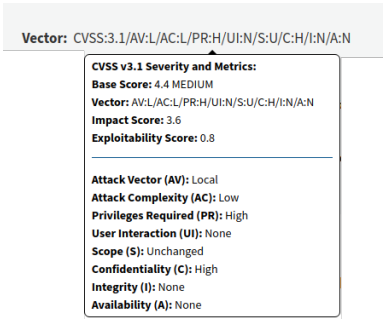


Figure 4.5: CVSS da vulnerabilidade CVE-2020-0349

Denial of Service em TCP/IP: Existem várias fraquezas associadas à colocação do protocolo TCP/IP indisponível para os utilizadores. Uma vulnerabilidade específica (CVE-2020-9464) centra-se no software não conseguir controlar adequadamente a alocação e manutenão de recursos limitados, permitindo que um atacante influencie na quantidade de recursos consumidos, levando ao esgostamento dos rescursos disponíveis.

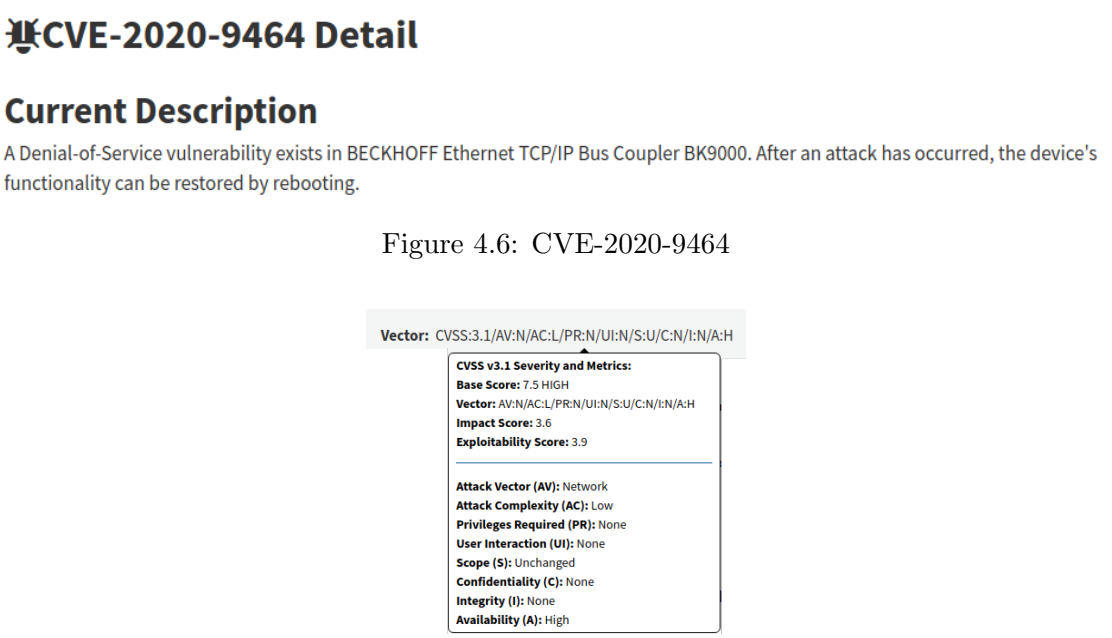


Figure 4.6: CVE-2020-9464

Figure 4.7: CVSS da vulnerabilidade CVE-2020-9464

Tampering CBOR: No caso do formato CBOR, a modificação de dados é uma vulnerabilidade existente. Num caso específico, vulnerabilidade CVE-2020-24753, existe uma falha de corrupção de memória que pode permitir a um atacante executar código via CBOR. Pode ocorrer também modificações na memória por erro não detetado ao descodificar o CBOR.

Figure 4.8: CVE-2020-24753

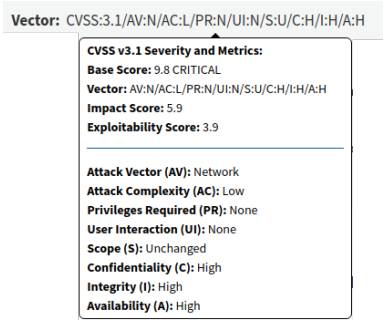


Figure 4.9: CVSS da vulnerabilidade CVE-2020-24753

Conclusão

Com a elaboração deste trabalho prático conseguimos pôr em prática conhecimentos obtidos tanto nas aulas teóricas como práticas desta unidade curricular. Permitiu-nos aprofundar conhecimentos sobre catalogação, modelação e análise de vulnerabilidades.

Em termos de dificuladades, a procura de informações relativas ao *Wi-Fi Aware* foi mais complicada uma vez que é uma API baseada AWDL.

Por último, pensamos que com a realização deste trabalho conseguimos atingir todos os objetivos que nos foram propostos.