Project Report

Cybersecurity & Next Generation Technologies and Services

Master in Computer Engineering Mobile Computing

WPA3 Wi-Fi Security Analysis

Filipe Henriques, 2180066

Tiago Martins, 2182716

Leiria, janeiro de 2019

Resumo

Hoje em dia, o Wi-Fi é cada vez mais uma das redes wireless mais utilizadas para vários ambientes, tal como ambientes empresariais, públicos e pessoais. A segurança nestas redes torna-se num assunto preocupante sendo que nestas circulam pelo ar vários dados e informações sensíveis e privadas. Desta forma foi desenvolvido um protocolo para garantir a segurança a estas redes, o WEP. No entanto este protocolo apresentou vários problemas de segurança. Só depois deste protocolo é que surge o WPA, é com este protocolo que foi possível estabelecer um nível aceitável de segurança. A Wi-Fi Alliance em com sucesso do WPA, tem continuado com a base do WPA para desenvolver novas versões (WPA2), sempre com diferentes funcionalidades à medida para responder às novas necessidades na segurança das redes Wi-Fi.

Mais recentemente, a Wi-Fi Alliance introduziu a nova versão do WPA, o WPA3, este surge com os objetivos de aumentar a segurança na rede contra ataques mais recentes, mais concretamente o ataque KRACK, e simplificar a forma como é reforçada a segurança nas redes Wi-Fi tanto em ambientes pessoais como empresariais. O WPA3 alcança estes objetivos especialmente com introdução do novo *handshake*, *dragonfly handshake*. Este *handshake* resolve de forma eficiente os problemas contra os ataques de dicionário *offline*, e especialmente o ataque KRACK que se focava no funcionamento do protocolo em si. O *dragonfly* simplifica a segurança da rede pessoal ao possibilitar com que as passwords usadas pelos clientes deixem de ser tão complexas para atingir um nível de segurança semelhante.

O que se pode constatar com o WPA3 é que apesar do novo *handshake* se verificar ser uma boa alternativa ao anterior, os requisitos do certificado parecem ser poucos quando este poderia ter sido uma boa oportunidade para aplicar as novas inovações na segurança do Wi-Fi introduzidas juntamente com o WPA3.

Abstract

Nowadays, Wi-Fi is being more and more used as the main wireless technology in many applications, such as business, public or personal environments. Security is a concerning issue since a lot of personal, private or even confidential information travels through air, a medium that facilitates eavesdropping.

To ensure information security, a security protocol was developed, WEP. However, this protocol has shown a lot of problems over the years and so a new protocol was developed, WPA. WPA addressed most of WEP's problems while still maintaining compatibility with most WEP based devices. Over the years a new version of WPA was developed WPA2, which introduced new functionalities.

Recently the Wi-Fi Alliance introduced a new version, WPA3. This new version was developed to combat the new attack directed to previous WPA versions, KRACK. In order to combat this attack, the authentication mechanism that was implemented in previous versions had to be changed, thus introducing the dragonfly handshake. This handshake eliminates threats such as offline dictionary attacks and KRACK.

This new handshake proves to be a good alternative to the previous one making a compelling point of WPA3, however the requirements to obtain a WPA3 certification are very little in which an opportunity to bring innovation with the new protocol was lost.

Lista de figuras

Lista de acrónimos

AES – *Advanced Encryption Standard*

AP – *Access Point*

ASCII – *America Standard Code for Information Interchange*

CBC-MAC – *Cipher Block Chaining - Message Authentication Code*

CCMP – *Counter Mode CBC-MAC Protocol*

CRC – *Cyclic Redundancy Check*

CTR – *Counter Mode*

ECC – *Ecliptic Curve Cryptography*

FFC – *Finite Field Cryptography*

GTK – *Group Transient Key*

ICV – *Integrity Check Value*

IETF – *Internet Engineering Task Force*

IV – *Initialization Vector*

KCK – *Key Confirmation Keys*

KEK – *Key Encryption Keys*

KRACK – *Key Reinstallation Attacks*

MAC – *Media Access Control*

MIC – *Message Integrity Code*

NIST – *National Institute of Standards and Technology*

PMF – *Protected Management Frames*

PMK – *Pairwise Master Key*

PSK – *Pre-Shared Key*

RFC – *Request For Comments*

RSA – Rivest Shamir Adleman

SAE – *Simultaneous Authentication of Equals*

SSID – *Service Set Identifier*

TK – *Temporal Keys*

TKIP – *Temporal Key Integrity Protocol*

WEP – *Wired Equivalent Privacy*

WPA – Wi-Fi *Protected Access*

XOR – *Exclusive* OR

Tabela de conteúdos

Introdução

No âmbito da unidade curricular de Projeto de Segurança 1, do curso de Mestrado Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi elaborado o presente relatório de modo a elaborar uma análise de crítica do novo protocolo de segurança Wi-Fi, WPA3.

Segurança informática tem sido um tópico nas organizações no qual se deveria prestar maior importância, apesar disto as organizações responsáveis por certas tecnologias ou certificados na área da segurança, tentam assegurar ao máximo a segurança nas suas tecnologias, como a segurança no Wi-Fi pela Wi-Fi Alliance e entre outros. Depois dos problemas encontrados dentro do protocolo WPA2, mais especificamente o ataque KRACK, a Wi-Fi Alliance lançou pouco tempo depois o WPA3. Considerando os acontecimentos aqui referidos, este relatório visa a analisar o protocolo WPA3 em termos das suas diferenças perante o seu antecessor e identificar as possíveis vulnerabilidades e problemas na segurança das comunicações Wi-Fi.

O presente relatório está dividido em três capítulos, sendo que o primeiro consiste no estado da arte da segurança na Wi-Fi, aqui são abordados as várias formas de segurança no Wi-Fi utilizadas ao longo dos anos até ao lançamento do WPA2.

O segundo capítulo é composto pela a análise em si do WPA3, aqui são expostas as novas caraterísticas de segurança estabelecidas no WPA3, a forma de funcionamento do WPA3, e as vulnerabilidades e possíveis soluções nesta nova versão do WPA.

E por fim, no terceiro capítulo o relatório termina na conclusão, em que é feito um balanço geral da análise crítica na segurança garantida pelo estado atual do WPA3.

1. Estado da Arte

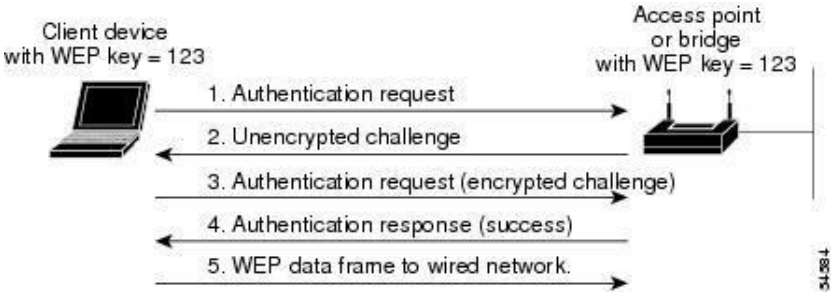
Uma vez que a temática do presente trabalho se prende com o protocolo de segurança Wi-Fi WPA3, neste capítulo, pareceu relevante tratar dos protocolos antecessores a este.

1.1. Pré-WPA

No início as redes Wi-Fi não possuíam qualquer tipo de autenticação ou segurança. O cliente apenas efetuava um pedido de ligação e o AP aceitava. Todo o tráfego entre o cliente e o servidor encontra-se em texto (*clear text*) e pode ser visualizado sem grandes dificuldades por qualquer pessoa que faça captura de pacotes. Com o crescimento das redes *wireless* e a popularização do Wi-Fi, houve a necessidade de acrescentar segurança para que houvesse confidencialidade da informação que era transmitida.

O WEP é um protocolo de segurança para redes wireless de especificação IEEE 802.11. Este protocolo foi estabelecido em 1997 com o intuito de criar confidencialidade na informação transmitida entre o cliente e o ponto de acesso. Dentro do WEP existem duas formas de autenticação, o *Open System Authentication* (ou *Open Key Autentication*) e o *Shared Key Autentication*. [1]

No *Shared Key Authentication*, o cliente efetua um pedido de autenticação e o AP envia um desafio ao cliente, tal como é visível na Figura 1. Este desafio é enviado em aberto (*clear text*) e o cliente tem que utilizar a chave partilhada para encriptar o texto (utilizando a encriptação WEP explicada mais à frente). O texto cifrado é enviado para o AP. O texto é decifrado e, se este coincidir com o texto original, o cliente é autenticado. [1]

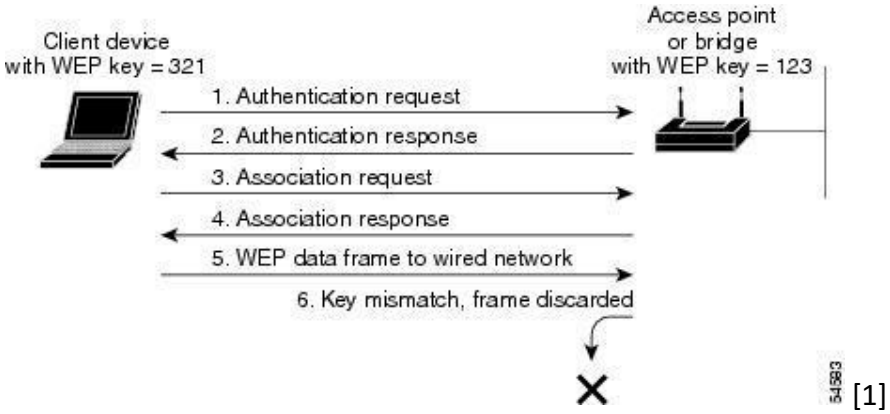


[1]

Figura 1 - WEP handshake

No *Open System Authentication*, tal como num AP sem segurança, o cliente faz um pedido de autenticação e o AP aceita o pedido e associa o dispositivo. Não é feita uma verificação da chave durante o processo de autenticação, isto é, ao conectar ao AP, indica-

se uma chave WEP e o AP vai associar o dispositivo independentemente de esta estar correta ou não. No entanto, quando o cliente tentar enviar pacotes, caso a chave seja errada, estes vão ser descartados pelo AP. [1]

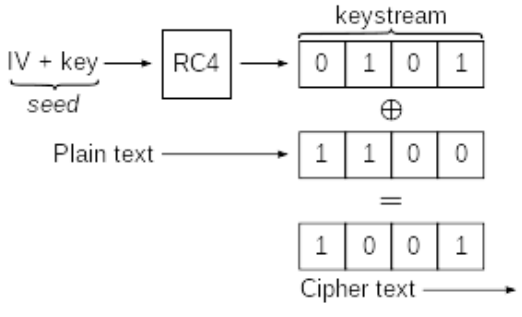


[1]

Figura 2 - WEP Open System Authentication

Inicialmente as chaves consistiam em 10 dígitos hexadecimais ou 5 ASCII correspondente a 40 bits (WEP-40) concatenados a um vetor de inicialização (IV) de 24 bits (64 bits) que era passado ao algoritmo de cifragem, mas mais tarde foi estendido para 26 dígitos hexadecimais ou 13 ASCII, (IV 24 bits + 104 bits WEP-104, 128 bits). [2]

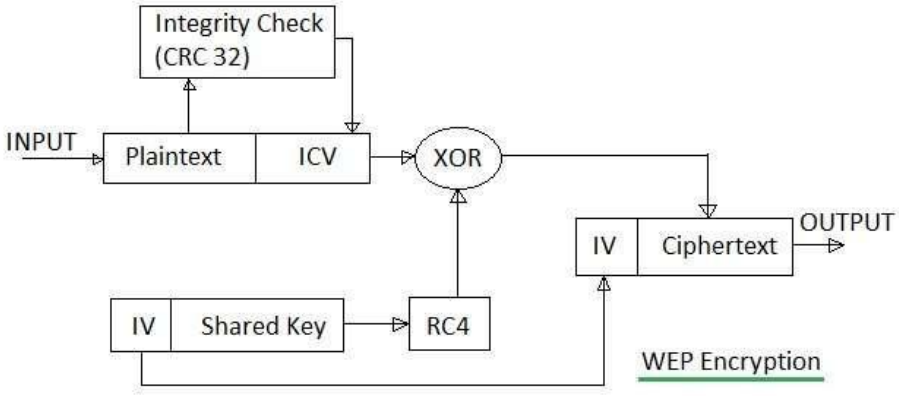
Como a chave partilhada (WEP-40/WEP-104) é sempre igual, o IV tem o propósito de criar pseudoaleatoriedade para ser empregue no algoritmo de cifragem RC4. Este algoritmo cria um *stream* de bits que é utilizado numa operação XOR (eXclusive OR) com o texto a cifrar, que dá origem ao texto cifrado. [2] Este processo está representado na imagem Figura 3.



[3]

Figura 3 - Funcionamento do algoritmo RC4

O texto que é cifrado contém ainda um ICV, de modo a assegurar a integridade dos dados. Após a passagem pelo RC4, o texto + ICV cifrados são agregados ao IV utilizado no RC4, e são então enviados para o cliente. Na Figura 4 é possível observar uma representação completa dos processos anteriores.



[4]

Figura 4 - Processo completo da encriptação na WEP

Em 2001 foi publicado um estudo de criptoanálise ao algoritmo de cifragem RC4, e foi revelado que existiam vários problemas de segurança na forma como este era implementado no protocolo WEP, mais nomeadamente na utilização de IV fracos. Os IVs utilizados no WEP, têm 24 bits, 2^24, que corresponde a 16777216 combinações diferentes. Em termos computacionais, é considerado um número pequeno, mesmo em hardware da época. [2]

Com o número de pacotes normalmente enviados numa rede wireless, a chave utilizada no RC4 acabaria por ser repetida. O CRC 32, o algoritmo responsável pela integridade da mensagem no WEP, é um algoritmo bastante linear, pelo que é vulnerável à alteração da mensagem enquanto mantendo o mesmo valor de hash. Em 2005, com a ajuda de ferramentas criadas com base no estudo criptográfico mencionado, o poder computacional era suficiente para quebrar uma chave WEP em 3 minutos. [5]

O WEP continha uma vasta lista de problemas:

1. No *shared key authentication*, o *challenge* é enviado em *cleartext* e recebido encriptado, pelo que é fácil de executar um ataque de força bruta à *password*;
2. Utilização da chave partilhada no processo de encriptação ao invés de utilizar chaves de sessão;
3. Chave partilhada apenas é concatenada com o IV;
4. O algoritmo de integridade dos dados não é confiável;
5. Utilização de IVs curtos e consequente repetição dos mesmos;
6. Vulnerável a ataques do tipo *Message-Replay*. [6]

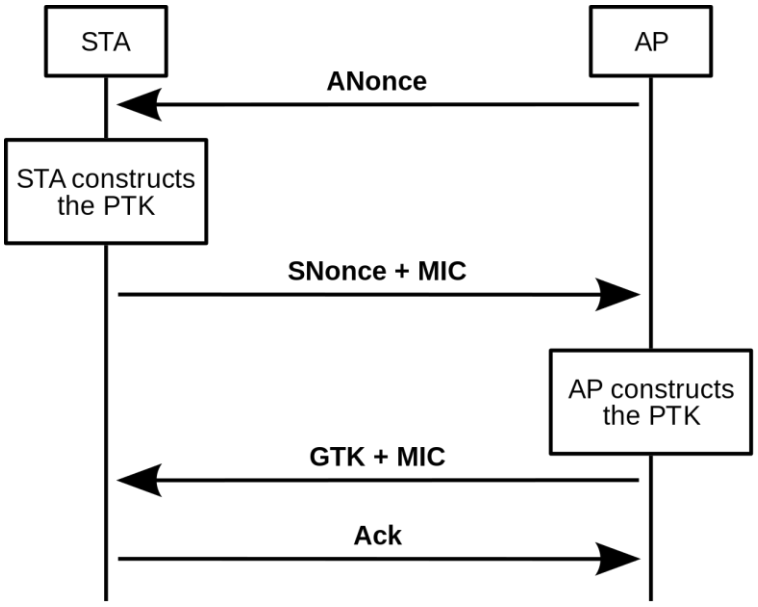
1.2. WPA

O WPA foi um protocolo intermediário estabelecido em 2003 pela Wi-Fi Alliance com o objetivo de corrigir a maior parte dos problemas que o protocolo WEP trazia, mas mantendo a compatibilidade com hardware de especificação IEEE 802.11, com o intuito de tornar as redes wireless já existentes mais seguras. Este protocolo é baseado na retificação à especificação IEEE 802.11, a 802.11i que veio mais tarde a ser integrada na especificação em 2007. [6]

A retificação 802.11i integra várias soluções aos problemas da WEP, tais como:

- Introdução de um novo processo de autenticação, o *4-Way Handshake* e o *Group Key Handshake*
- Melhorias no processo de encriptação e integridade, com o TKIP e o CCMP

Uma das principais alterações foi o processo de autenticação que é completamente diferente do *challenge* enviado pelo WEP. O novo processo de autenticação, chamado de *4-Way Handshake*, é composto por 4 passos. Neste processo é introduzido o conceito de PMK (*Pairwise-Master-Key*), que em WPA-PSK são gerados a partir da PSK (*shared key*), SSID e tamanho do SSID. Apesar de tanto o cliente como o AP conhecerem a PMK, esta nunca é trocada. Após o cliente se ligar ao AP, o AP vai enviar ao cliente um ANonce (Authenticator Number Once), que é um número de autenticação gerado aleatoriamente e apenas utilizado uma vez. Depois do Cliente receber este ANonce o cliente (também conhecido como *supplicant*), tem todos os elementos necessários para derivar a chave PTK (Pairwise-Transient-Key), uma chave de sessão de 512 bits. Esta chave é gerada a partir do ANonce, SNonce, MAC do AP, MAC do cliente e PMK. Com esta chave gerada, vai enviar um SNonce juntamente com um MIC que foi gerado com a PTK. O AP recebe estes dados e gera também a PTK. Com o MIC enviado, o AP pode verificar se a chave gerada é correta ou se houve alguma alteração feita por terceiros na mensagem. O AP gera também uma GTK, se necessário, e envia-a juntamente com um MIC ao cliente. Por fim, o cliente envia um ACK e o processo de autenticação dá-se por concluído. Na Figura 5 é possível observar-se com maior detalhe o processo previamente descrito. [7]

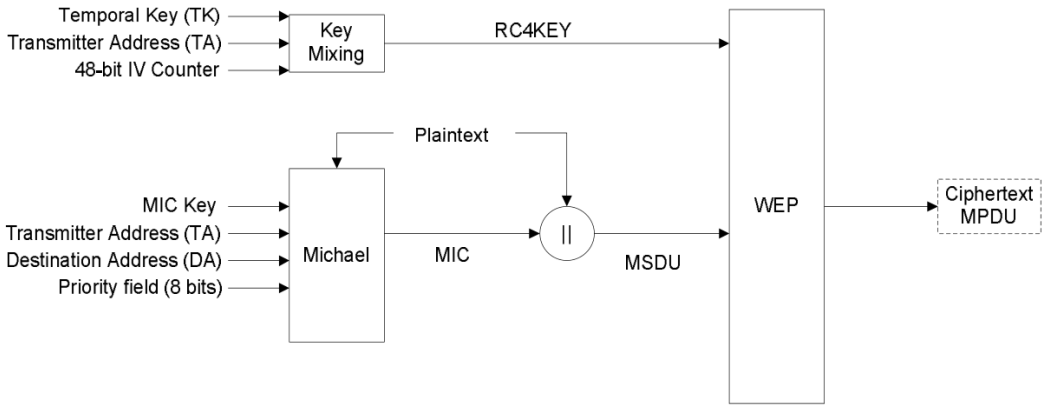


[8]

Figura 5 - 4-way handshake

Através da PTK são derivadas várias chaves tais como TK, MIC keys, KEK e KCK.

O WPA traz o TKIP (*Temporal Key Integrity Protocol*), um novo protocolo de encriptação. O TKIP foi introduzido para manter retrocompatibilidade com equipamentos que originalmente funcionavam com WEP. Enquanto que na encriptação do WEP, apenas era concatenada uma chave única com o vetor de inicialização e depois passado ao algoritmo RC4, no WPA a chave é misturada com o IV (agora chamado de TSC, *TKIP Sequence Counter*) em duas fases diferentes, antes de ser passado ao RC4. O TKIP implementa também um MIC de 64 bits de modo a assegurar a integridade da mensagem, este é muito menos linear do que o CRC-32. [9]



[6]

Figura 6 - Esquema do TKIP

O TSC consiste num IV de 48 bits que também é utilizado para numeração de pacotes, isto dificulta a execução de ataques de *Message-Replay*. A Figura 6 esquematiza o TKIP. Com IVs maiores e sem se conhecer especificamente a "chave WEP", o TKIP parecia fazer uma boa implementação do algoritmo de cifragem RC4, no entanto mais tarde chegou-se à conclusão que o TKIP também não era suficientemente forte. [6]

1.3. WPA2

O WPA2 é uma melhoria do WPA, sendo que este mantém o mesmo processo de autenticação, o *4-Way-Handshake*, e mantém também o protocolo TKIP de modo a garantir retrocompatibilidade, no entanto traz um novo protocolo de encriptação, o CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*), que é baseado no AES (*Advanced Encryption Standard*). O protocolo de encriptação normalmente utilizado no WPA2 é o CCMP, não sendo aconselhada a utilização do TKIP. Existem dois modos de utilização do AES no CCMP, o CTR (*Counter-Mode*), que garante a privacidade e confidencialidade dos dados ao encriptar a *frame*, e o CBC-MAC (*Cipher Block Chaining - Message Authentication Code*), que garante a integridade dos dados. Este protocolo é muito mais forte que o TKIP, e é o protocolo criptográfico utilizado no WPA3. [6]

Em 2009 com a introdução da revisão 802.11w, uma das novidades era o PMF (*Protected Managed Frames*). Visto que o Wi-Fi opera num meio que qualquer pessoa pode escutar, houve necessidade de proteger os *management frames* que eram enviados em aberto como o caso dos de de-autenticação e desassociação, entre outros, sendo que os de de-autenticação e desassociação podiam ser utilizados para fazer ataques de negação de serviço, no entanto esta nova funcionalidade não era necessária para se obter certificação WPA2. O KRACK (*Key Reinstallation AttaCK*) foi publicado publicamente em outubro de 2017. Este ataque explorava uma falha na implementação do *4-Way-Handshake* onde era possível proceder-se à reinstalação de chaves PTK e GTK, o que levava ao *reset* do número incremental de contagem de pacotes. Após o ataque, para se obter certificação WPA2 era necessário implementar o PMF, como forma de tentar dificultar os ataques KRACK, e em janeiro de 2018 a Wi-Fi Alliance anunciou o WPA3. [10] [11]

2. Análise de segurança do WPA3

Neste capítulo serão expostas e analisadas as novas funcionalidades, e também as possíveis vulnerabilidades e soluções.

2.1.Visão global do WPA3

O WPA3 é a versão melhorada do seu antecessor, o WPA2, mas com a adição de novas funcionalidades. Estas funcionalidades vêm simplificar a segurança no Wi-Fi e melhorar o método de autenticação, como também, aumentar o nível de criptografia para os dados mais sensíveis nos casos empresariais, e garantir que as redes se mantenham resilientes a falhas. [12]

O WPA3 introduz 4 novas funcionalidades:

1. Um novo protocolo de autenticação, chamado SAE (*Simultaneous Acquisition of Equals*).
2. Um método mais seguro de adicionar dispositivos facilmente à rede, *Device Provisioning Protocol* que vem substituir o antigo WPS (Wi-Fi *Protected Setup*) que era provado inseguro.
3. Um mecanismo de encriptação em redes abertas e não protegidas, *Opportunistic Wireless Encryption*.
4. Uso de chaves 192-bit.

No entanto, apesar destas novidades todas, apenas é necessário implementar a primeira para se obter certificação WPA3. Sendo que as restantes são certificações complementares, *Easy Connect*, *Enhanced Open*, e WPA3-Enterprise *certified* respetivamente. Comparativamente ao WPA2, o WPA3 emprega essencialmente as mesmas funcionalidades, mais as referidas acima. No entanto, protocolos *legacy* como TKIP não fazem parte deste novo protocolo e a utilização de PMF torna-se também obrigatório. [12] [13]

2.2. SAE

A grande novidade para o WPA3 em geral, é o novo protocolo de autenticação, SAE (*Simultaneous Acquisition of Equals*), baseado no *dragonfly handshake*, que vem substituir o *4-way handshake* usado anteriormente. Este novo *handshake* deverá aumentar a resistência contra ataques de dicionário *offline*, que era um dos problemas principais de segurança no

WPA2, visto que o mesmo é um protocolo SPEKE (*Simple Password Exponential Key Exchange*). [12]

2.2.1. Dragonfly Handshake

O *Dragonfly handshake* é um mecanismo para troca de chaves através do uso de criptografia logarítmica discreta que são autenticadas usando uma *password*, mais concretamente, é usado a Criptografia de Curva Elíptica (ECC), ou a Criptografia de Campos Finitos (FFC) que é essencialmente o mesmo que ECC mas num campo de valores finitos. O processo deste *handshake* usando ECC funciona da seguinte forma:

- Duas entidades, Alice e Bob, escolhem um ECC, **E**, e um número primo, **p**, em comum;
- Alice e Bob partilham uma chave secreta **P**, estabelecida através de um mecanismo *out-of-band*. Esta chave secreta é essencialmente a mesma que a PSK no *4-way handshake*;
- Estes derivam uma coordenada **X** a partir de **P**, de uma função de hash, **H**, e uma função de derivação de chaves, **KDF**. Este processo é denominado pela rfc7664 como a técnica de "*hunting-and-peeking*". Esta técnica envolve a repetição da derivação de **X** até este ser um resíduo quadrático válido do modelo de **p**, isto é, um ponto que válido na curva elíptica usada no **E** escolhido. Depois de encontrada o ponto válido este resulta num gerador que é definido como o elemento password (**PE**);
- Depois são gerados dois números aleatórios, **private** e **mask** através de **E**, estes são usados para construir os valores, **scalar** e **element**;
- Estes depois são partilhados entre a Alice e o Bob, e verificam se os valores são válidos;
- Agora que ambos partilham o **scalar** e **element** do lado oposto, este podem criar a PMK, este passo é semelhante ao que acontece no algoritmo de troca de chaves de Diffie-Hellman;
- Para confirmar que ambos os lados criaram a mesma password, é enviado o valor a função de hash especificada na rfc77664. [14]

O *Dragonfly handshake* é basicamente uma troca de duas mensagens, a "*Commit Exchange*" no qual ambos os lados comprometem a uma adivinha da password, e a

mensagem de "*Confirm Exchange*" para confirmar que ambos as entidades conhecem a password pertencente ao lado oposto. [14] Como é possível verificar, com este *handshake* as passwords dos utilizadores são utilizados como parâmetro para obter uma PMK, o que torna o nível de complexidade exigido pela password do utilizador ser menos exigente já que o *Dragonfly key Exchange* consegue estabelecer uma melhor password. Desta forma, o novo *handshake* no WPA3 é um melhoramento na segurança no sentido que é mais simples aplicar segurança num ambiente pessoal.

Ataque de dicionário

Com o *Dragonfly* um ataque de dicionário torna-se impraticável devido aos números **private** e **mask** serem aleatórios, deixando apenas o gerador da curva elíptica, **PE**, como a variável que um atacante consegue adivinhar. Isto é essencialmente o problema do logaritmo discreto, em que é fácil obter o resultado num sentido mas difícil no sentido oposto. Isto é possível se considerarmos que o grupo de valores usado na curva elíptica é grande o suficiente para tornar este tipo de ataque impraticável. Desta forma é também impossível efetuar um ataque de dicionário *offline* pois este só conseguirá ter a certeza de que encontrou a password partilha através de ataques ativos. [14]

Ataque KRACK

Apesar do *4-way handshake* ter sido matematicamente comprovado com seguro este não o torna imune a certas ações, o ataque KRACK tira partido das próprias mensagens transmitidas no *handshake* para enganar a vítima a reinstalar uma chave quando este já tem uma instalada, isto é, ao colecionar e retransmitir mensagens do 3ª passo no *4-way handshake* este consegue reinstalar a chave, e reiniciar os parâmetros associados como o número incremental da transmissão de pacote (*nonce*) e número do pacote recetor (*replay counter*) para o seus valores iniciais. Desta forma o ataque consegue manipular o *handshake* e abusar esta fraqueza. [15] O WPA3 combate este ataque ao usar o *Dragonfly handshake* que torna este tipo de ataque impraticável devido à diferente forma de estabelecimento da PMK nos dois *handshakes*.

2.2.2. Pros e contras do Dragonfly handshake

A grande vantagem do novo *handshake* é o facto de este tirar partido da criptografia de Curva Elíptica, esta é considerada ser uma boa alternativa a outros tipos de criptografias como o RSA que usa aritmética modular. Tal como nas criptografias de aritmética modular,

a ECC disfruta também do problema de logaritmo discreto o que torna o processo para quebrar o algoritmo difícil. Mas ao contrário das outras criptografias o ECC usa uma curva elíptica para definir um conjunto de valores no qual é usada para estabelecer a PMK.

Outra vantagem com o ECC está nos tamanhos de chaves necessários para aplicar um nível de segurança serem mais pequenos. Como se pode visualizar na Figura 7, o tamanho de uma chave no ECC necessário para alcançar a mesma segurança no RSA é mais pequena.

RSA key size (bits)	ECC key size (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

[16]

Figura 7 - Tamanho de chaves para aplicar o mesmo nível de segurança

Assim, o ECC consegue obter a mesma segurança usando menos recursos da memória e de espaço de armazenamento para chaves e poder de processamento para gerar chaves. Este resultado na figura é justificado essencialmente através das técnicas existente para quebrar estas criptografias, o ECC apresenta as técnicas *Pollard's rho* e *baby-step giant-step* enquanto que o RSA por exemplo, tem técnicas mais rápidas como o *General number field sieve*. [16]

A desvantagem do *Dragonfly* é de existir a potencialidade do *handshake* ser um *backdoor* da NSA, isto advém da natureza das curvas elípticas especificadas pela NIST. Isto normalmente é possível quando uma curva é estabelecida com certos parâmetros que tornam o problema do logaritmo discreto fácil, deixando assim vulnerabilidades na curva colocadas de forma intencional, mas para evitar este tipo de ações é usado nas curvas elípticas o parâmetro de domínio adicional *seed*, que é um valor aleatório utilizado para gerar os coeficientes usados no gerador de um ponto na curva elíptica, assim é possível dar algum tipo de garantia de que a curva não foi criada com vulnerabilidades em mente. [17] Mas, o problema que surge aqui é que apesar do uso do *seed*, é possível que esta garantia seja

ignorada ao encontrar um conjunto de curvas fracas e testar vários *seeds* até encontrar uma vulnerabilidade por onde é possível explorar um algoritmo que use essas curvas. [16]

2.3. Problemas e possíveis soluções para o WPA3

No momento de realização do presente trabalho, das novas funcionalidades introduzidas pela Wi-Fi Alliance juntamente com o WPA3, apenas a implementação do *Dragonfly handshake* é necessário para obter a certificação WPA3, e o modo opcional de segura de mínima força de 192-bit para o certificado WPA3-Enterprise, o que é basicamente um aumento do tamanho das chaves usadas nos mecanismos de segurança. As outras funcionalidades novas, *Easy Connect* e *Opportunistic Wireless Encryption*, tem as suas certificações separadas, deixando assim uma oportunidade perdida para aumentar a segurança nas redes Wi-Fi. [18]

O *Dragonfly handshake* em si não aparenta ter grandes problemas severos, sendo que a única falha de segurança possível será a possibilidade da existência de uma *backdoor* nas curvas elípticas recomendadas pela NIST. Como estas curvas são fundamentais no processo do estabelecimento para os elementos usados para criar a PMK, através do problema do logaritmo discreto que deve ser difícil no sentido oposto, a possibilidade das curvas recomendadas serem fracas conseguem permitir a existência da *backdoor*. Assim o problema do logaritmo deixa de ser difícil, o que leva ao comprometimento da própria PMK.

Em termos de soluções para estes problemas, poderá não ser simples a aplicação de soluções visto que o WPA3 ainda é um protocolo recente e para atrair os fabricantes de equipamento de rede a certificarem os seus equipamentos em WPA3 em vez do WPA2, a Wi-Fi Alliance parece ter separado as novas funcionalidades em diferentes certificados precisamente para isto. Esta decisão do nosso ponto de vista é compreensível, mas isto não justifica a possibilidade de existir um certificado WPA3 com apenas uma funcionalidade requerida. Certamente o melhor a fazer para garantir uma melhor segurança no Wi-Fi seria adicionar as funcionalidades, *Easy Connect* e *Opportunistic Wireless Encryption*, ao certificado WPA3 mas manter a existência de certificados separados para cada uma destas funcionalidades, desta forma os equipamentos certificados em WPA3 poderão usufruir das melhores tecnologias de segurança, e manter a liberdade de escolha caso um fabricante precise apenas usar uma destas funcionalidades num dos seus equipamentos. Da mesma

forma, a única solução para o problema no *Dragonfly handshake* seria usar um *handshake* diferente que não se baseie na ECC, ou usar curvas elípticas recomendadas por outra entidade confiada globalmente e que não pertença a nenhum organismo governamental, contrário ao caso da NIST que pertence ao governo dos Estados Unidos da América.

3. Conclusão

Com este trabalho, os objetivos propostos era analisar o funcionamento do WPA3, testar o seu funcionamento e identificar possíveis vulnerabilidades e problemas neste. De todos estes apenas a implementação de um cenário de testes do WPA3 não foi possível realizar, sendo este protocolo bastante recente e os routers disponíveis para testar o protocolo verificaram mostrar menos adaptabilidade do que inicialmente era pressuposto. De resto, foi possível concretizar todos os objetivos definidos para este trabalho, principalmente a análise do novo *handshake* do WPA3 e como este resolve um dos mais recentes ataques ao WPA2, o ataque KRACK.

O desenvolvimento deste trabalho possibilitou o enriquecimento dos nossos conhecimentos sobre os vários protocolos de segurança usados ao longo dos anos nas redes Wi-Fi, e percebemos que a segurança implementada nestas redes tem vindo a aumentar mas que poderia ser melhor se a organização responsável pelo Wi-Fi, a Wi-Fi Alliance, interagisse mais com entidades universitárias e académicas de forma a diminuir a ocorrência de falhas nos protocolos de segurança antes destas serem lançadas, um exemplo desta prática é os RFC pela IETF. Esta opinião é partilhada pelo autor pela descoberta do ataque KRACK, Mathy Vanhoef.

No futuro seria importante realizar um trabalho que explorasse o funcionamento do WPA3 em modo transacional. Neste modo um cliente que ainda não suporte WPA3 poderá estabelecer ligação com um AP WPA3, apesar de serem usados *handshakes* diferentes. Também seria interessante efetuar um estudo no uso de PMF neste modo transacional, pelo que um dispositivo *legacy*, que não suporta PMF, deve conseguir comunicar com um AP WPA3 no modo transacional, no qual define o uso de PMF como não necessário apesar do uso de PMF nas comunicações SAE ser obrigatório. Este modo está muito dependente da implementação feita pelos fabricantes, e devido à falta de dispositivos que tragam WPA3 no mercado, ainda não existe muita informação quanto ao tema.

Referências

[1] Cisco, “Cisco IOS Wireless LAN Configuration Guide, Release 15.1,” [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/wlan/configuration/guide/15_1/wl_15_1_book/wi_secure.html#wp1074995. [Acedido em 11 12 2018].

[2] S. Fluhrer, I. Mantin e A. Shamir, “Weaknesses in the Key Scheduling Algoritm of RC4,” [Online]. Available: https://www.mattblaze.org/papers/others/rc4_ksaproc.pdf. [Acedido em 11 12 2018].

[3] Wikipedia, “Wired Equivalent Privacy,” Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy. [Acedido em 11 12 2018].

[4] RF Wireless World, “WEP vs WPA vs WPA2 | Difference between WEP,WPA,WPA2,” RF Wireless World, [Online]. Available: http://www.rfwireless-world.com/Terminology/WEP-vs-WPA-vs-WPA2.html. [Acedido em 11 12 2018].

[5] H. Cheung, “The Feds can own your WLAN too,” [Online]. Available: https://web.archive.org/web/20050827104827/http://www.tomsnetworking.com/Sections-article111.php. [Acedido em 11 12 2018].

[6] M. Ihonen, A. Salo e T. Timonen, “802.11 security protocols, Lappeenranta University of Technology,” [Online]. Available: http://edu.pegax.com/lib/exe/fetch.php?media=secc:seminar_report_802.11_protocols_ver.1.0_final.pdf. [Acedido em 12 12 2018].

[7] mtroi, “4-Way Handshake,” [Online]. Available: https://wlan1nde.wordpress.com/2014/10/27/4-way-handshake/?fbclid=IwAR2GOeKN0ePv-Bo_Ih_XcrZyT_89c7mkkxn6g95OqshDoF_Zp6iS1LG9qo4. [Acedido em 20 1 2019].

[8] Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/File:4-way-handshake.svg. [Acedido em 19 1 2019].

[9] D. Akin e J. Geier, “CWAP, Certified Wireless Analysis Professional, Official Study Guide,” [Online]. Available: https://www.cwnp.com/wp-content/uploads/pdf/CWAP_WLAN_ANALYSIS.pdf. [Acedido em 12 12 2018].

[10 Cisco, “802.11w Protected Management Frames,” [Online]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.pdf. [Acedido em 20 1 2019].

[11 mtroi, “Protected Management Frames (802.11w),” [Online]. Available: https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w/?fbclid=IwAR15fDD7JV3axc3iijeGLl25-uXin69VxwPQ6mlN-ETKbSb0qmkFHMRlIHc. [Acedido em 20 1 2019].

[12 Wi-Fi Alliance, “Security,” [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security. [Acedido em 27 12 2018].

[13 Diffen, “WPA2 vs. WPA3,” Diffen, [Online]. Available: https://www.diffen.com/difference/WPA2_vs_WPA3?fbclid=IwAR01ruCd6L926NzBieFk3DdI8crOQu1E5UHiKYDtwiFLe1siuQ1qvUwJV44#Device_Provisioning_Protocol_.28DPP.29. [Acedido em 20 1 2019].

[14 D. Harkins, “rfc7664 - Dragonfly Key Exchange,” [Online]. Available: https://tools.ietf.org/html/rfc7664. [Acedido em 20 12 2019].

[15 M. Vanhoef, “Key Reinstallation Attacks, Breaking WPA2 by forcing nonce reuse,” [Online]. Available: https://www.krackattacks.com/. [Acedido em 10 12 2018].

[16 A. Corbellini, “Elliptic Curve Cryptography: breaking security and a comparison with RSA,” [Online]. Available: https://andrea.corbellini.name/2015/06/08/elliptic-curve-cryptography-breaking-security-and-a-comparison-with-rsa/. [Acedido em 20 12 2018].

[17 A. Corbellini, “Elliptic Curve Cryptography: ECDH and ECDSA,” [Online]. Available: https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/. [Acedido em 20 12 2018].

M. Vanhoef, “WPA3: A Missed Opportunity,” 27 6 2018. [Online]. Available: https://www.mathyvanhoef.com/2018/06/wpa3-missed-opportunity.html. [Acedido em 20 12 2018].
[18]