Universidade Federal de Pernambuco

Centro de Informática

Graduação em Ciência da Computação

AUTENTICAÇÃO BASEADA EM ECDH PARA REDES IEEE 802.11

Eduardo Ferreira de Souza

TRABALHO DE GRADUAÇÃO

Recife

06 de dezembro de 2010

Universidade Federal de Pernambuco

Centro de Informática

Eduardo Ferreira de Souza

AUTENTICAÇÃO BASEADA EM ECDH PARA REDES IEEE 802.11

Trabalho apresentado ao Programa de Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: *Paulo André da Silva Gonçalves*

Recife

06 de dezembro de 2010

Dedico este trabalho primeiramente a Deus, pois sem Ele minha vida não faria nenhum sentido. Dedico aos meus pais Mário e Celma, por todo estímulo e apoio que me deram, sendo sempre referenciais para mim. Também à minha irmã Mariana e minha sobrinha Marina, que me fazem viver em constante sentimento de saudade. Finalmente, dedico à minha namorada Karol, por ser muito mais que uma namorada para mim.

AGRADECIMENTOS

Agradeço a Deus, que têm me dado oportunidades que eu nunca imaginei ter, me permitindo crescer academicamente e em outras áreas de minha vida.

Ao meu orientador, professor Paulo Gonçalves, que sempre se mostrou presente durante minhas pesquisas, me instigando a sempre procurar melhorar e ajudando a tomar decisões que me deram bons resultados.

Agradeço aos meus colegas do grupo de pesquisa Bruno Gentilini, Bruno de Jesus, Bruno Almeida, Caio, Júlio e Marcos, pela troca de experiência e apoio nas pesquisas. Agradeço também a eles pelo conhecimento que me passaram através das reuniões do grupo.

Agradeço aos professores do Centro de Informática que contribuíram com minha formação acadêmica. Em especial, aos professores Paulo Gonçalves e Fernando Fonseca, que além de grades mestres, tornaram-se grandes amigos meus.

Agradeço aos meus amigos Carlos Eduardo, Augusto, Marília, Rafael, Valdir e Luiz Paulo, pelo apoio, pelos momentos descontração e pela compreensão por minha ausência por diversas vezes. Agradeço também aos meus amigos do Centro de Informática Guilherme, Gileno, Lailson, Ygor, Gabriel, Filipe, Caio, Camila, Igor, Luis Felipe, Bruno, Daniel e todos os que contribuíram para que essa graduação fosse extremamente agradável e por me ajudarem na minha formação através dos projetos que realizamos juntos.

Agradeço à minha família, meus pais Mário e Celma e minha irmã Mariana, pelo apoio e por todo amor que sempre me deram. Agradeço à namorada Karol, por ser minha companheira para todos os momentos, por ser uma grande amiga e por me animar nas horas de desânimo.

“ Não fiz o melhor,

mas fiz tudo para que o melhor fosse feito.”

—MARTIN LUTHER KING

RESUMO

Em redes que utilizam os protocolos WPA, WPA2 ou IEEE 802.11i e esses dois protocolos com a emenda IEEE 802.11w, as chaves que compõem a PTK (*Pairwise Transient Key*) permitem que os clientes da rede possam trocar mensagens com a devida criptografia e verificação de integridade. Devido a sua importância, a PTK deve ser mantida em completo sigilo pelo protocolo. Porém, nos protocolos mencionados, o processo *4-Way Handshake* é falho quando o método de autenticação pessoal é usado, permitindo que entidades maliciosas que possuam a chave pré-compartilhada da rede (PSK - *Pre-Shared Key*) possam reproduzir o processo de derivação da chave PTK de todos os clientes autenticados.

Este trabalho propõe e avalia experimentalmente um novo processo de *handshake*. O mecanismo proposto, denominado *Improved Handshake*, é baseado no protocolo Diffie-Hellman sobre Curvas Elípticas (ECDH) e elimina a vulnerabilidade que permite ataques de derivação indevida da PTK. Além disso, o também é apresentada uma adaptação do *Improved Handshake* para ser utilizado como processo de autenticação dos usuários em redes abertas. Essa adaptação permite que os usuários sejam autenticados na rede sem a necessidade de fornecimento prévio de chaves. Desse modo, o *Improved Handshake* permite que os usuários troquem o informações criptografadas na camada de enlace, diferentemente das redes abertas tradicionais.

ABSTRACT

In networks that use the protocols WPA, WPA2 or IEEE 802.11i and these protocols enhanced by the amendment IEEE 802.11w, the keys that compose the PTK (Pairwise Transient Key) allow network devices to exchange messages with proper encryption and integrity check. Because of its importance, the PTK should be kept in secret by the protocol. However, in all of aforementioned protocols, the 4-Way Handshake is flawed when the personal authentication method is used, allowing malicious entities that possess the PSK (Pre-Shared Key) of the network to reproduce the process of deriving the PTK key of all authenticated clients.

In this work, we propose and evaluate a new handshake protocol. The proposed mechanism, named Improved Handshake, is based on Elliptic Curves Diffie-Hellman protocol (ECDH) and solves the problem of undue PTK derivation. We also present a solution to provide automatic authentication on open networks. This solution allows users to be authenticated on the network without the need of providing keys. Thus, allowing users to exchange encrypted information in the link layer, unlike traditional open networks.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

GLOSSÁRIO

AES *Advanced Encryption Standard*: Algoritmo de cifra por blocos. 9

AP *Access Point* ou Ponto de Acesso. 6

BIP *Broadcast/multicast Integrity Protocol*. 10

CBC-MAC *Cipher Block Chaining Message Authentication Code*. 9, 18

CCMP *Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*. 9, 17, 18

DH Diffie-Hellman: Protocolo de acordo de chaves seguras sobre canal inseguro. 22, 24–27, 29, 36

EAP *Extensible Authentication Protocol*. 11, 12

EAPOL *Extensible Authentication Protocol over LAN*. 11

ECDH *Elliptic Curve Diffie-Hellman* ou Protocolo Diffie-Hellman sobre Curvas Elípticas. 22, 24, 25, 28–31, 35, 37

GEK *Group Encryption Key*: Chave para cifrar os quadros em *broadcast* e *multicast*. 18

GIK *Group Integrity Key*: Chave de verificação de integridade no TKIP para *broadcast* e *multicast*. 19

GTK *Group Temporal Key*: Conjunto de chaves para quadros em *broadcast* e *multicast*. 14, 16–18, 32, 34

ICV *Integrity Check Value* ou Valor de Checagem de Integridade. 7, 8

IEEE *Institute of Electrical and Electronics Engineers*. 6, 26

IEEE 802.11i Padrão de segurança para redes IEEE 802.11. 1, 4–9, 16

IEEE 802.11w Emenda aos padrões WPA e IEEE 802.11i. 1–6, 10, 11, 14, 15, 17, 28, 33, 35

IEEE 802.1X Padrão para controle de acesso com base em portas. 3, 11, 13

IGTK *Integrity Group Temporal Key*. 10, 14, 17, 33, 34

IH *Improved Handshake*: Proposta desse trabalho. 30, 31, 33

IV *Initialization Vector* ou Vetor de Inicialização. 7

KCK *Key Confirmation Key*: Chave de verificação de integridade durante os *handshakes*. 14, 17

KEK *Key Encryption Key*: Chave para cifrar outras chaves nos *handshakes*. 14, 17, 34

MAC *Medium Access Control*, ou Camada de Controle de Acesso ao Meio. 14, 15

MIC *Message Integrity Check*: Campo de verificação de integridade. 8, 9, 14, 17, 31, 32

PLD Problema do Logaritmo Discreto. 20–22

PLDCE Problema do Logaritmo Discreto sobre Curvas Elipticas. 22, 23, 34

PMK *Pairwise Master Key*. 12, 13, 15, 26, 27, 31–34

PRF *Pseudo-Random Function* ou Função Pseudoaleatória. 15, 32

PSK *Pre-Shared Key* ou Chave Pré-Compartilhada. 3, 13, 15, 16, 26

PTK *Pairwise Transient Key*: Conjunto de chaves para quadros em *unicast*. 3, 4, 9, 10, 14–18, 26, 27, 30–34

RC4 *Ron's Code 4* ou *Rivest Cypher 4*: Algoritmo de cifra por fluxo. 7–9

TEK *Temporary Encription Key*. 18

TK *Temporary Key*: Outro nome para TEK. 18

TKIP *Temporary Key Integrity Protocol*. 8, 17–19

TLS *Transport Layer Security*. 12

TMK *Temporary MIC Key*: Chave de verificação de integridade no TKIP. 18

WEP *Wired Equivalent Privacy*. 1, 6–10

Wi-Fi *Wireless Fidelity*. 1

WPA *Wi-Fi Protected Access*. 1–11, 13–15, 17, 28, 35

WPA-PSK WPA no modo de autenticação por PSK. 8, 26

WPA2 *Wi-Fi Protected Access 2* ou IEEE 802.11i. 1–3, 9–11, 13–15, 17, 28, 35

WPA2-PSK WPA2 no modo de autenticação por PSK. 26

CAPÍTULO 1

INTRODUÇÃO

A comunicação em redes sem fio entre dispositivos computacionais têm crescido significativamente graças à mobilidade fornecida aos seus usuários nessas redes. Para acessar as informações que trafegam na rede, basta que o usuário disponha de um dispositivo que capte o sinal transmitido, tornando-as altamente flexíveis e expansíveis. Atualmente a principal tecnologia de rede sem fios utilizada para acesso à Internet e criação de redes locais em ambientes domésticos e corporativos é a IEEE 802.11, conhecida como *Wi-Fi*. O IEEE 802.11 é um conjunto de especificações que envolve uma grande família de protocolos voltados para a comunicação segura entre hosts sem fio. As especificações compreendem as camadas física e enlace.

O principal problema das redes sem fios é que o meio por onde trafegam as informações permite a captura indevida do tráfego. Para suprir o problema de acesso indevido aos dados no padrão IEEE 802.11 são criados protocolos de segurança. Tais protocolos têm por objetivo prover autenticação aos usuários genuínos, certificar que os dados cheguem íntegros ao receptor e garantir confidência dos dados da camada de enlace. Ao longo dos anos, os seguintes protocolos de segurança foram definidos para atuarem na camada enlace dessas redes protegendo os quadros de dados: WEP (*Wired Equivalent Privacy*) [1], WPA (*Wi-Fi Protected Access*) [2] e IEEE 802.11i ou WPA2 [3]. Em 2009 foi publicada a emenda IEEE 802.11w [4], que complementa o WPA e o WPA2 e provê proteção aos quadros de gerenciamento. Dentre esses protocolos, o WEP é considerado ultrapassado devido à sua longa lista de vulnerabilidades [5].

As redes IEEE 802.11 também podem ser utilizadas em modo aberto. Nesses casos, nenhum protocolo é configurado para prover segurança à camada de enlace de tais redes e não há chaves de segurança para que os usuários se autentiquem na rede, visto que não

há autenticação. As redes abertas geralmente são utilizadas em ambientes públicos como *shoppings*, aeroportos e restaurantes. Nesses ambientes os usuários podem precisar, no máximo, fornecer credenciais (*e.g.* CPF ou *login*/senha) para terem o acesso à Internet permitido, como acontece geralmente em aeroportos. Além disso, muitas redes IEEE 802.11 residenciais são previamente configuradas para operarem no modo aberto. Isso ocorre, em geral, por falta de conhecimento técnico dos usuários em relação ao uso de um protocolo de segurança.

1.1 MOTIVAÇÃO

Apesar da constante necessidade de se melhorar os protocolos de segurança, as redes IEEE 802.11 possuem poucas vulnerabilidades que ainda não foram propostas soluções eficazes para solucioná-las. Em geral, os ataques existentes para tais redes nos protocolos WPA e WPA2 apenas são possíveis caso a rede esteja utilizando configurações específicas que abram brechas de segurança. Exemplos dessas configurações são: tempo elevado de validade das chaves temporárias e chaves de acesso pequenas ou formadas por palavras conhecidas. Assim sendo, esse tipo de problema geralmente pode ser solucionado bastando-se modificar algumas configurações da rede. Porém, ainda existem vulnerabilidades nos protocolos de segurança que independem da configuração da rede e que ainda não possuem soluções eficazes.

Atualmente o processo de autenticação dos usuários apresenta vulnerabilidades que comprometem significativamente a segurança da rede. Em geral, problemas de segurança na etapa de autenticação são extremamente críticos, pois nessa fase são definidas as chaves de segurança a serem utilizadas na comunicação posterior. Assim sendo, caso o protocolo permita a realização de ataques que comprometam a obtenção de forma segura das chaves, toda a comunicação pode tornar-se insegura. As vulnerabilidades nos mecanismos de autenticação motivam este trabalho a focar em soluções relacionadas a estes mecanismos nos protocolos de segurança das redes IEEE 802.11.

Os protocolos WPA, WPA2 e ambos os protocolos utilizando a emenda IEEE 802.11w especificam dois métodos de autenticação de usuários à rede: autenticação corporativa e

autenticação pessoal. No método de autenticação corporativa um servidor de autenticação baseado no padrão IEEE 802.1X [6] é responsável por verificar as credenciais dos usuários e fornecer uma chave mestra ao cliente e ao ponto de acesso. Esse método de autenticação é especificado com foco em redes de médio e grande porte, visto que se faz necessário de uma infraestrutura mais robusta, permitindo um melhor gerenciamento dos usuários da rede.

O método de autenticação pessoal é utilizado geralmente em redes de pequeno porte ou em ambientes que não dispõem de um servidor de autenticação. Nesse caso, a autenticação dos usuários é realizada por completo pelo ponto de acesso. Contudo, o ponto de acesso não autentica os usuários em caráter individual, mas verifica apenas se eles possuem a chave pré-compartilhada da rede. Essa chave é denominada PSK (*Pre-Shared Key*) e deve ser possuída por todos os usuários legítimos.

A autenticação propriamente dita é realizado durante o processo de *4-Way Handshake* entre o cliente e o ponto de acesso. Nesse processo, que independe do método de autenticação utilizado, o cliente e o ponto de acesso derivam uma chave PTK (*Pairwise Transient Key*) comum e exclusiva a eles que representa, na prática, um conjunto de chaves temporárias. A PTK é utilizada, entre outras coisas, para a criptografia de quadros e verificação da integridade dos mesmos.

O *4-Way Handshake* é vulnerável em redes que usam o método de autenticação pessoal. São afetados os protocolos WPA, WPA2 e ambos complementados pela emenda IEEE 802.11w. Tal vulnerabilidade permite que a derivação da PTK de qualquer cliente autenticado seja reproduzida por entidades maliciosas que conheçam a chave pré-compartilhada da rede. Para a realização do ataque, a entidade maliciosa apenas precisa capturar as duas primeiras mensagens trocadas durante o *4-Way Handshake* do cliente alvo. De posse dessas informações, uma entidade maliciosa pode ter acesso aos dados transmitidos e recebidos por outros clientes. No Capítulo 3 será apresentado detalhadamente o funcionamento do *4-Way Handshake* e sua vulnerabilidade de derivação indevida da PTK.

Além das vulnerabilidades dos protocolos de segurança, as redes IEEE 802.11 quando

configuradas em modo aberto são extremamente vulneráveis a acesso indevido de informações. Nesses ambientes, como não há um processo de autenticação dos clientes na rede sem fio, qualquer entidade maliciosa pode também se associar à rede. Além disso, nessas redes os dados dos usuários trafegam sem qualquer criptografia, excetuando-se quando a mesma é provida por camadas superiores da pilha de protocolos (e.g. uso de HTTPS). Assim sendo, um atacante pode capturar e adulterar os dados de todos os usuários da rede.

1.2 OBJETIVOS

O objetivo geral desse trabalho é propor mecanismos que solucionem o problema de derivação indevida das chaves PTK e a falta de autenticação nas redes IEEE 802.11 abertas. Serão abordados os problemas dos protocolos WPA, IEEE 802.11i e ambos os protocolos estendidos pela emenda IEEE 802.11w, além das propostas existentes no estado da arte.

Para alcançar o objetivo geral, os seguintes objetivos específicos são definidos:

1. Realizar uma análise aprofundada dos mecanismos de autenticação de cada protocolo de segurança e verificar motivos que permitem a realização de ataques de derivação indevida da chave PTK;

2. Analisar as propostas que visam solucionar tal vulnerabilidade nos protocolos de segurança das redes IEEE 802.11;

3. Propor um mecanismo de segurança que elimine o problema da derivação indevida da PTK e que permita autenticação automática nas redes abertas;

4. Avaliar experimentalmente o mecanismo proposto e compará-lo aos mecanismos de autenticação utilizados pelos protocolos de segurança e aos trabalhos relacionados.

1.3 ORGANIZAÇÃO DO TRABALHO

O restante deste trabalho está organizado da seguinte forma: o Capítulo 2 descreve, de modo geral, os protocolos de segurança das redes IEEE 802.11. O Capítulo 3 apresenta uma descrição aprofundada dos mecanismos de autenticação utilizados nos protocolos WPA, IEEE 802.11i e ambos com a emenda IEEE 802.11w, além de descrever as chaves utilizadas em cada um desses protocolos. No Capítulo 4 são descritos e comparados dois protocolos de acordo de chaves seguras, utilizados como base para as propostas desse trabalho e dos trabalhos relacionados. No Capítulo 6 são apresentadas as duas propostas desse trabalho. O Capítulo 7 apresenta a avaliação experimental realizada sobre os propostas desse trabalho, realizando uma comparação com os trabalhos relacionados. Finalmente, o Capítulo 8 apresenta as conclusões do trabalho.

CAPÍTULO 2

PROTOCOLOS DE SEGURANÇA DAS REDES IEEE 802.11

Esse capítulo apresenta os uma descrição dos protocolos de segurança WEP, WPA, IEEE 802.11i e da emenda IEEE 802.11w. Apesar de também ser um protocolo de segurança para as redes IEEE 802.11, o WEP não é utilizado como foco para a proposta desse trabalho. Essa decisão é tomada pelo fato do WEP ser considerado obsoleto e possuir várias vulnerabilidades em aspectos que independem do processo de autenticação. Os protocolos de segurança são descritos a seguir considerando os seus procedimentos de: autenticação dos usuários, verificação de integridade e confidência dos dados.

2.1 WIRED EQUIVALENT PRIVACY (WEP)

O protocolo WEP foi o primeiro padrão especificado pelo IEEE (*Institute of Electrical and Electronic Engineers* para prover segurança em redes IEEE 802.11 [1]. O WEP foi desenvolvido para prover um grau de confidência comparável às redes cabeadas, no entanto isso não acontece na prática. No ano de 2001 começaram a surgir ataques que comprometiam significativamente a segurança do protocolo. Atualmente o protocolo é considerado obsoleto devido à sua longa lista de vulnerabilidades.

No WEP todo processo de autenticação dos clientes na rede é realizado pelo ponto de acesso (*Access Point* - AP) através de uma chave pré-compartilhada. Essa chave deve ser conhecida por todas as entidades da rede (clientes e AP). Para se autenticar, o cliente solicita autenticação ao AP que, em seguida, envia ao cliente um texto-desafio com conteúdo aleatório. O cliente cifra o texto-desafio com sua chave pré-compartilhada e envia o resultado ao AP. O AP ao decifrar a mensagem recebida, verifica se o resultado

é o texto-desafio originalmente enviado. Em caso positivo, o cliente é autenticado na rede.

Para verificar a integridade das mensagens trocadas, o WEP concatena um campo de verificação de integridade (*Integrity Check Value* - ICV) a cada mensagem enviada, para que em seguida possa ser realizada a crifragem. Ao receber uma mensagem, o receptor a decifra e, em seguida, calcula o ICV do texto-plano. O ICV calculado no receptor é verificado se possui valor idêntico ao ICV concatenado à mensagem. Caso sejam diferentes, a mensagem é descartada.

Visando garantir confidência às mensagens, o WEP utiliza o algoritmo de cifra de fluxo RC4. A chave base utilizada para cifra das mensagens é uma concatenação entre um vetor de inicialização (IV) e a chave pré-compartilhada. O vetor de inicialização varia a cada nova mensagem e é enviado em texto-plano juntamente com o texto-cifrado da mensagem. O RC4 gera a partir da chave base (IV e chave pré-compartilhada) um *keystream*. Para a cifragem e decifragem da mensagem, é realizada uma operação de *ou exclusivo* entre seu conteúdo e o *keystream*.

São várias as vulnerabilidades já encontradas no WEP que comprometem sua segurança nos aspectos de confidência, integridade e autenticação: o mecanismo de confidência permite que a senha de segurança possa ser descoberta a partir de ataques estatísticos [7] [8] [9]; a integridade dos pacotes não é provida de forma segura, visto que este mecanismo permite ataques onde se descobre o conteúdo das mensagens sem ao menos saber a chave de criptografia (ataques *chopchop*) [10]; e o processo de autenticação do WEP permite que um atacante possa se autenticar na rede sem conhecer a chave, através de uma escuta dos pacotes trocados durante a autenticação de um cliente na rede.

2.2 WI-FI PROTECTED ACCESS (WPA)

As vulnerabilidades existentes no protocolo WEP motivou o desenvolvimento de um novo padrão de segurança, denominado IEEE 802.11i. Ainda durante o desenvolvimento do IEEE 802.11i foi lançada uma versão preliminar de sua especificação, que foi utilizada como base para a criação do protocolo WPA [2]. Assim sendo, apesar de o WPA possuir

várias semelhanças com o IEEE 802.11i, ainda há alguns mecanismos do protocolo WEP que são mantidos. A principal alteração do WPA em relação ao WEP ocorreu no processo de autenticação, que foi completamente modificado. Diferentemente do WEP, o WPA possui dois possíveis métodos de autenticação: autenticação corporativa e autenticação pessoal (WPA-PSK). No entanto, também houve mudanças significativas nos processos de verificação de integridade e confidência das mensagens.

O WPA é utilizado, por padrão, conjuntamente o TKIP (*Temporal Key Integrity Protocol*), que é um protocolo baseado em chaves hierárquicas e temporárias. As chaves temporárias são utilizadas apenas por um determinado período de tempo e posteriormente são substituídas dinamicamente. No TKIP existem chaves mestras, que têm o objetivo de permitir a derivação de novas chaves. As chaves derivadas com base nas chaves mestra são, em geral, temporárias e possuem objetivos mais específicos, como a cifragem ou verificação da integridade das mensagens trocadas.

No WPA é utilizado o RC4 para prover confidência às mensagens trocadas, que é algoritmo de cifra utilizado pelo protocolo WEP. No entanto, a estrutura de chaves provida pelo TKIP e a utilização de um mecanismo de mistura de chaves, realizado antes de os quadros serem cifrados, impedem a realização dos diversos ataques de recuperação de chaves existentes para o WEP. Até onde se sabe, não existem ataques práticos que atuem diretamente em vulnerabilidades do mecanismo de confidência do WPA.

O mecanismo de verificação de integridade das mensagens provido pelo WPA é uma adaptação feita sobre o mecanismo provido pelo WEP. Além do campo ICV, é adicionado ao quadro um novo campo de verificação de integridade, denominado *Message Integrity Check* (MIC). O MIC, diferentemente do ICV, é calculado com base em uma chave de integridade, provendo assim mais segurança ao mecanismo de verificação de integridade. Apesar do maior grau de segurança existente na verificação de integridade das mensagens, o WPA possui vulnerabilidades nesse mecanismo que permitem a realização de ataques do tipo *chopchop*, adaptados para o WPA [11] [12]. Tais ataques, quando realizados sobre o WPA, não possuem a mesma eficácia em relação ao protocolo WEP, pois permitem a obtenção de apenas uma parte do texto-plano de alguns pacotes específicos [13].

No entanto, de posse dessa informação, um atacante é capaz de recuperar a chave de integridade utilizada para gerar os campos MIC. Tal chave permite ao atacante forjar mensagens falsas e enviar aos clientes da rede como autênticas.

O protocolo WPA especifica dois métodos de autenticação de usuários na rede: autenticação corporativa e autenticação pessoal. Tais mecanismos serão apresentados detalhadamente no Capítulo 3. Ambos os mecanismos são vulneráveis a diversos ataques, sendo a maioria deles ataques de negação de serviço (*DoS*), que têm por objetivo tornar os recursos da rede indisponíveis. Porém, o mecanismo de autenticação pessoal do WPA também é vulnerável a ataques de derivação indevida das chaves PTK, que permite a um atacante obter as chaves temporárias (PTK) de todos os clientes da rede [14]. Esse é o ataque mais crítico para a segurança do WPA, pois de posse das chaves PTK dos clientes, o atacante é capaz, além de outras coisas, de decifrar mensagens capturadas ou forjar mensagens falsas e enviá-las como autênticas.

2.3 IEEE 802.11I (WPA2)

O padrão IEEE 802.11i (ou WPA2) [3] foi desenvolvido com objetivo de eliminar as diversas vulnerabilidades existentes no protocolo WEP. Como o WPA tem como base uma versão preliminar do IEEE 802.11i, esses protocolos possuem significativas semelhanças, principalmente em seus mecanismos de autenticação. Assim sendo, todas as vulnerabilidades citadas em relação à autenticação do WPA também são válidas para o IEEE 802.11i.

O padrão IEEE 802.11i especifica o uso do protocolo CCMP (*Counter-Mode/CBC-MAC Protocol*) para garantir verificação de integridade e confidência às mensagens trocadas. O CCMP utiliza como algoritmo de criptografia o cifrador de blocos AES *Advanced Encryption Standard*, que é significativamente mais seguro que o RC4, utilizado pelos protocolos WEP e WPA. A verificação de integridade das mensagens no IEEE 802.11i é realizada através de uma função CBC-MAC (*Cipher Block Chaining Message Authentication Code*, especificada pelo CCMP. Até onde se sabe, não existem ataques práticos que explorem vulnerabilidade no mecanismo de verificação de integridade do IEEE 802.11i,

diferentemente dos protocolos WEP e WPA.

2.4 IEEE 802.11W

O IEEE 802.11w [4] é uma emenda ao padrão IEEE 802.11. Tal emenda foi desenvolvida visando prover segurança aos quadros de gerenciamento da rede, que trafegam em texto-plano nos protocolos WPA e WPA2. A troca de quadros de gerenciamento em texto-plano é um dos fatores responsáveis pela possibilidade de criação de ataques de *DoS* nos protocolos WPA e WPA2 durante seus processos de autenticação. Além disso, alguns padrões como IEEE 802.11r, IEEE 802.11u e IEEE 802.11k trafegam informações sensíveis em tais quadros, de modo que se faz necessário garantir-lhes segurança. A emenda IEEE 802.11w pode ser utilizada sobre os padrões WPA e WPA2, evitando assim alguns ataques de negação de serviços durante o processo de autenticação dos clientes à rede.

O IEEE 802.11w utiliza o protocolo BIP (*Broadcast/Multicast Integrity Protocol*) para prover verificação de integridade dos quadros de gerenciamento trocados na rede. Essa proteção se dá através da chave IGTK *Integrity Group Temporal Key*, que é enviada pelo ponto de acesso aos clientes durante o processo de autenticação. Tal emenda, no entanto, ainda possibilita a realização de alguns ataques de *DoS*. Esses ataques ainda são possíveis porque apenas os quadros de gerenciamento são protegidos, no entanto os quadros de controle trafegam em texto-plano. Assim sendo, os ataques de *DoS* que exploram os quadros de controle ainda são efetivos. Além disso, as modificações inseridas pela emenda não interferem na realização dos ataques de derivação indevida da PTK.

CAPÍTULO 3

MECANISMOS DE AUTENTICAÇÃO

Nas redes que IEEE 802.11 que utilizam protocolos de segurança, todos os clientes precisam passar pelo processo de autenticação para ter acesso aos recursos da rede. Esse processo, em geral, permite tanto à rede verificar a autenticidade dos clientes, quanto aos clientes verificarem a autenticidade do ponto de acesso que está servido os recursos. Existem dois métodos de autenticação providos pelos protocolos de segurança WPA, WPA2 e ambos o protocolos utilizando a emenda IEEE 802.11w, são eles a autenticação corporativa e autenticação pessoal. A escolha do método a ser utilizado é feita pelo administrador da rede e depende, em geral, da infraestrutura existente. O método de autenticação corporativa utiliza o padrão IEEE 802.1X, que é descrito a seguir.

3.1 IEEE 802.1X

O padrão IEEE 802.1X possui três entidades participantes: o cliente, o controlador de acesso e o servidor de autenticação. O cliente é a entidade que deseja acessar os recursos da rede; o controlador de acesso, representado pelo ponto de acesso, intermedia a comunicação entre o cliente e o servidor de autenticação; e o servidor de autenticação valida as credenciais do cliente e dá-lhe acesso aos serviços associados à identificação fornecida.

O padrão IEEE 802.1X define o encapsulamento do *Extensible Authentication Protocol* (EAP) sobre redes IEEE 802. Esse encapsulamento, conhecido como EAPOL, foi desenvolvido originalmente para redes *Ethernet* IEEE 802.3 em [15], mas foi adaptado para as redes sem fio IEEE 802.11 em [6]. Durante o processo de autenticação sobre o padrão IEEE 802.1X, o ponto de acesso atua apenas repassando as mensagens trocadas entre o cliente e o servidor de autenticação. A comunicação é realizada sobre um

modo seguro do protocolo EAP, como o EAP-*Transport Layer Security* (EAP-TLS) ou EAP-*Tunneled Transport Layer Security* (EAP-TTLS). Assim sendo, mensagens trocadas nessa comunicação trafegam criptografadas.

Como apresentado na Figura 3.1, inicialmente o cliente requisita se autenticar ao servidor de autenticação e envia-lhe suas credenciais para a verificação de autenticidade. Após a verificação da autenticidade do cliente, o servidor de autenticação envia uma chave *Master Key* (MK), de modo que a MK fica conhecida apenas pelas duas entidades. Com base na chave MK, o cliente e o servidor de autenticação derivam uma nova chave, chamada *Pairwise Master Key* (PMK). A PMK é uma chave simétrica, válida apenas para a seção atual, de modo que uma nova seção exige uma nova chave PMK. Em seguida o servidor de autenticação envia a PMK ao ponto de acesso. A partir dessa etapa o servidor não tem mais participação no processo de autenticação.

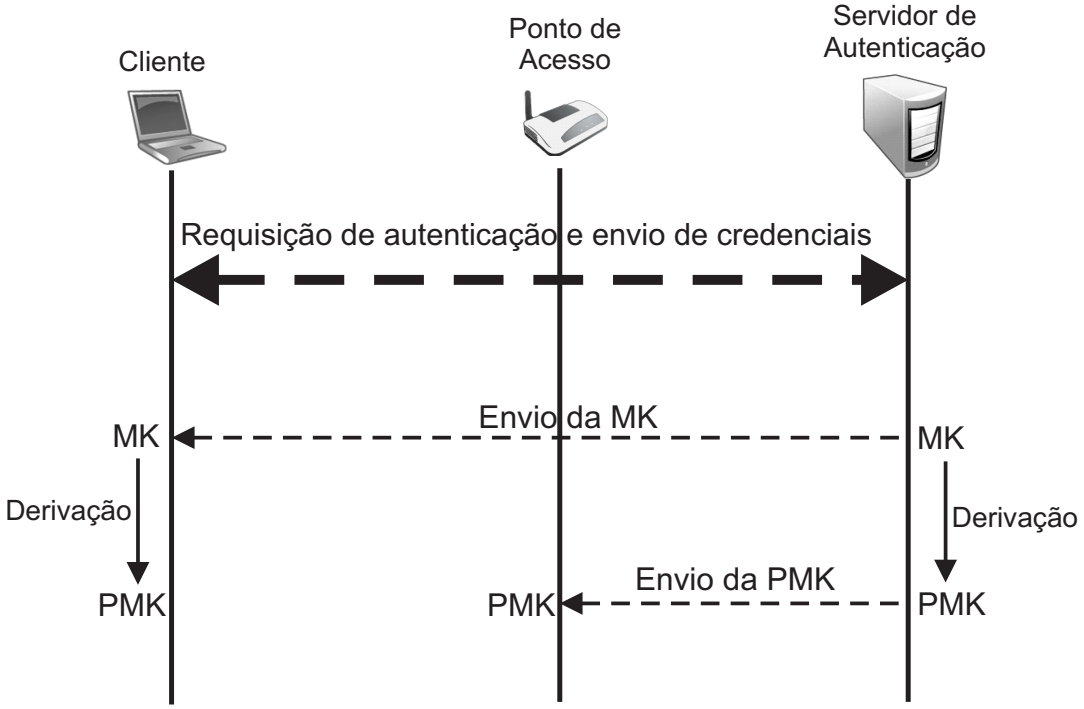

Figura 3.1 Obtenção da PTK pelo cliente e AP através do padrão IEEE 802.1X

3.2 AUTENTICAÇÃO CORPORATIVA

O método de autenticação corporativa é especificado com foco em redes locais de médio e grande porte, como empresas com um significativo número de usuários. Isso ocorre porque, como citado, esse método necessita de um servidor de autenticação, responsável por verificar as credenciais dos clientes. Assim sendo, esse recurso geralmente não é disponível em redes de pequeno porte. Nesse método, inicialmente é feita uma autenticação sobre o padrão IEEE 802.1X, de modo que o cliente e o AP obtêm uma chave PMK em comum. Posteriormente ocorre o processo de *4-Way Handshake*, apresentado na seção 3.4.

3.3 AUTENTICAÇÃO PESSOAL

O método de autenticação pessoal é mais simples que a autenticação corporativa, visto que não há utilização do padrão IEEE 802.1X e, por consequência, do servidor de autenticação. Nesse caso, a autenticação dos usuários é realizada por completo pelo ponto de acesso. Para provar a autenticidade, todos os clientes da rede e o ponto de acesso precisam possuir a chave pré-compartilhada PSK. No entanto, uma mesma chave para todos os clientes da rede não permite que o ponto de acesso autentique os usuários em caráter individual.

O processo de *4-Way Handshake* é o principal mecanismo da etapa de autenticação. Esse processo necessita que o cliente e o ponto de acesso possuam previamente uma chave PMK em comum. Como na autenticação pessoal não há um servidor de autenticação para permitir o cálculo da PMK ao cliente, tal chave é a própria PSK da rede nesse método de autenticação. O processo de *4-Way Handshake* ocorre de modo idêntico nos dois métodos de autenticação.

3.4 4-WAY HANDSHAKE

O *4-Way Handshake* existe tanto no método de autenticação pessoal quanto no método de autenticação corporativa oferecidos pelos protocolos WPA, WPA2 e nas modificações

destes introduzidas pelo IEEE 802.11w. Seu objetivo é autenticar mutuamente o cliente e o ponto de acesso, permitindo, entre outras coisas, que ambos derivem uma chave PTK comum e exclusiva a eles. A PTK é um conjunto de chaves temporárias de extrema importância para garantir segurança aos clientes da rede. As chaves que compõem a PTK permitem, entre outras coisas, criptografia de quadros enviados em *unicast* e verificação da integridade dos mesmos. Durante o *4-Way Handshake*, o ponto de acesso também envia ao cliente, em texto-cifrado, a chave GTK (*Group Temporal Key*). Caso a emenda IEEE 802.11w estiver sendo utilizada, também é enviada uma chave IGTK (*Integrity Group Temporal Key*). A GTK e a IGTK são chaves comuns a todas as entidades da rede. A GTK tem por objetivo criptografar e verificar a integridade dos quadros enviados em *broadcast* e *multicast*. A IGTK é utilizada pela emenda IEEE 802.11w para prover integridade aos quadros de gerenciamento.

Dependendo da configuração da rede, o *4-Way Handshake* pode sofrer pequenas variações no conteúdo das mensagens. Contudo, a essência do processo é a mesma. A Figura 3.2 ilustra o *4-Way Handshake*, resumindo os principais parâmetros usados em comum nos protocolos WPA, WPA2 e nas modificações desses dois protocolos feitas pelo IEEE 802.11w. Na figura é apresentado o *4-Way Handshake* considerando a utilização da emenda IEEE 802.11w, no entanto, no caso da ausência de tal emenda, não há existência das chaves IGTK no *handshake*. Nesse processo, o cliente (S) e o ponto de acesso (A) trocam quatro mensagens. Os principais parâmetros enviados são: *nonce* do cliente ($SNonce$); endereço MAC do cliente (AS); *nonce* do ponto de acesso ($ANonce$); endereço MAC do ponto de acesso (AA); os campos de verificação de integridade das mensagens (MIC); e as chaves GTK e IGTK, encriptadas com a KEK (*Key Encryption Key*), que é uma das chaves pertencentes a PTK.

O valor do MIC é calculado com base na KCK (*Key Confirmation Key*), que também é uma das chaves que compõem a PTK. Esse campo é utilizado para verificar se a mensagem não foi adulterada após ser enviada. Os *Nonces* são números gerados aleatoriamente, tendo o objetivo de permitir que a chave PTK derivada seja diferente a cada novo processo de *handshake*. A derivação da chave PTK é feita após o recebimento do endereço

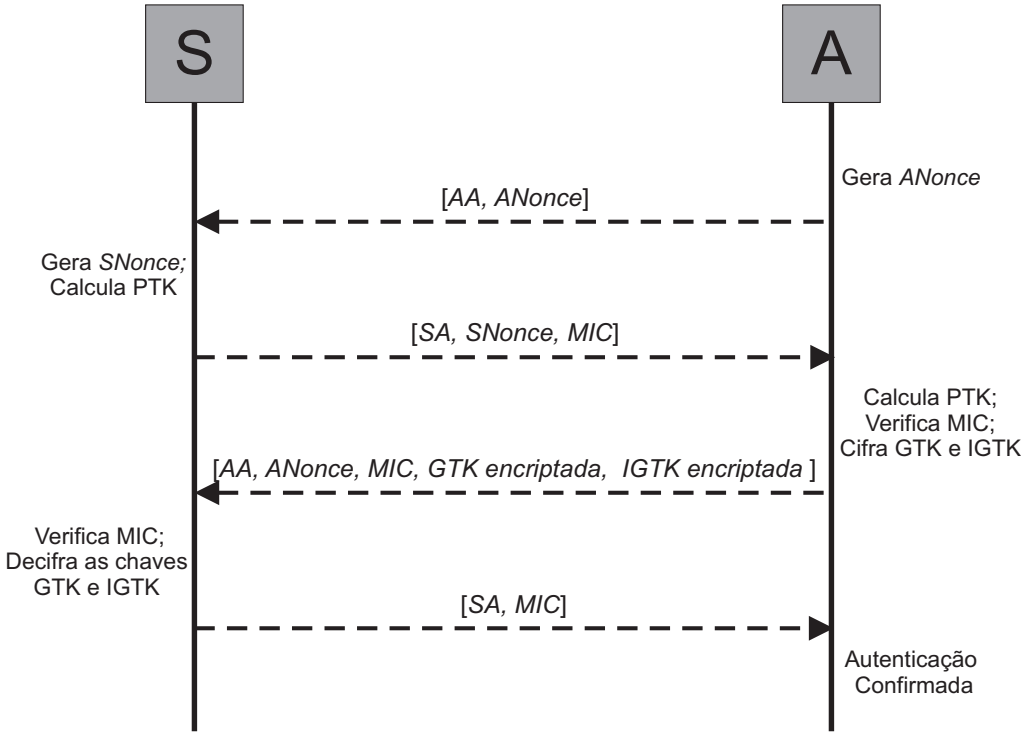

Figura 3.2 *4-Way Handshake*

MAC e do *Nonce* da outra entidade comunicante. Essa derivação é feita utilizando-se uma função pseudoaleatória (*Pseudo Random Function* - PRF) [3] de tal forma que:

$$\text{PTK} = \text{PRF}(\text{PMK}, \text{“}\textit{Pairwise key expansion}\text{”}, Min(AA, SA) \,||\, Max(AA, SA) \,||\, Min(ANonce, SNonce) \,||\, Max(ANonce, SNonce)).$$

No caso do método de autenticação ser o pessoal, a PMK (*Pairwise Master Key*) utilizada como parâmetro para a PRF é a própria PSK. Caso o método de autenticação seja o corporativo, a PMK é obtida como apresentado na Seção 3.1. Após a obtenção da chave PMK, inicia-se o *4-Way Handshake* entre o cliente e o ponto de acesso.

A possibilidade de derivação indevida da chave PTK é um problema que afeta o WPA, o WPA2 e esses dois padrões com a emenda IEEE 802.11w quando o método de autenticação pessoal é utilizado. Isso ocorre pelo seguinte: um dos parâmetros da função de derivação da PTK é a *string* “*Pairwise key expansion*”, que possui valor fixo. Dentre os outros argumentos que são aplicados à PRF, apenas a chave PMK não trafega em claro através das mensagens trocadas. Como no método de autenticação pessoal a PMK

é a própria PSK, uma entidade maliciosa que possua a PSK poderá derivar a chave PTK de todos os outros clientes da rede apenas escutando o canal durante os *handshakes* para a obtenção dos parâmetros necessários ao cálculo da PTK [16].

Mesmo que uma entidade maliciosa não pertença à rede e não possua a PSK, ainda assim é possível encontrá-la capturando-se mensagens do *4-Way Handshake* e realizando-se um ataque de dicionário. Esse ataque é praticável somente se a *passphrase* usada na criação da PSK possuir poucos caracteres ou for formada por conteúdo previsível [14] [17]. Nesse caso a vulnerabilidade não é considerada do protocolo de segurança, mas sim uma falha do usuário/administrador.

3.5 GROUP KEY HANDSHAKE

O padrão IEEE 802.11i especifica dois processos de *handshake* que permitem a distribuição de chaves GTK: o *4-Way Handshake* e o *Group Key Handshake*. O segundo processo, no entanto, tem por objetivo distribuir uma nova chave GTK a todos os clientes da rede sem a necessidade de reautenticar todos os clientes. Em geral, cada vez que um cliente sai da rede, o ponto de acesso realiza um processo de *Group Key Handshake* para distribuir novas chaves GTK a todos os clientes. Desse modo, os cliente que saíram da rede não terão mais acesso aos quadros enviados em *broadcast* ou *multicast*.

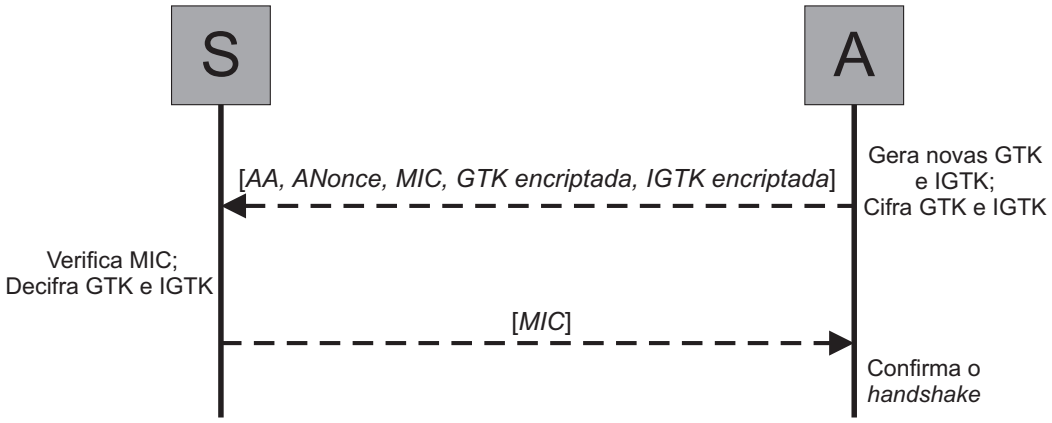

Figura 3.3 *Group Key Handshake*

O *Group Key Handshake* ocorre apenas após o processo de *4-Way Handshake*, visto

que a GTK distribuída é cifrada com uma das chaves que compõem a PTK, obtida através do *4-Way Handshake*. No *Group Key Handshake*, o cliente (S) e o ponto de acesso (A) trocam apenas duas mensagens, como apresentado na Figura 3.3. Em tal figura é apresentado o *Group Key Handshake* considerando a utilização da emenda IEEE 802.11w, no entanto, no caso da ausência de tal emenda, não há existência das chaves IGTK. A primeira mensagem é utilizada para enviar a GTK cifrada ao cliente e a segunda mensagem é a confirmação de que o cliente recebeu corretamente tal chave. Vale ressaltar que a GTK trafega encriptada no *4-Way Handshake* e no *Group Key Handshake*, de modo que uma entidade não pertencente à rede não consegue obtê-la sem possuir previamente a PTK. No entanto, caso o atacante esteja autenticado na rede, ele também receberá a GTK do ponto de acesso, visto que essa chave é comum a todas as entidades autenticadas.

3.6 HIERARQUIA DE CHAVES

A PTK e a GTK consistem em conjuntos hierárquicos de chaves temporárias, apesar de serem usualmente conhecidas como chave PTK e chave GTK, respectivamente. Ao serem obtidas pelas entidades comunicantes, tais chaves são subdivididas em chaves menores, cada uma com finalidade específica.

A Figura 3.4 apresenta as chaves que compõem a PTK. O tamanho e a estrutura da chave PTK depende do protocolo de cifra utilizado. O WPA utiliza o TKIP e, tradicionalmente o WP2 utiliza apenas o CCMP como protocolo de cifra. No entanto, existem implementações que permitem que o WPA2 utilize o TKIP em conjunto com o CCMP. A emenda IEEE 802.11w necessita ser utilizada conjuntamente com o WPA ou com WPA2, assim sendo, a hierarquia da PTK segue o modelo utilizado por tais protocolos. A seguir são descritas a função de cada uma das chaves que compõem a PTK:

- KCK (*Key Confirmation Key*): Chave utilizada na verificação da integridade dos quadros, através do campo MIC, durante os processos de *4-Way Handshake* e *Group Key Handshake*;
- KEK (*Key Encryption Key*): Chave utilizada para cifrar as chaves GTK e IGTK

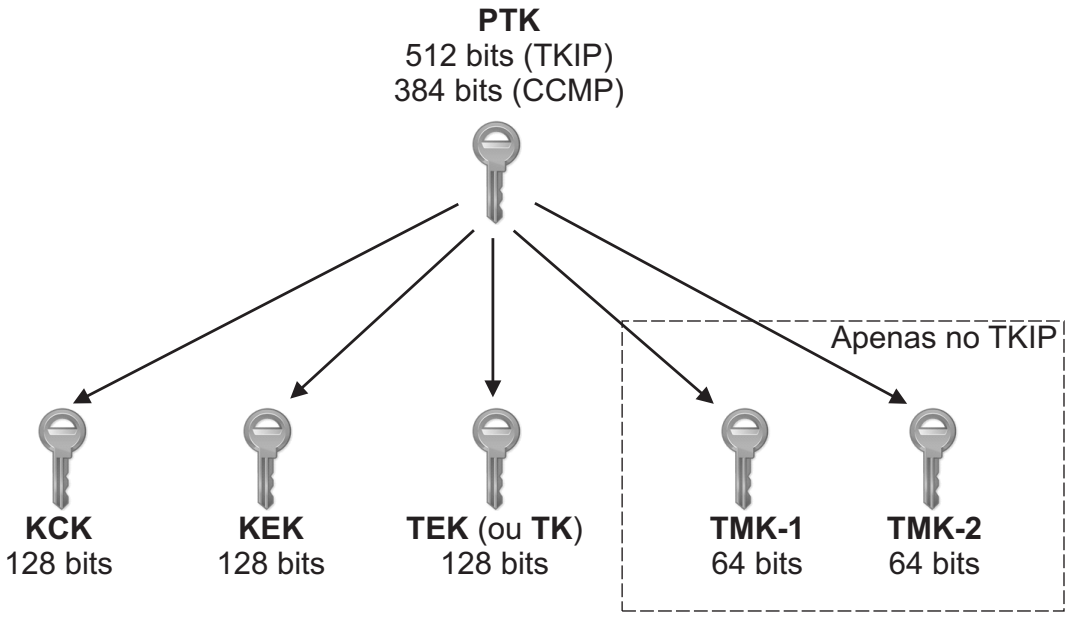

Figura 3.4 Chaves que compõem a PTK

durante o *4-Way Handshake* e o *Group Key Handshake*;

- TEK (*Temporary Encryption Key*) ou TK (*Temporary Key*): Chave utilizada para cifrar e decifrar quadros trocados em *unicast* pelas entidades da rede;
- TMK-1 e TMK-2 (*Temporary MIC Key*): Chaves utilizadas apenas pelo TKIP para prover verificação de autenticidade dos quadros. Cada chave é utilizada por um lado da comunicação. O CCMP não necessita dessas chaves para tal finalidade, visto que ele insere o campo de verificação de integridade através de uma função CBC-MAC juntamente com o processo de cifragem.

As chaves que compõem a GTK são apresentadas na Figura 3.5. Tal estrutura é mais simples que a PTK, porém, de modo similar também depende do protocolo utilizado. A seguir são descritas as chaves que compõem a GTK:

- GEK (*Group Encryption Key*): Chave utilizada para cifrar os quadros enviados em *broadcast* e *multicast*;

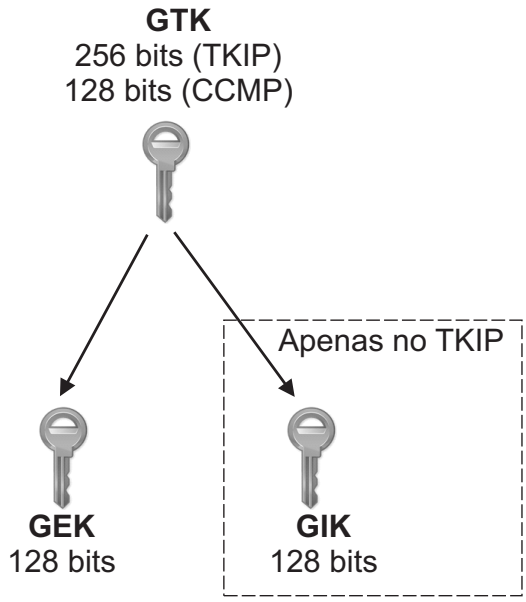

Figura 3.5 Chaves que compõem a GTK

- GIK (*Group Integrity Key*): Chave utilizada pelo TKIP para prover integridade aos quadros trocados em *broadcast* e *multicast*.

CAPÍTULO 4

PROTOCOLOS DE ACORDO DE CHAVES SEGURAS

Neste capítulo são apresentados dois protocolos de acordo de chaves seguras entre entidades remotas. Uma característica importante é que, mesmo que o canal de comunicação seja inseguro, a chave acordada entre as entidades comunicantes não é revelada. Assim sendo, todas as informações trocadas pelas podem ser capturadas por qualquer entidade maliciosa, mas, ainda assim, a segurança do protocolo é mantida. Um dos protocolos apresentados é utilizado como base pelos trabalhos relacionados e o outro é utilizado pela proposta deste trabalho.

4.1 DIFFIE-HELLMAN (DH)

No ano de 1976, Whitfield Diffie e Martin Hellman propuseram o primeiro método prático para estabelecimento de chaves secretas sobre um meio inseguro. Esse protocolo [18] é conhecido atualmente como Diffie-Hellman. A segurança de tal proposta reside na dificuldade de se resolver uma instância do problema do logaritmo discreto, que é um problema da classe de problemas NP equiparável ao problema de fatoração de inteiros.

O problema do logaritmo discreto (PLD) é aplicado a grupos cíclicos, ou seja, grupos que podem ser gerados por um único elemento. Dado um grupo cíclico $\mathbb{G}$ e dois elementos g e y pertencentes a $\mathbb{G}$, o problema do logaritmo discreto consiste em encontrar um inteiro x, tal que $y = g^x$, ou seja, encontrar o $\log_g y$. Assumindo que p é um número primo que representa ordem do grupo, tem-se que $\log_g y \equiv x \pmod{p}$.

Sejam duas entidades remotas S e A, o protocolo Diffie-Hellman é realizado da seguinte forma:

1. Um número primo p é tornado público, bem como um valor g, gerador do grupo

cíclico em questão. Esses valores podem ser definidos por uma das entidades comunicantes;

2. A entidade A gera uma chave privada pseudoaleatória k_A e calcula sua chave pública $P_A = g^{k_A} \pmod{p}$;

3. Similarmente, a entidade S gera uma chave privada pseudoaleatória k_S e calcula sua chave pública $P_S = g^{k_S} \pmod{p}$;

4. As entidades trocam suas chaves públicas P_A e P_S;

5. A entidade A calcula a chave $K = P_S^{k_A} \pmod{p}$ e a entidade S calcula $K = P_A^{k_S} \pmod{p}$.

A chave K calculada entre ambas as entidades são iguais a $g^{k_A \times k_S} \pmod{p}$. Um adversário que escute o tráfego do canal de comunicação estará impossibilitado de descobrir o valor da chave K. Essa segurança é garantida, pois se faz necessário o conhecimento de, ao menos, o valor de k_A ou k_S para que se possa obter o valor de K.

Algumas considerações devem ser feitas a respeito dos valores k_A, k_S, g e p para que o mecanismo de derivação de chaves possa ser considerado difícil de ser invertido em relação a sua complexidade computacional. A variável p devem ser um número primo, além de que $(p-1)/2$ também deve ser um número primo [19]. Considerando o poder computacional dos computadores atuais, protocolos que tem sua segurança baseada na infactibilidade de resolução em tempo hábil do PLD apenas são considerados seguros com p maiores que 1024 bits [20]. Os valores de k_A e k_S devem pertencer ao grupo cíclico, ou seja, devem ser inteiros menores que p. O inteiro g deve ser um gerador do grupo e deve ser uma raiz primitiva do módulo p. Assim sendo, a ordem multiplicativa de $g \pmod{p}$ deve ser $\phi(n)$, onde ϕ é a função totiente [Lehmer 1932]. A função totiente de n representa a quantidade de números menores que n que são co-primos de n.

Como citado, o protocolo Diffie-Hellman baseia-se na dificuldade de resolver o PLD. A dificuldade de se quebrar a segurança do protocolo e obter as chaves K em tempo hábil apenas escutando-se o canal de comunicação é equivalente à dificuldade de resolver,

em tempo polinomial, qualquer instância do PLD. Atualmente, existem algoritmos que resolvem o PLD em tempo subexponencial em relação à ordem do grupo cíclico. Em geral, esses algoritmos são variações do método apresentado em [21]. Um algoritmo que executa em tempo subexponencial, quando aplicado a uma instância do PLD de ordem elevada, ainda assim é inviável do ponto de vista prático. Apesar da existência desses algoritmos não quebrar totalmente a segurança dos mecanismos baseados em DH, tais mecanismos já possuem sua segurança ameaçada.

4.2 DIFFIE-HELLMAN SOBRE CURVAS ELÍPTICAS (ECDH)

Em 1985 foi proposta a primeira utilização de curvas elípticas em sistemas criptográficos. Tal proposição, feita independente por Neal Koblitz e Victor Miller, está sendo cada vez mais utilizada em sistemas de segurança computacional. A criptografia de curvas elípticas (*Elliptic Curve Cryptography* - ECC) permitiu a criação de diversos novos mecanismos de segurança, além da adaptação de mecanismos já existentes. Um grande exemplo de mecanismo já existente, mas que foi adaptado para um modelo baseado em curvas elípticas, é o protocolo Diffie-Hellman.

O protocolo Diffie-Hellman sobre Curvas Elípticas (*Elliptic Curve Diffie-Hellman* - ECDH) tem sua segurança baseada na dificuldade de se resolver o Problema do Logaritmo Discreto sobre Curvas Elípticas (PLDCE). Uma curva elíptica sobre um campo finito F é o conjunto de pontos $\mathrm{P}(x, y)$ juntamente com um ponto no infinito, onde as variáveis x e y satisfazem uma equação de *Weierstrass* [22] dada por:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \tag{4.1}$$

As variáveis e os coeficientes pertencem ao campo finito F. Para curvas elípticas sobre campos finitos gerados por números primos, a Equação 4.1 pode ser simplificada, desde que não possua raízes múltiplas, tomando a forma da Equação 4.2. A inexistência de raízes múltiplas é garantida para $4a_4^3 + 27a_5^2 \neq 0$.

$$y^2 = x^3 + a_4x + a_5 \tag{4.2}$$

A Figura 4.1 ilustra a adição de pontos sobre uma curva elíptica. Sejam dois pontos distintos $P_1(x_1, y_1)$ e $P_2(x_2, y_2)$ pertencentes a uma curva elíptica E. Uma reta L que atravessa P_1 e P_2 é traçada de forma que a mesma intercepte um terceiro ponto P_3. Ao refletir P_3 em relação ao eixo x se obtém um ponto $P_4 = P_1 + P_2$. Caso $P = P_1 = P_2$, então a reta traçada é tangente a E no ponto P.

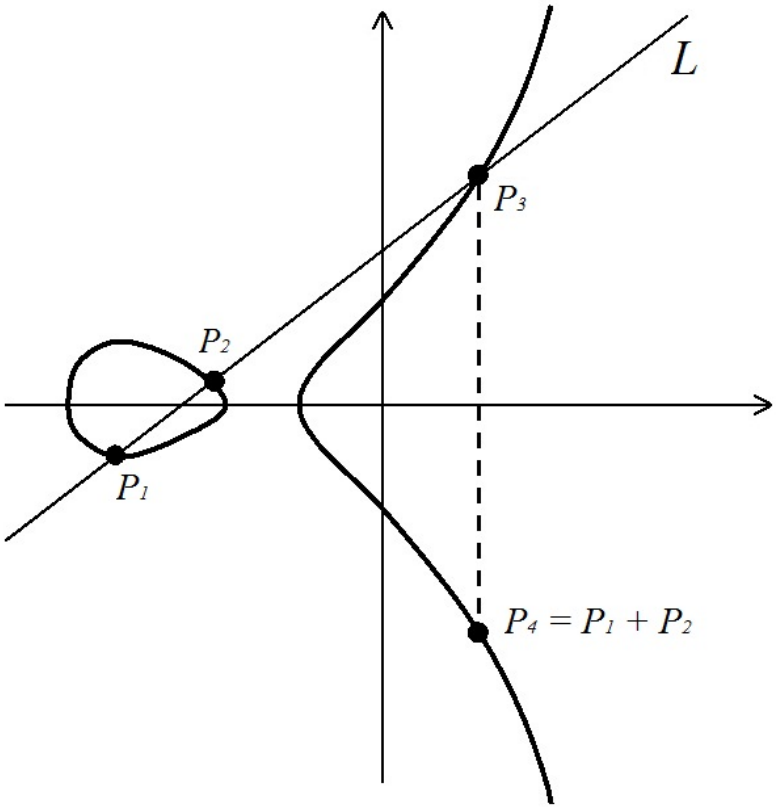

Figura 4.1 Adição entre pontos sobre curvas elípticas

Uma curva elíptica E é um grupo abeliano por uma operação de adição. Assim sendo, a exponenciação de um ponto em E é computado através de operações de adições repetidas. A n-ésima potência de P, para $P \in E$, é igual ao n-ésimo múltiplo de P. Sendo o n-ésimo múltiplo de P representado por Q, isso significa que $Q = P^n = nP$, onde $Q \in E$. A resolução do problema do PLDCE consiste em se determinar o logaritmo de Q na base P.

Para que o acordo de chaves possa ser feito entre duas entidades A e S utilizando-

se o protocolo EDCH, inicialmente devem ser conhecidos os parâmetros de domínio. Esses valores podem ser definidos por uma das entidades comunicantes no início de cada comunicação, porém também podem ser fixos. Tais parâmetros consistem em um campo finito, que pode ser um *campo de Galois* primo ($GF(p)$) ou binário ($GF(2^m)$); uma curva E sobre o campo finito; e um ponto base G pertencente à curva. Em função dos parâmetros de domínio, duas entidades A e S realizam o acordo da chave K da seguinte forma:

1. A entidade A gera uma chave privada pseudoaleatória k_A, que é um inteiro pertencente ao campo, e calcula sua chave pública $P_A = k_A \times G$, que é um ponto em E;

2. Similarmente, a entidade S gera uma chave privada pseudoaleatória k_S e calcula sua chave pública $P_S = k_S \times G$;

3. As entidades trocam suas chaves públicas P_A e P_S;

4. A entidade A calcula a chave $K = k_A \times P_S$ e a entidade S calcula $K = k_S \times P_A$.

Desse modo, ambas as entidades derivam a chave $K = k_A \times P_S = k_S \times P_A = k_A \times (k_S \times G) = k_S \times (k_A \times G)$, onde K é um ponto pertencente à curva elíptica E. Esse protocolo permite um acordo de chaves de forma segura mesmo que o canal de comunicação seja inseguro. Assim como no DH, para uma entidade maliciosa calcular K, é necessário que ela conheça ao menos uma das chaves privadas. Como essa informação é mantida em sigilo, o cálculo de K em função apenas das chaves públicas P_A e P_S torna-se inviável.

4.3 DH X ECDH

A utilização de criptossistemas baseados em curvas elípticas, como o ECDH, tem crescido expressivamente nos mecanismos de segurança computacional. Isso ocorre devido ao grau de segurança provido em relação à quantidade de recursos computacionais requeridos. Comparado às abordagens baseadas em logaritmo discreto e fatoração de inteiros, o ECDH necessita de uma quantidade significativamente menor de recursos como, por

Tabela 4.1 Tamanho das chaves públicas (em bits) para prover um grau de segurança equivalente

DH	ECDH
1.024	163
3.072	283
7.680	409
15.360	571

exemplo: tamanho de parâmetros e chaves; tempo processamento; e espaço de armazenamento [23], [24].

Atualmente os ataques mais eficientes para ECDH executam em tempo exponencial [25]. No entanto, existem ataques ao protocolo DH que executam em tempo subexponencial [21] [26]. A Tabela 4.1 apresenta uma comparação entre o tamanho de chaves em sistemas baseados em ECDH e DH para proverem um grau de segurança equivalente [23]. Além das chaves no ECDH serem substancialmente menores para um mesmo grau de segurança, à medida que se necessita elevar a segurança do sistema, o tamanho das chaves no DH cresce expressivamente mais rápido. Com o crescimento do tamanho de chaves públicas, eleva-se também o tempo de processamento requerido para o cálculo das chaves acordadas entre as entidades.

CAPÍTULO 5

TRABALHOS RELACIONADOS

O problema de derivação indevida da PTK não vem recebendo a devida atenção por parte do IEEE. Além disso, até onde se sabe, existem apenas dois trabalhos na literatura que buscam soluções para esse problema [27] [28]. Dentre os trabalhos citados, a solução apresentada em [28] foi proposta também pelo autor desse trabalho de graduação.

Em [27] é proposta uma adaptação no *4-Way Handshake* do WPA-PSK que soluciona o problema de derivação indevida da chave PSK. Essa proposta se baseia no protocolo de acordo de chaves Diffie-Hellman. A Figura 5.1 apresenta o funcionamento, de forma geral, do mecanismo apresentado em [27]. Em tal proposta, as duas primeiras mensagens do *4-Way Handshake* são cifradas através da chave mestra PMK. Além disso, tais mensagens trocadas também permitem que as duas entidades derivem, através do protocolo DH, uma chave em comum, denominada DPMK (*Dynamic Pairwise Master Key*). Essa chave fica sendo conhecida apenas pelo cliente em autenticação e pelo AP e é utilizada em substituição da PMK durante a derivação da PTK. Isso impede que qualquer entidade maliciosa que possua a PMK derive a PTK de outros clientes da rede. A DPMK também é utilizada para cifrar as duas últimas mensagens do *4-Way Handshake* do WPA-PSK.

Nessa proposta a PMK é utilizada para cifrar as duas primeiras mensagens do *handshake*. Isso não é recomendado, pois a chave mestra está sendo utilizada diretamente na criptografia de informações e de forma repetida a cada *handshake*. Essa proposta também possui como ponto negativo o fato de ser baseada no protocolo DH que, como apresentado no Capítulo 4, possui problemas relacionados ao grau de segurança provido e aos recursos computacionais requeridos.

Em [28] é proposto um mecanismo que estende o *4-Way-Handshake* do WPA2-PSK, solucionando o problema de derivação indevida da PTK. Essa proposta também se baseia

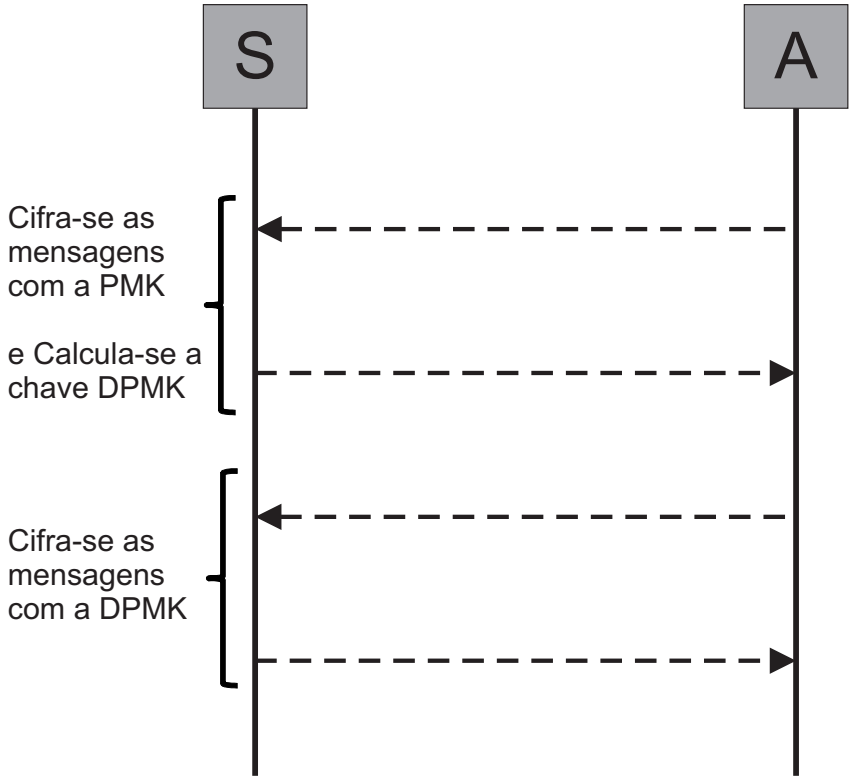

Figura 5.1 Descrição geral do trabalho relacionado 1

no problema do logaritmo discreto e no protocolo de derivação de chaves DH. A Figura 5.2 apresenta, de modo geral, o funcionamento do mecanismo proposto em tal trabalho. Nessa proposta, duas novas mensagens são incluídas no início do *handshake* entre o cliente e o ponto de acesso. Essas duas primeiras mensagens servem para que as duas entidades comunicantes derivem uma chave K com base no protocolo DH. Essa chave é utilizada apenas para cifrar os *Nonces* trocados entre as entidades.

As quatro últimas mensagens do *handshake* são exatamente iguais às mensagens do *handshake* tradicional, exceto pelo fato de que os *Nonces* trafegam cifrados. A proposta soluciona o problema de derivação indevida da PTK, pois mesmo que uma entidade maliciosa conheça a PMK, ela não terá como conhecer o texto-plano dos *Nonces* utilizados como argumentos no cálculo da PTK.

Diferentemente dos trabalhos relacionados, este trabalho propõe uma adaptação no *4-Way Handshake* como solução ao problema de derivação indevida da PTK tendo como

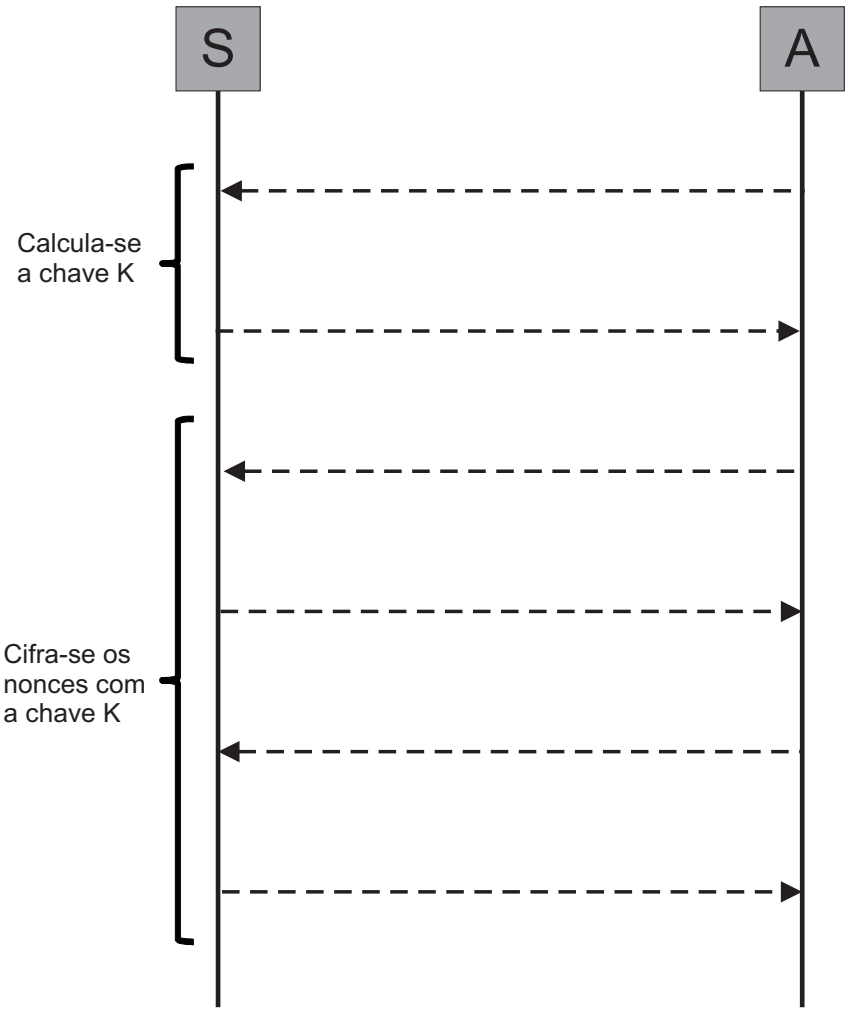

Figura 5.2 Descrição geral do trabalho relacionado 2

base o protocolo Diffie-Hellman sobre Curvas Elípticas (ECDH). O objetivo é prover um maior grau de segurança e reduzir a quantidade de recursos computacionais no processo de derivação de chaves sem aumentar o número de mensagens do *4-Way Handshake* e sem aumentar significativamente duração deste. Além disso, este trabalho foca em prover uma solução que possa ser utilizada nos protocolos WPA, WPA2 e nas versões destes dois protocolos acrescidas pelo IEEE 802.11w. Também de forma diferente dos trabalhos relacionados, este trabalho avalia experimentalmente o impacto da solução proposta em termos da duração do *handshake* e do aumento médio no tamanho de mensagens trocadas durante o mesmo.

Além das fraquezas do protocolo DH, o uso desse protocolo introduz um *overhead* de processamento significativo quando comparado ao uso do protocolo ECDH [24]. Assim, o uso do protocolo DH durante o *handshake* não é adequado em cenários onde os dispositivos necessitem realizar *handoffs* constantes já que, nesses casos, é necessário um tempo de autenticação baixo. O tamanho elevado de chaves públicas do DH requer o uso de dispositivos com poder computacional elevado, além de aumentar o consumo de energia e memória [24]. Isso é um fator relevante principalmente para dispositivos com baixa capacidade computacional. Uma comparação entre os *overheads* inseridos ao *handshake* pelos trabalhos relacionados e o *overhead* da proposta desse trabalho é apresentada no Capítulo 7, através da avaliação experimental da proposta.

CAPÍTULO 6

PROPOSTAS

Neste capítulo serão apresentadas as duas propostas desse trabalho. Os mecanismos propostos consistem em adaptações do *4-Way handshake* para uso do protocolo de acordo de chaves ECDH. Doravante, o *4-Way Handshake* adaptado será denominado *Improved Handshake* (IH). Primeiramente o IH, descrito na Seção 6.1, possui objetivo de eliminar o problema da derivação indevida das chaves PTK. Em seguida, a Seção 6.2 apresenta uma adaptação do IH para prover autenticação aos usuários das redes IEEE 802.11 abertas.

6.1 IMPROVED HANDSHAKE

Para que o cliente e o ponto de acesso possam realizar o processo de IH, ambas as entidades precisam conhecer os parâmetros de domínio, descritos na Seção 4.2, os quais definem a curva elíptica a ser utilizada. Em particular, o IH propõe a utilização das chaves públicas do ECDH também como *Nonces*. Nessa proposta, os parâmetros de domínio são fixos e públicos, ou seja, o protocolo define seus valores de modo que as entidades que realizam o processo de *Improved Handshake* os conhecem previamente. Definir previamente tais valores não compromete a segurança do sistema, visto que a reutilização de curvas elípticas em ECC não resulta na possibilidade de realização de ataques [26]. Além disso, todas as curvas utilizadas nesta proposta são recomendadas pelo NIST (*National Institute of Standards and Technology*) como curvas elípticas de elevado grau de segurança. Por outro lado, o conhecimento prévio de tais parâmetros pelas entidades comunicantes elimina a necessidade de comunicação para acordo destas informações, reduzindo assim o *overhead* do sistema. A escolha de uma curva elíptica adequada para o *Improved Handshake* é apresentada no Capítulo 7.

Durante o *Improved Handshake*, o cliente (S) e o ponto de acesso (A) definem suas chaves públicas (*Spub* e *Apub*) e privadas (*Spriv* e *Apriv*) com base na curva elíptica. Tradicionalmente, a chave acordada entre as duas entidades no ECDH representa um ponto sobre a curva elíptica, porém para o IH é necessário que a chave secreta seja um número inteiro. Para estes casos, em [20] é recomendado que a chave secreta seja apenas a coordenada x de tal ponto. Seguindo tal recomendação, o IH utiliza o ECDH para acordar a chave Ke entre o cliente e o ponto de acesso. Tal chave é utilizada juntamente com a PMK para derivação da PTK.

Além do cálculo de Ke, as chaves públicas *Spub* e *Apub* são utilizadas como *Nonces* (respectivamente, $SNonce$ e $ANonce$ do *4-Way Handshake*). As chaves públicas possuem característica pseudoaleatória, visto que são calculadas em função das chaves privadas, que são geradas de forma pseudoaleatória. A característica pseudoaleatória das chaves públicas permite as permitem ser utilizadas como *Nonces*, pois o objetivo de gerar diferentes chaves PTK a cada *handshake* é mantido. Assim como no *4-Way Handshake*, os endereços físicos SA e AA do cliente e do ponto de acesso são utilizados pelo IH para o cálculo da PTK.

A Figura 6.1 ilustra o *Improved Handshake*. Essa figura apresenta somente os campos das mensagens que são utilizados diretamente pelo *Improved Handshake*. Os círculos numerados representam as ações realizadas pelas entidades em cada etapa do acordo de chaves. Essas ações são descritas a seguir:

1. O ponto de acesso A gera *Apriv* e calcula *Apub* com base em *Apriv* e nos parâmetros de domínio;

2. O cliente S gera *Spriv* e calcula *Spub* com base em *Spriv* e nos parâmetros de domínio;
   O cliente S calcula Ke com base em *Apub*, *Spub* e *Spriv*;
   O cliente S deriva a PTK;

3. O ponto de acesso A calcula o MIC e verifica a integridade da mensagem de S;
   O ponto de acesso A calcula Ke com base em *Spub*, *Apub* e *Apriv*;

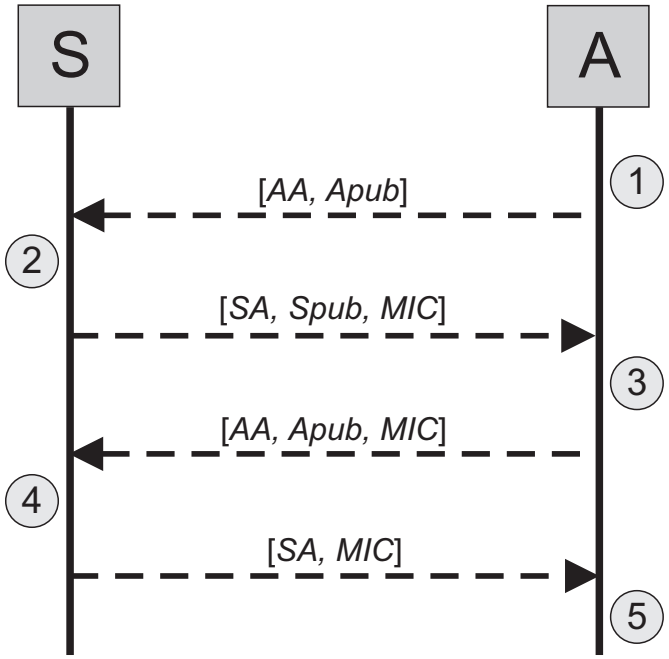

Figura 6.1 *Improved Handshake*

O ponto de acesso A deriva a PTK;

4. O cliente S calcula o MIC e verifica a integridade da mensagem de A;

5. Autenticação finalizada. Ambas as entidades possuem uma PTK em comum.

Para a derivação da PTK na proposta deste trabalho, a função pseudoaleatória utilizada para o cálculo da PTK recebe os argumentos PMK, Ke, AA, SA, $Apub$, $Spub$ e uma *string* de diferenciação fixa, de modo que:

$$\text{PTK} = \text{PRF}(PMK,\ Ke,\ \text{“}\textit{Elliptic pairwise key expansion}\text{”},\ Min(AA, SA)\ ||\ Max(AA, SA)\ ||\ Min(Apub, Spub)\ ||\ Max(Apub, Spub)).$$

Para um atacante que conheça previamente a chave PMK, ao escutar o tráfego da rede durante o *Improved Handshake* serão obtidos todos os argumentos da PRF, exceto Ke. Isso ocorre pelo fato dos endereços físicos e das chaves públicas trafegarem em claro na rede. No entanto, o desconhecimento de Ke impossibilita a derivação da PTK.

Vale ressaltar que, apesar de não ser apresentado na descrição do *Improved Handshake*, ainda existe o envio da GTK durante esse processo da mesmo forma que ocorre no *4-Way*

Handshake. Além disso, caso o *Improved Handshake* seja utilizado juntamente à emenda IEEE 802.11w, a chave IGTK também é enviada em texto-cifrado pelo ponto de acesso ao cliente. A descrição do *Improved Handshake* omitiu tais informações pois este trabalho não propõe qualquer modificação em tais chaves ou na forma como elas são derivadas.

Atualmente não são conhecidos problemas que permitam a realização de ataques de derivação indevida da PTK em redes que usam o método de autenticação corporativo. Entretanto, como o *Improved Handshake* é inerentemente mais seguro do que o *4-Way Handshake*, o *handshake* proposto se torna mais adequado também para esse tipo de rede. O método de autenticação corporativa apenas distingue da autenticação pessoal na forma de obtenção da PMK, porém para o processo de *handshake* é indiferente a forma como tais chaves foram obtidas. Deste modo, o IH pode ser utilizado na autenticação corporativa sem a necessidade de configurações adicionais.

6.2 IMPROVED HANDSHAKE EM REDES ABERTAS

Este trabalho também possui objetivo de solucionar o problema da falta de autenticação nas redes abertas. Com essa finalidade o *Improved Handshake* foi adaptado para tais redes. Com uma pequena modificação no cálculo da PTK, o *Improved Handshake* pode ser utilizado para prover autenticação automática em redes abertas sem a necessidade do fornecimento de chaves pelos usuários. Deste modo, mesmo sem possuir previamente uma chave de segurança, o cliente e o ponto de acesso acordam chaves PTK seguras. De posse da PTK as entidades comunicantes são agora capazes de enviar quadros na rede com a devida confidência e verificação de integridade.

O *Improved Handshake* para redes abertas possui a mesma estrutura de mensagens anteriormente proposta, apresentada na figura Figura 6.1. No entanto, para redes abertas há diferença nos argumentos da função de derivação da PTK. Nesse caso, a PTK é derivada de modo que:

$$\text{PTK} = \text{PRF}(Ke, \text{“}\textit{Elliptic pairwise key expansion}\text{”}, Min(AA, SA) \mid\mid Max(AA, SA) \mid\mid Min(ANonce, SNonce) \mid\mid Max(Apub, Spub)).$$

Note que a PMK não participa da derivação, visto que tal chave não existe em redes abertas.

A segurança da PTK é garantida em decorrência da derivação da chave Ke ser baseada no PLDCE, cujas soluções existentes executam apenas em tempo exponencial. Deste modo, mesmo sem a utilização da chave PMK, o *Improved Handshake* para redes abertas é seguro contra ataques de derivação indevida da PTK. Por consequência da derivação da PTK nas redes abertas, as entidades da rede podem realizar o processo de *Group Key Handshake* e acordar chaves GTK e IGTK. Isso se tornou possível porque as entidades agora possuem as chaves KEK, utilizadas para cifrar as chaves GTK e IGTK.

CAPÍTULO 7

AVALIAÇÃO EXPERIMENTAL

Esse capítulo avalia o impacto do *Improved Handshake* em termos do aumento médio no tamanho de mensagens trocadas e duração do mesmo em relação ao *4-Way Handshake* tradicional. A duração média do *handshake* considera apenas o processo de *handshake* propriamente dito, ou seja, desconsiderada as etapas externas a esse mecanismo durante a autenticação, como o envio de *probes*. As mensagens do *4-Way Handshake* seguem o padrão *EAPOL-Key frames* [3], de modo que seus tamanhos podem sofrer variações dependendo do contexto e do tipo de mensagem. No entanto, para fins comparativos com o mecanismo proposto, foi calculado o tamanho médio das mensagens do *4-Way Handshake*, resultando em 112 *bytes*.

Para a avaliação experimental, o *Improved Handshake* foi adicionado aos projetos *open source wpa_supplicant 0.71* e *hostapd 0.71* [29], que são utilizados em sistemas operacionais, como *Linux*, para que o dispositivo possa atuar como cliente e ponto de acesso, respectivamente. O protocolo de acordo de chaves ECDH foi implementado sobre da infraestrutura provida pelo projeto *OpenSSL 0.9.8m* [30]. O *Improved Handshake* foi desenvolvido para dar suporte aos mecanismos de autenticação pessoal dos protocolos WPA, WPA2, assim como das versões desses dois protocolos com a emenda IEEE 802.11w.

O NIST (*National Institute of Standards and Technology*) recomenda a utilização de quinze curvas elípticas [31]. Dentre elas, estão dez curvas sobre campos finitos binários e cinco curvas sobre campos finitos primos. O *Improved Handshake* foi avaliado com cada uma das quinze curvas elípticas recomendadas. Todos os experimentos foram repetidos 1000 vezes e foram realizados em um ambiente real de comunicação entre o cliente e o ponto de acesso.

A Tabela 7.1 mostra que o *Improved Handshake* com as curvas de índices 1, 2, 6 e 7

Tabela 7.1 Aumento Médio (em *bytes*) do tamanho das mensagens com o *Improved Handshake* (IH)

Índice	Mecanismo	Aumento Médio por Mensagem
1	IH com Curva P-192	36
2	IH com Curva P-224	42
3	IH com Curva P-256	48
4	IH com Curva P-384	72
5	IH com Curva P-521	97,5
6	IH com Curva K-163	30,75
7	IH com Curva B-163	30,75
8	IH com Curva K-233	44,25
9	IH com Curva B-233	44,25
10	IH com Curva K-283	53,25
11	IH com Curva B-283	53,25
12	IH com Curva K-409	77,25
13	IH com Curva B-409	77,25
14	IH com Curva K-571	107,25
15	IH com Curva B-571	107,25

apresenta os menores aumentos no tamanho médio das mensagens em relação as outras curvas avaliadas. Considerando esses casos, o aumento médio é em torno de 27,5% a 37,5% quando comparado ao *4-Way Handshake* tradicional. Ao se analisar o aumento médio na proposta em [27], observa-se que o mesmo seria maior do que 85%. Já ao se analisar a proposta em [28], observa-se que o aumento médio seria maior do que 164%. Assim sendo, o *Improved Handshake* se mostra significativamente melhor em termos do *overhead* introduzido, em relação aos trabalhos relacionados. É importante ressaltar que as curvas 6 e 7 possuem as menores chaves públicas (328 bits), mas ainda assim provêem um grau de segurança elevado em relação ao protocolo DH com chaves de 1024 bits. As

Tabela 7.2 Duração Total Média (em milisegundos) do *Improved Handshake* (IH) e do *4-Way Handshake*.

Índice	Mecanismo	Duração Total Média (ms)	Desvio Padrão
0	*4-Way Handshake*	15,08	6,13
1	IH com Curva P-192	18,34	6,56
2	IH com Curva P-224	20,30	5,97
3	IH com Curva P-256	23,87	7,14
4	IH com Curva P-384	39,81	7,03
5	IH com Curva P-521	68,19	7,83
6	IH com Curva K-163	20,10	6,02
7	IH com Curva B-163	20,52	5,82
8	IH com Curva K-233	30,12	6,64
9	IH com Curva B-233	31,16	5,99
10	IH com Curva K-283	45,30	8,81
11	IH com Curva B-283	50,09	8,79
12	IH com Curva K-409	92,32	9,53
13	IH com Curva B-409	103,77	11,00
14	IH com Curva K-571	200,10	11,34
15	IH com Curva B-571	223,25	12,53

chaves públicas para as curvas 1 e 2 possuem, respectivamente, 384 e 448 bits, provendo uma segurança ainda melhor. Estima-se que uma chave ECDH deve possuir 224 bits para ser considerada segura até o ano de 2030 [32]. Assim sendo, uma chave ECDH com pelo menos 328 bits pode ser potencialmente utilizada com segurança por mais tempo.

A Tabela 7.2 apresenta a duração média do *Improved Handshake* e do *4-Way Handshake*. O *Improved Handshake* com as curvas de índices 1, 2, 6 e 7 foi realizado mais rapidamente do que com o uso das outras curvas. Nesses casos, o aumento médio na duração do *handshake* foi em torno de 3 a 5 ms. Esses acréscimos podem ser considerados baixos

em relação à duração total média do *4-Way Handshake*, que foi de 15,08 ms.

Entre as curvas que permitiram um melhor desempenho, a curva cujo índice é 1 permite uma segurança adequada devido ao tamanho de sua chave pública. Além disso, a menor duração média do *Improved Handshake* foi obtida com essa mesma curva. Assim sendo, recomenda-se a utilização dela com o *Improved Handshake*. Além disso, por essa curva pertencer a um campo finito primo, ela permite a simplificação equação que a define para a Equação 4.2. Deste modo, as operações realizadas sobre tal curva foram computadas em tempos reduzidos em relação às curvas pertencentes a campos finitos binários.

CAPÍTULO 8

CONCLUSÕES

Esse trabalho propôs primeiramente uma adaptação ao processo de *4-Way Handshake*, utilizado na autenticação dos clientes à rede nos padrões de segurança WPA, WPA2 e desses dois padrões acrescidos pela emenda IEEE 802.11w. Essa adaptação, denominada *Improved Handshake*, tem por objetivo eliminar o problema de derivação indevida das chaves PTK em redes que usam o método de autenticação pessoal. A solução proposta tem sua segurança baseada no Problema do Logaritmo Discreto sobre Curvas Elípticas, através do protocolo ECDH. Apesar de desenvolvido com foco para o método de autenticação pessoal, o *Improved Handshake* também é adequado ao método de autenticação coorporativa, visto que este mecanismo é inerentemente mais seguro que o *4-Way Handshake*, utilizado até então.

Posteriormente, a solução proposta foi adaptada para prover autenticação automática em redes abertas, permitindo que possam ser acordados os conjuntos de chaves temporárias PTK e GTK entre as entidades da rede. Desse modo, o *Improved Handshake* para redes abertas permite que os quadros trocados na rede trafeguem com a devida criptografia, mesmo sem a necessidade do fornecimento prévio de chaves pelos usuários.

O *Improved Handshake* foi implementado e avaliado experimentalmente em ambientes reais. Foi avaliado o desempenho do *Improved Handshake* utilizando quinze curvas elípticas recomendadas pelo NIST e comparado com o *4-Way Handshake*, sendo cinco curvas sobre campo finito primo e dez curvas sobre campo finito binário. Com o uso da curva elíptica P-192 é possível obter um alto grau de segurança no processo de derivação da PTK, aumentando, em média, a duração do *handshake* em pouco mais de 3 ms. Em comparação com trabalhos relacionados, o *Improved Handshake* utiliza mensagens significativamente menores. Adicionalmente, como tais propostas utilizam o protocolo

Diffie-Hellman, elas introduzem custos computacionais elevados para proverem um grau de segurança relativamente baixo quando comparado ao grau de segurança provido pelo *Improved Handshake*.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] IEEE Standard 802.11, "IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

[2] Wi-Fi Alliance, "Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for Today's Wi-Fi Networks," 2003.

[3] IEEE Standard 802.11i, "IEEE Standard for Information Technology – Telecommunications and Information Exchange between System – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements Interpretation," 2004.

[4] IEEE Standard 802.11w, "IEEE Standard for Information technology – Telecommunications and Information Exchange between System – Local and Metropolitan area networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 4: Protected Management Frames," 2009.

[5] E. Tews, "Attacks on the WEP Protocol," Cryptology ePrint Archive, Report 2007/471, 2007.

[6] IEEE 802.1X, "IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control," 2004.

[7] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," in *Lecture Notes in Computer Science*, 2001, pp. 1–24.

[8] A. Klein, "Attacks on the RC4 Stream Cipher," *Designs, Codes and Cryptography*, vol. 48, pp. 269–286, 2008.

[9] E. Tews, R.-P. Weinmann, and A. Pyshkin, "Breaking 104 Bit WEP in Less Than 60 Seconds," *Lecture Notes in Computer Science - Information Security Applications*, no. 4867, pp. 188–202, 2007.

[10] KoreK, "Chopchop (Experimental WEP Attacks)," 2004. [Online]. Available: http://www.netstumbler.org/f50/chopchop-experimental-wep-attacks-12489/

[11] M. Beck and E. Tews, "Practical Attacks Against WEP and WPA," in *Proceedings of the Second ACM Conference on Wireless Network Security - WiSec'09*, 2009, pp. 79–86.

[12] T. Ohigashi and M. Morii, "A Practical Message Falsification Attack on WPA," in *Procedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System*, August 2009.

[13] B. G. D'Ambrosio, E. F. Souza, and P. A. S. Gonçalves, "Um Mecanismo de Proteção Contra a Previsibilidade de Informações em Pacotes," in *Proceedings of Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – WTICG SBSeg'10*, Fortaleza, 2010, pp. 41–50.

[14] S. Fogie, "Cracking Wi-Fi Protected Access (WPA), Part 2," http://www.ciscopress.com/articles/article.asp?p=370636, March 2005.

[15] IEEE 802.1X, "IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control," 2001.

[16] G. Lehembre, "Wi-Fi security – WEP, WPA and WPA2," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, 2005.

[17] R. Moskowitz, "Weakness in Passphrase Choice in WPA Interface," http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html, 2003.

[18] W. Diffie and M. E. Hellman, "New Directions in Cryptography," pp. 644–654, 1976.

[19] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.* John Wiley & Sons, 1996.

[20] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management â Part 1: General(Revised)," in *NIST Special Publication*, 2007.

[21] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," in *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, Washington, 1979, pp. 55–60.

[22] J. T. Tate, "The Arithmetic of Elliptic Curves," in *Inventiones Mathematicae*, vol. 23, 1973, pp. 179–206.

[23] V. Gupta, S. Gupta, and S. Chang, "Performance Analysis of Elliptic Curve Cryptography for SSL," in *Proceedings of Workshop on Wireless Security 2002*, 2002, pp. 87–94.

[24] S. A. Vanstone, "Next Generation Security for Wireless: Elliptic Curve Cryptography," in *Computers and Security*, vol. 22, no. 5, 2003.

[25] C. Lederer, R. Mader, M. Koschuch, J. Groszschaedl, A. Szekely, and S. Tillich, "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks," in *Proceedings of Workshop on Information Security Theory and Practices*, 2009, pp. 112–127.

[26] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography.* Springer Verlag, 2004.

[27] C. D. Mano and A. Striegel, "Resolving WPA Limitations in SOHO and Open Public Wireless Networks," in *Proceedings of IEEE Wireless Communications and Networking Conference 2006*, Las Vegas, 2006.

[28] E. F. Souza and P. A. S. Gonçalves, "Um Mecanismo de Proteção de Nonces para a Melhoria da Segurança de Redes IEEE 802.11i," in *Proceedings of Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – WTICG/SBSeg'09*, Campinas, 2009, pp. 291–300.

[29] J. Malinen and contributors, "Host AP driver for Intersil Prism2/2.5/3, hostapd, and WPA Supplicant," http://hostap.epitest.fi/, 2010.

[30] OpenSSL, "The OpenSSL Project," http://www.openssl.org/, 2010.

[31] National Institute of Standards and Technology, "FIPS PUB 186-3 - Federal Information Processing Standards Publication," in *Digital Signature Standard*, 2009.

[32] T. Ahmad, J. Hu, and S. Han, "An Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography," in *Proceedings of Third International Conference on Network and System Security*, Australia, 2009, pp. 474–479.