Os perigos do Bluetooth: análise na perspetiva da Cibersegurança

F. Henriques, T. Martins
Estudantes no Mestrado em Cibersegurança e Informática Forense
Instituto Politécnico de Leiria
{2180066, 2182716}@my.ipleiria.pt

***Abstract*—After the creation of the Bluetooth technology by Jaap Haartsen and Sven Mattisson, the technology has evolved and improved to the point of gaining a vast widespread acceptance. Due to the convenient and the easy use design direction of the technology, many security problems have occurred over the years. Thus, this paper aims to show the dangers of Bluetooth by explaining and analyzing the vulnerabilities and threats on this technology. Even though many of the problems illustrated here have been solved through the different versions of Bluetooth, many of these vulnerabilities persist since devises continue to use the older versions, which are insecure.**

***Index Terms*—Ameaças; Cibersegurança; Bluetooth; Vulnerabilidades**

I. Introdução

O Bluetooth é uma tecnologia *wireless* para a troca de dados sobre pequenas distâncias, esta foi desenvolvida por Jaap Haartsen e Sven Mattison, engenheiros eletrónicos ao serviço da Ericsson em 1994. Atualmente, o Bluetooth é gerido pelo *Bluetooth Special Interest Group* no qual tem desenvolvido novas versões Bluetooth por forma a corrigir problemas de segurança e a acompanhar as necessidades das novas tecnologias. Apesar disto, problemas de segurança têm se mantido presentes, estes problemas veem na forma de vulnerabilidades, ou de falhas de implementação, e deste modo a continua existência da possibilidade de ataques. Quando descrevendo tais ataques, partem-se do suposto que o atacante está sempre dentro do campo de alcance de comunicação de um dispositivo Bluetooth. Aqui iremos explorar os vários tipos de ataques possíveis no Bluetooth, tanto devido a vulnerabilidades existentes em versões antigas, como também em versões mais recentes. É importante discutir as vulnerabilidades existentes nas várias versões do Bluetooth pois é nestas versões onde ocorrem muitos dos ataques. Isto deve-se ao facto de muitos dispositivos Bluetooth ainda utilizarem versões antigas pelo que são consideradas inseguras.

II. Bluetooth

O Bluetooth é uma tecnologia usada para comunicações *wireless* de curto alcance, esta tecnologia possibilita a partilha de dados entre computadores, dipositivos móveis, equipamentos médicos e muitos outros tipos de dispositivos da *Internet of Things* (IoT) de forma segura, robusta, baixa em energia e em custo.

O Bluetooth utiliza a tecnologia de rádio *frequency-hopping spread spectrum* que evita problemas de interferência por parte de outros dispositivos tanto de Bluetooth ou não. Este usa 79 frequências de rádio tendo início na 2402 MHz continuando depois por cada 1 MHz. É nestas frequências que o Bluetooth faz o "*hopping*" o que torna a possibilidade de interferência de outros dispositivos difícil. O Bluetooth usa uma estrutura baseada em pacotes para implementar uma arquitetura de *master-slave*, por outras palavras, a informação é transmitida através dos pacotes, e em cada rede Bluetooth (piconet) existe um dispositivo master que efetua a administração dos dispositivos (*slaves*) que estão em comunicação nessa piconet. Estes cargos de *master* e *slave* nos dispositivos podem mudar para o oposto sempre que necessário, ou até mesmo desempenhar o cargo de *master* e de *slave* ao mesmo tempo, isto é, um dispositivo é *master* numa piconet e *slave* noutra piconet. [1]

Atualmente existem dois tipos de Bluetooth, o Bluetooth clássico e o Bluetooth *Low Energy*, que é a versão Bluetooth mais focada para dispositivos com baixo poder computacional como em muitos dispositivos de IoT.

Cada dispositivo Bluetooth tem um endereço único de 48 bit que é atribuído pelo fabricante, este endereço denomina-se de BD_ADDR e é utilizado nos processos de comunicação entre dispositivos Bluetooth. Nestes processos também são utilizados várias chaves secretas para autenticação e de encriptação para assegurar confidencialidade, estas chaves são geradas de forma aleatória e são referidas como *random number* (RAND). [2]

A primeira vez que uma tentativa de comunicação é iniciada entre dois dispositivos, existe a necessidade de efetuar um processo de autenticação para estabelecer uma relação de confiança entre estes, este processo chama-se "*pairing*". Nas versões 2.1 e mais recentes é utilizado o protocolo *Secure Simple Pairing* (SSP) como processo para *pairing*, este usa a criptografia assimétrica de chave pública em vez do uso do PIN. [2]

A pilha protocolar do Bluetooth inclui uma variedade de protocolos pelo que se pode destacar: O *Logical Link Control Adaption Protocol* (L2CAP) para passar os pacotes de dados

para as camadas superiores; O *Link Management Protocol* que estabelece e controla a ligação entre dispositivos; o protocolo *Radio Frequency Communications* (RFCOMM) para fornecer comunicações serial e para gerir as comunicações ativas entre dispositivos; E por fim temos o *Service Discovery Protocol* (SDP), este oferece aos dispositivos uma forma de publicar os serviços que eles oferecem e também para encontrarem outros dispositivos. [2]

III. Segurança no Bluetooth

Para a tecnologia Bluetooth existem pelo menos um guia e uma norma essencial para assegurar a sua segurança, o NIST 800-121 *Revision* 2 e a norma IEEE 802.15.1, pelo que o guia do NIST apresenta recomendações sobre os processos a tomar na segurança do Bluetooth como a confidencialidade de informação, a autorização sobre quem controla o acesso a informação, e a autenticação e verificação do dispositivo que tenta iniciar uma comunicação. A norma IEEE 802.15.1 foca-se nos protocolos envolta da tecnologia Bluetooth.

A. *Modos de segurança*

O Bluetooth apresenta 4 modos de segurança no qual pode operar:

- Modo de segurança 1, neste modo o dispositivo é considerado como inseguro e muito das funcionalidades de segurança nunca não iniciadas, apesar deste modo não ser recomendado pelo NIST, este ainda existe nas versões Bluetooth 2.0 e posteriores para estas conseguirem interagir com versões mais antigas do Bluetooth; [3]
- Modo de segurança 2 é o modo de segurança ao nível do serviço, aqui os procedimentos de segurança podem ser iniciados antes de ser estabelecida uma ligação física e depois de estabelecida uma ligação lógico; [3]
- Modo de segurança 3, este é o modo de segurança ao nível da ligação no qual cada dispositivo Bluetooth inicia antes da ligação física ser completamente estabelecida; [3]
- Modo de segurança 4, tal como no modo de segurança 2 o 4 é também um modo de segurança ao nível do serviço, pelo que se diferencia com o uso do SSP para estabelecer a geração e troca de chaves, usando o algoritmo SHA-256 para *hashing* e o AES CCM para a encriptação. [3]

B. *Descoberta de dispositivos*

A funcionalidade de descoberta de dispositivos Bluetooth, o protocolo SDP, afeta a segurança do dispositivo. Quando um dispositivo está no modo de descoberta de dispositivos este está mais vulnerável a ataques, isto porque o atacante pode descobrir informações como o nome do dispositivo, a classe, os serviços em uso, e outras informações técnicas. Estas são os dados que os dispositivos no modo de descoberta trocam entre si (num alcance de aproximadamente 10 metros entre si) para quando ocorrer a necessidade de iniciar um estabelecimento de uma comunicação. [4] Aqui é também usado parte do BD_ADDR.

C. *Modos de confiança e Serviços de segurança*

Para além de modos de segurança, o Bluetooth apresenta dois modos de confiança: O modo *Trusted* é quando um dispositivo *trusted* estabeleceu uma relação fixa com outro dispositivo e tem acesso total a todos os serviços; e o modo *Untrusted* é quando um dispositivo *untrusted* ainda não tem estabelecida uma relação de confiança com o outro dispositivo, no qual resulta numa restrição ao acesso dos serviços no dispositivo que o dispositivo *untrusted* quer aceder. [3]
O Bluetooth apresenta três serviços de segurança.

1) *Autenticação*

A autenticação é realizada quando o dispositivo requerente tenta provar a sua identidade ao dispositivo verificador. Aqui o requerente envia um pedido ao verificador juntamente com a chave secreta de ligação, depois o requerente envia a sua BD_ADDR. O verificador responde com um número aleatório AU_RAND. Ambos os dispositivos efetuam a autenticação usando o AU_RAND, a BD_ADDR e a chave secreta de ligação. Por fim o requerente envia o valor resultado, denominado de SRES, para o verificador, pelo que este compara o valor com o seu resultado. [2]

2) *Confidencialidade*

A confidencialidade é obtida usando a função de encriptação em *stream*, E0. Aqui uma *keystream* é gerada através da chave de ligação e do BD_ADDR do dispositivo, pelo que depois combina com a mensagem não cifrada para transformar em texto cifrado. [2]

3) *Autorização*

A autorização é realizada através da pesquisa na base de dados do dispositivo por registos sobre se o dispositivo já esteve autorizado anteriormente como sendo um dispositivo *trusted*, se não encontrar o registo os dipositivos devem iniciar um processo para estabelecer uma relação de confiança. [2]

IV. Ameaças e vulnerabilidades no Bluetooth

Nesta seção serão apresentados as vulnerabilidades, os tipos de ataques, e os ataques mais comuns nos dispositivos Bluetooth.

A. *As Vulnerabilidades*

Bluetooth é uma tecnologia cujos processos de comunicação tem possibilitado várias falhas de segurança, largamente devido ao processo *pairing* de um dispositivo com outro. E mesmo depois dos dispositivos realizarem o *pairing* de forma segura, um atacante consegue obter informação suficiente para fazer um ataque de *Man-in-the-Middle* ou de personificação. Mas o maior fator nas vulnerabilidades no Bluetooth está na sua versão em uso, aqui quanto mais antiga a versão for maior será a vulnerabilidade de segurança no dispositivo. E como muitos dispositivos ainda utilização versões antigas isto implica a continua existência destas vulnerabilidades para serem exploradas por atacantes. [2] De seguida serão apresentadas algumas das vulnerabilidades mais conhecidas.

1) Versões do Bluetooth anteriores a 1.2

Nas primeiras versões do Bluetooth, as chaves de ligação são baseadas em chaves de unidades estáticas e são reutilizadas em cada *pairing*. Se as chaves forem relevadas, qualquer pessoa com intenções maliciosas poderá usar um dispositivo para escutar na ligação ou para *spoofing*. [2]

2) Versões do Bluetooth anteriores a 2.1 + EDR

Nestas versões, códigos PIN pequenos são permitidos o que são facilmente revelados com um ataque de força bruta. Não existe gestão dos códigos PIN. E o *keystream* repete-se depois de 23.3 horas de utilização, isto possibilita um atacante decifrar as mensagens transmitidas se descobrir a chave secreta usada. [2]

3) Versões 2.1 e 3.0

Nestas duas versões os dispositivos do modo de segurança 4 podem reverter para versões mais antigas de forma a comunicarem com dispositivos que não suportem o mesmo modo de segurança. É também utilizado chaves estáticas no *SSP* que pode conduzir a ataques de *Man-in-the-Middle*. [2]

4) Versões do Bluetooth anteriores a 4.0

Nas versões anteriores ao 4.0, o número de tentativas de autenticação é ilimitado, pelo que possibilita um atacante eventualmente descobrir informação sobre a chave secreta de ligação. Nestas versões, a função de cifração de *stream* E0, é considerada fraca. [2]

5) Todas as versões

Em todas as versões, se as chaves de ligação forem armazenadas indevidamente, um atacante poderá visualizar ou modificar essas chaves. O comprimento da chave de encriptação pode ser tão pequena como 1 byte. Não existe autenticação dos utilizadores, apenas existe do dispositivo e é no Bluetooth clássico. Um dispositivo pode permanecer no modo de descoberta de forma indefinida. [2] E mais recentemente, uma vulnerabilidade conhecida como CVE-2018-5383, o *firmware* do Bluetooth poderá não validar de forma suficiente os parâmetros do mecanismo de *pairing* baseada na curva elíptica Diffie-Hellman, isto pode permitir um atacante remoto a obter a chave de encriptação utilizada pelo dispositivo. [5]

B. Classificação de ataques no Bluetooth

No Bluetooth existem vários tipos de ataques, na Table 1 estão classificadas as ameaças/ataques baseados no Bluetooth. Algumas ameaças podem apresentar várias classificações, no entanto, a classificação está baseada nas suas caraterísticas pré-denominadas. [6] Alguns dos ataques ou ameaças aqui mencionados serão apresentadas na secção seguinte.

Table 1 - Tabela de classificações de ataques

Classificação	**Método e Ameaças**
Obfuscation	São usadas técnicas para esconder o ataque e prevenir a deteção. **Ameaças**: *HCIConfig* (Nome do dispositivo), *HCIConfig/BTClass* (Classe do dispositivo), *Bdaddr* (Endereço do dispositivo), *SpoofTooph*
Surveillance	A monotorização do dispositivo é feita para recolher informação. **Ameaças**: *HCIConfig* (Descoberta de dispositivo), *SdpTool* (Descoberta de serviço), *Redfang*, *Blueprinting*, *Bt Audit*, *War-Nibbling*, *Bluefish*, *BNAP BNAP/BlueProPro*, *BlueScanner*.
Range Extension	O alcance da ligação é alargado para que os ataques possam ser realizados numa maior distância. **Ameaças**: BlueSniping/Bluetooone.
Sniffing	O *sniffer* é usado para intercetar dados ao capturar o tráfego de rede. **Ameaças**: *Merlin/FT4USB* (Baseado externamente), *BlueSniff* (Baseados na frequência), *HCIDump* (Baseado no hospedeiro).
Man-In-The-Middle	Os atacantes enganam os dispositivos a pensar que eles estão ligados (*pairing*), quando na realidade estes estão ligados ao atacante. **Ameaça**: *Bthidproxy*.
Unauthorized Direct Data Access	Os dados guardados na *cloud* são diretamente acedidos devido a vulnerabilidades. **Ameaças**: *Bluesnarf/Blooover*, *BTCrack/Btpincrack*, *Car Whisperer*, *HeloMoto*, *Bluebugger*, *HID Attack*, *Btaptap*.
Denial of Service	Os serviços são interrompidos fazendo com que o dispositivo ou rede esteja indisponível para os utilizadores. **Ameaças**: *BlueSmack/Tanya*, *Blueper*, *Bluejacking/BlueSpam/Smurf*, *vCardBaster*, *Sginal Jamming*, *BlueSyn/Pingblender* (DoS multi vetore), *Battery Exhaustion*.
Malware	Software intrusivo e prejudicial é colocado no dispositivo para interromper operações, roubar dados ou extorquir o alvo para ganhar alguma coisa em troca. **Ameaças**: *BlueBag*, *Caribe*, *CommWarrior*, *Skuller*.
Fuzzer	Dados são injetados numa pilha ou num programa, este tem a habilidade de encontrar *bugs* do programa ou na pilha. **Ameaças**: *Bluetooth Stack Smasher/BluePAss*, *BlueStab*, *HCIDump Crash*, *L2CAP Header Overflow*, *Nokia N70 L2CAP Dos*, *Sonyericson Reset Display*.

C. Os ataques mais comuns no Bluetooth

1) MAC *Spoofing*

O ataque de *MAC Spoofing* é um ataque realizado antes do processo de encriptação estar estabelecido e durante a formação do *piconet* quando as chaves de ligação estão a ser geradas.

Como os dispositivos Bluetooth precisão de se autenticar, estes geram chaves de ligação para tal, com isto os atacantes podem imitar o outro utilizador. Eles têm também a habilidade de terminar as ligações ou mesmo intercetar ou modificar os dados com uso de ferramentas especiais. [4]

2) PIN Cracking

O ataque de *PIN Cracking* envolve intercetar o dispositivo durante o processo de *pairing*. Aqui um atacante usa uma ferramenta de *sniffing* de frequências para recolher o RAND e o BD_ADDR dos dispositivos alvo, depois disto o atacante testa todas as permutações do PIN com os dados recolhidos através de um algoritmo de força bruta. [4]

3) Man-in-the-Middle

O ataque de *Man-in-the-Middle* é realizado durante o processo de *pairing* dos dispositivos. O atacante começa por obstruir a ligação física ao enviar informação a cada intervalo de tempo da comunicação, podendo depois o atacante fazer-se passar pelo dispositivo legitimo, depois disto o atacante interceta toda os dados, podendo depois retransmitir esses dados, modificados ou não, para o outro dispositivo destino. [7]

4) BlueJacking

BlueJacking consiste num ataque onde o atacante envia mensagens não solicitadas para o dispositivo por forma a enganar o utilizador a usar um código de acesso, assim o atacante consegue aceder a ficheiros no dispositivo alvo. Este é um ataque que apesar de não alterar os dados, ele possibilita a existência de outros ataques no dispositivo. [4]

5) BlueSnarfing

BlueSnarfing é um ataque que consiste no acesso indevido de um dispositivo móvel e roubar qualquer informação guardada na memória desse dispositivo. Neste ataque, o atacante consegue ligar-se ao dispositivo através de uma vulnerabilidade no protocolo de transferência de ficheiros OBEX, que é um programa usado pelo Bluetooth, com isto o atacante pode efetuar o *pairing* com o dispositivo alvo. [4]

6) BlueBugging

O ataque *BlueBugging* ocorre dentro do protocolo RFCOMM, aqui as ligações físicas são realizadas via L2CAP mais uma frequência de banda base, pelo que isto possibilita emular uma ligação RS-232. Este ataque é iniciado quando o atacante se liga ao dispositivo alvo sem o conhecimento do dono, com isto o atacante ganha controlo do dispositivo ao aceder aos comandos "AT" do dispositivo, isto possibilita que o atacante execute comandos no dispositivo alvo como se ele fosse o próprio dono. A partir do momento que o atacante toma controlo do dispositivo este pode também roubar informação e aceder aos serviços e configurações do dispositivo. [4]

7) BlueBump

BlueBump é um ataque que é efetuado através de vulnerabilidades na gestão de chaves de ligação. Neste ataque, é usado a engenharia social para o atacante estabelecer contacto com o alvo de forma a forçar o alvo a se autenticar. O atacante depois mantém a ligação aberta e diz ao alvo para apagar a chave de ligação do dispositivo do atacante, pelo que o alvo não sabe que a ligação ainda permanece aberta. Depois disto o atacante gera uma nova chave de ligação, e o dispositivo do atacante consegue ganhar entrada ao dispositivo do alvo a qualquer momento sem fazer autenticação, isto se a nova chave não for removida. [8]

8) BlueDump

O ataque *BlueDump* consiste no ato de causar um dispositivo Bluetooth a efetuar um "*dump"* das suas chaves de ligação armazenadas. Neste ataque, o atacante precisa de conhecer a BD_ADDR de um conjunto de dipositivos que tenham realizado o *pairing*. O atacante imita um dos endereços destes dispositivos e ligasse a um deles. E como o atacante não tem a chave de ligação este recebe um pedido de autenticação pelo que aqui o dispositivo do atacante responde com uma "*HCI_Link_Key_Request_Negative_Reply*", que poderá causar o dispositivo do alvo a eliminar a sua chave de ligação e entrar no modo de *pairing*. [9]

9) BluePrinting

BluePrinting é um ataque que envolve a combinação de informação conhecida de um dispositivo para adquirir mais informação dele. Este ataque depende do conhecimento do endereço BD_ADDR do dispositivo alvo. [4]

10) Blueover

O ataque de *Blueover* consiste no uso de ferramentas de auditoria para determinar se um dispositivo Bluetooth está vulnerável, ou suscetível a um ataque de *BlueBugging*. [4]

11) BlueBorne

O ataque *BlueBorne* envolve o uso da falha do *buffer overflow*. Esta falha existe no processamento de respostas de configuração do cliente L2CAP que é explorada pelo atacante para tomar posse de ligações Bluetooth. Desta forma o atacante consegue controlar o conteúdo e funções embutidas no dispositivo alvo. [4]

12) Fuzzing

Num ataque *Fuzzing* o atacante tenta causar um comportamento anormal no dispositivo através do envio de pacotes de dados malformados, e de dados fora de padrão para o rádio Bluetooth do dispositivo. Se o atacante conseguir causar o comportamento desejado, este pode encontrar vulnerabilidades na pilha protocolar. [4]

13) Off-Line PIN Recovery

Este é um ataque que tenta intercetar o valor do IN_RAND, LK_RAND, AU_RAND, e o valor do sinal de resposta (SRES), este último valor é um valor usado para o processo de autenticação. Aqui o atacante usa um ataque de força bruta para obter o PIN que pode ser usado para determinar o valor correto do SRES igual ao valor SRES intercetado. [4]

14) Ataque de força bruta ao *BD_ADDR*

Este é um ataque de força bruta que consiste na procura dos últimos três bytes do BD_ADDR de um dispositivo, isto porque apenas os três primeiros bytes são públicos. [4]

15) Reflection/Relay

O ataque de *Reflection/Relay* envolve o atacante fingir que é o dispositivo recetor de uma ligação legitima. Neste ataque o objetivo é apenas de refletir a informação de um dispositivo. [4]

16) Backdoor

Ataque de *Backdoor* consiste na exploração do processo de estabelecimento de uma relação de confiança durante o *pairing*. Depois de estabelecida a relação, o atacante tem acesso aos serviços e recursos do dispositivo alvo. Este acesso e a relação que tem com o atacante não é conhecido pelo alvo porque não aparece no registo de dispositivos no qual efetuou *pairing*. Para este ataque se concretizar o BD_ADDR do dispositivo alvo deve ser conhecido e o dispositivo alvo deve ser vulnerável a este ataque. [4]

17) Denial of Service e Distributed Denail of Service

Os ataques de *DoS* e *DDoS* envolvem o atacante tentar impedir o funcionamento da rede ou reiniciar o sistema ao enviar pacotes para o sistema alvo. Estes ataques para alem de conseguirem desligar uma rede, estes podem também impedir a acessibilidade entre redes de tamanhos diferentes. Este tipo de ataque foca-se na camada física da pilha protocolar ou aquelas acima desta. [4]

18) Ataques de Worm

O ataque *Worm* é um tipo de software malicioso ou *Trojan* que é enviado de forma autónoma para dispositivos Bluetooth. Este tipo de ataque tem o objetivo de infetar um dispositivo por forma a usá-lo para se replicar e enviar para outros dispositivos de forma contínua. [4]

19) Bluesmack

Bluesmack é um ataque de ataque de *DoS* em dispositivos *Bluetooth* e é similar a ataques em dispositivos baseadas em IP. Este ataque envolve o envio de *pings* ou de pedidos L2CAP para dispositivos Bluetooth, pelo que resulta no *overflow* do buffer de entrada e assim incapacitando o dispositivo. [4]

20) MultiBlue

MultiBlue é um ataque que usa um *MultiBlue dongle* para visualizar, aceder e controlar um dispositivo Bluetooth dentro da sua área de alcance. [4]

21) Bluecasing/War Nibbling

Bluecasing é um ataque que explora as vulnerabilidades em telefones Bluetooth para conseguir acesso nestes. Aqui o atacante tem recurso a um computador ou portátil com uma antena de alta frequência mais um software especializado para descobrir e usar as vulnerabilidades para efetuar a o ataque. [4]

V. Conclusão

O Bluetooth é uma tecnologia com mais de 15 anos de existência, e é cada vez mais utilizada no mundo dos dispositivos IoT por ser uma tecnologia acessível e conveniente. Por este motivo, a utilização do Bluetooth no future irá aumentar pelo que prolongará o seu tempo de vida por muitos anos. No entanto, com os vários perigos de segurança presentes nas várias versões do Bluetooth, é importante que estas sejam expostas ao utilizadores de forma a conhecerem os riscos de segurança ao utilizar dispositivos Bluetooth em versões antigas. Este é certamente o maior problema com tecnologia Bluetooth, o facto de versões antigas de Bluetooth continuarem a serem utilizadas, e até mesmo nas versões mais recentes poder existir a possibilidade em reverter para uma versão anterior por forma a estabelecer uma ligação com um dispositivo de versão inferior. Estes são certamente os maiores fatores que possibilitam a continua existência de ameaças sobre a segurança dos dispositivos Bluetooth quaisquer que sejam as suas versões.

Referências

[1] G. Roth, “Bluetooth Wireless Technology,” 2013 Maio 22. [Online]. Available: http://large.stanford.edu/courses/2012/ph250/roth1/.

[2] J. C. T. H. Peter Cope, “An Investigation of Bluetooth Security Vulnerabilities,” em *IEEE CCWC 2017*, 2017.

[3] National Institute of Standards and Technology, “NIST Special Publication 800-121 Revision 2 - Guide to BluetoothSecurity,” NIST, 2017.

[4] P. C. J. C. B. J. M. Angela M. Lonzetta, “Security Vulnerabilities in Bluetooth Technology as Used in IoT,” *Sensor and Actuator Networks*, 2018.

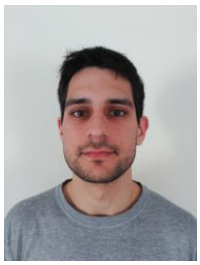
[5] Carnegie Mellon University, “Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange,” [Online]. Available: https://www.kb.cert.org/vuls/id/304725/. [Acedido em 2 12 2018].

[6] J. P. Dunning, “Bluetooth Threat Taxonomy,” [Online]. Available: https://vtechworks.lib.vt.edu/bitstream/handle/10919/76883/etd-10242010-163002_Dunning_JP_T_2010.pdf?sequence%20=1&isAllowed=y). [Acedido em 2018 11 21].

[7] L. R. K.Saravanan, “A Novel Bluetooth Man-In-The-Middle Attack Based On SSP using OOB Association model,” [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1203/1203.4649.pdf. [Acedido em 22 11 2018].

[8] Trifinite, “BlueBump,” [Online]. Available: https://trifinite.org/trifinite_stuff_bluebump.html. [Acedido em 23 11 2018].

[9] Trifinite, “BlueDump,” [Online]. Available: https://trifinite.org/trifinite_stuff_bluedump.html. [Acedido em 23 11 2018].



F. Henriques nasceu em Caldas da Rainha, Leiria, Portugal em 1992. Ele recebeu certificado em Construção e Administração de Websites em 2015 no Instituto Politécnico de Leiria e licenciou-se em Engenharia Informática em 2018 também no Instituto Politécnico de Leiria, Portugal. Ele está correntemente a tirar um mestrado em Cibersegurança e Informática Forense no Instituto Politécnico de Leiria, Portugal.

T. Martins nasceu em Leiria, Leiria, Portugal em 1995. Ele recebeu certificado em Construção e Administração de Websites em 2015 no Instituto Politécnico de Leiria e licenciou-se em Engenharia Informática em 2018 também no Instituto Politécnico de Leiria, Portugal. Ele está correntemente a tirar um mestrado em Cibersegurança e Informática Forense no Instituto Politécnico de Leiria, Portugal.