Um Mecanismo de Autenticação Baseado em ECDH para Redes IEEE 802.11

Eduardo Ferreira de Souza, Paulo André da S. Gonçalves

Centro de Informática (CIn) - Universidade Federal de Pernambuco (UFPE)
Av. Professor Luís Freire, s/n – Cidade Universitária – 50.740-540 – Recife – PE – Brasil

{efs, pasg}@cin.ufpe.br

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 paper, we propose and evaluate a new handshake protocol, which is based on the ECDH (Elliptic Curve Diffie-Hellman) protocol and solves the problem of undue PTK derivation. We also present a solution to provide automatic authentication on open networks, allowing encrypted traffic information to be exchanged without the need of providing keys by the users.*

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 4-Way Handshake é falho quando o método de autenticação pessoal é usado, permitindo que entidades maliciosas que possuam a PSK (Pre-Shared Key) da rede possam reproduzir o processo de derivação da chave PTK de todos os clientes autenticados. Este artigo propõe e avalia experimentalmente um novo processo de handshake. Ele é baseado no protocolo Diffie-Hellman sobre Curvas Elípticas (ECDH) e resolve o problema de derivação indevida da PTK. Além disso, também é apresentada uma solução para prover autenticação automática em redes abertas, permitindo o tráfego criptografado de informações na rede sem a necessidade do fornecimento de chaves pelos usuários.*

1. Introdução

A adoção de redes locais sem fio IEEE 802.11 tem crescido significativamente graças ao baixo custo dos equipamentos necessários à implantação dessas redes e à mobilidade fornecida aos seus usuários. 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*) [IEEE Standard 802.11 1999], WPA (*Wi-Fi Protected*

Access) [Wi-Fi Alliance 2003] e IEEE 802.11i ou WPA2 [IEEE Standard 802.11i 2004]. Recentemente foi lançada a emenda IEEE 802.11w [IEEE Standard 802.11w 2009] que complementa o WPA e o WPA2, adicionando proteção nos quadros de gerenciamento. Dentre esses protocolos, o WEP é considerado ultrapassado devido a sua longa lista de vulnerabilidades [Tews 2007].

Os protocolos WPA e WPA2 especificam dois métodos de autenticação de usuários à rede: autenticação corporativa e autenticação pessoal. No primeiro método, um servidor de autenticação (padrão IEEE 802.1X) [IEEE 802.1X 2004] é responsável por verificar as credenciais dos usuários e fornecer uma chave mestra ao cliente e ao ponto de acesso. O segundo método é utilizado em ambientes que não dispõem de um servidor de autenticação. Nesse caso, a autenticação 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 mestra da rede, sendo esta uma chave pré-compartilhada. Essa chave é denominada PSK (*Pre-Shared Key*) e deve ser possuída por todos os usuários legítimos da rede. Esse método de autenticação pessoal é conhecido por WPA-PSK ou WPA2-PSK de acordo com o protocolo utilizado.

O processo de autenticação é realizado durante o *4-Way Handshake* entre o cliente e o ponto de acesso. Nesse processo, 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 processo de derivação da PTK é vulnerável em redes que usam os métodos de autenticação WPA-PSK [Lehembre 2005], WPA2-PSK e ambos os métodos complementados pelo IEEE 802.11w, pois permite que a derivação da PTK de qualquer cliente autenticado seja reproduzida por entidades maliciosas que conheçam a chave pré-compartilhada da rede e tenham capturado 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.

O acesso indevido a dados também pode ocorrer em redes IEEE 802.11 que são utilizadas em ambientes públicos como *shoppings*, aeroportos e restaurantes. Nesses ambientes, as redes são abertas e os usuários podem precisar, no máximo, fornecer credenciais (*e.g.* CPF ou login/senha) para terem o acesso à Internet permitido. Contudo, como não há um processo de autenticação dos clientes na rede sem fio, os dados dos usuários trafegam sem criptografia, excetuando-se quando a mesma é provida por camadas superiores da pilha de protocolos (*e.g.* uso de HTTPS). 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. Apesar das redes abertas, geralmente, não terem por objetivo o provimento de segurança aos seus usuários, é importante prover algum mecanismo de autenticação automática, permitindo que cada dispositivo da rede possa trocar quadros criptografados sem a necessidade do fornecimento de chaves pelos usuários.

Este artigo lida tanto com o problema de derivação indevida da PTK quanto com problema da falta de autenticação em redes abertas. Primeiramente, este trabalho propõe uma adaptação no *4-Way Handshake* como solução ao problema de derivação indevida da PTK em redes que usam o método de autenticação pessoal dos padrões de segurança

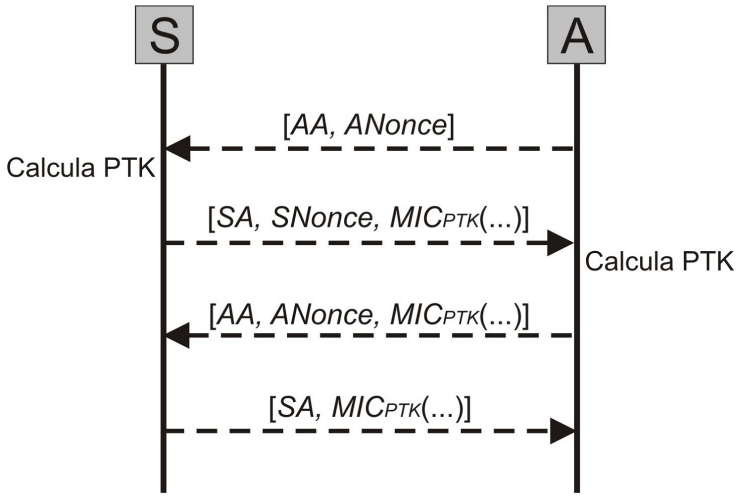

Figura 1. *4-Way Handshake*

WPA, WPA2 e desses dois padrões com a emenda IEEE 802.11w. A solução proposta se baseia no protocolo Diffie-Hellman sobre Curvas Elípticas (*Elliptic Curve Diffie–Hellman* - ECDH). Em seguida, a solução proposta é adaptada para prover autenticação automática em redes abertas, permitindo a troca de informações criptografadas sem a necessidade do fornecimento de chaves pelos usuários. As soluções propostas neste artigo têm por requisito não inserirem um elevado tempo de execução ao *Handshake*. Esse requisito se faz necessário, pois existem redes onde os dispositivos necessitam realizar constantes *handoffs*, e nesses casos, um tempo de autenticação elevado se torna inadequado.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta o *4-Way Handshake*. A Seção 3 apresenta os trabalhos relacionados e como os mesmos se diferenciam do trabalho proposto. A Seção 4 apresenta os conceitos sobre o protocolo Diffie-Hellman sobre Curvas Elípticas. A Seção 5 apresenta o mecanismo de autenticação proposto neste trabalho. A Seção 6 avalia o impacto do mecanismo proposto em termos do aumento médio no tamanho de mensagens trocadas no *handshake* e duração do mesmo. Finalmente, a Seção 7 apresenta as conclusões do trabalho.

2. O *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 exclusivamente para eles. A PTK é importante, pois como dito, serve para a criptografia de quadros, verificação da integridade dos mesmos, entre outras coisas.

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 1 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. 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); e os códigos de verificação de integridade das mensagens (MIC_{PTK}). O valor do MIC_{PTK} é calculado com base na chave PTK derivada entre as entidades. Ele serve para a verificação da integridade da mensagem recebida. 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 MAC e do *Nonce* da outra entidade comunicante. Essa derivação é feita utilizando-se uma função pseudo-aleatória (*Pseudo Random Function* – PRF) [IEEE Standard 802.11i 2004] de tal forma que:

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

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, antes do *4-Way Handshake*, o servidor de autenticação envia ao cliente uma chave MSK (*Master Session Key*) por intermédio do ponto de acesso. A MSK é então utilizada para a derivação da PMK. 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 função, 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 [Lehembre 2005]. 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 [Moskowitz 2003]. Esse ataque é praticável somente se a *passphrase* usada na criação da PSK possuir menos de 20 caracteres [Fogie 2005]. Nesse caso a vulnerabilidade não é considerada do protocolo de segurança, mas sim uma falha do usuário/administrador.

3. Trabalhos Relacionados

O problema de derivação indevida da PTK não vem recebendo a devida atenção por parte do IEEE. Além disso, poucos trabalhos na literatura buscam soluções para esse problema [Mano and Striegel 2006] [Souza and Gonçalves 2009].

Em [Mano and Striegel 2006] 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 problema do logaritmo discreto sobre um grupo multiplicativo de inteiros e utiliza o protocolo de acordo de chaves Diffie-Hellman (DH) [Diffie and Hellman 1976]. O problema do logaritmo discreto consiste em encontrar um inteiro x, tal que $y = g^x$, ou seja, consiste na dificuldade de se encontrar o $log_g y$. Baseando-se na dificuldade de resolver o problema do logaritmo discreto, o protocolo DH permite que duas entidades

consigam derivar uma mesma chave de forma segura, mesmo que o canal de comunicação seja inseguro. Na proposta em [Mano and Striegel 2006], as duas primeiras mensagens do *4-Way Handshake* são utilizadas para se derivar uma chave denominada DPMK (*Dynamic Pairwise Master Key*) com base no protocolo DH. Essa chave fica sendo conhecida apenas pelo cliente em autenticação e pelo ponto de acesso 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. Contudo, 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*.

Em [Souza and Gonçalves 2009] 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 no problema do logaritmo discreto e no protocolo de derivação de chaves DH. 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 utiliza 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 os *Nonces* utilizados como argumento no processo de derivação da PTK sem conhecer a chave K.

Diferentemente dos trabalhos relacionados, este trabalho propõe uma adaptação no *4-Way Handshake* como solução ao problema de derivação indevida da PTK tendo como base o protocolo Diffie-Hellman sobre Curvas Elípticas (*Elliptic Curve Diffie–Hellman* - 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 artigo 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.

A utilização de criptossistemas baseados em curvas elípticas, como o ECDH, tem crescido expressivamente em 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 exemplo: tamanho de parâmetros e chaves; tempo processamento; e espaço de armazenamento [Gupta et al. 2002], [Vanstone 2003].

Atualmente os ataques mais eficientes para ECDH executam em tempo exponencial [Lederer et al. 2009]. No entanto, existem ataques ao protocolo DH que executam em tempo sub-exponencial [Hankerson et al. 2004]. A Tabela 1 apresenta uma comparação entre o tamanho de chaves em sistemas baseados em ECDH e DH para proverem um grau

Tabela 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

de segurança equivalente [Gupta et al. 2002]. 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.

Além das fraquezas do protocolo DH, o uso desse protocolo introduz um *overhead* de processamento significativo quando comparado ao uso do protocolo ECDH [Vanstone 2003]. 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 [Vanstone 2003]. Isso é um fator relevante principalmente para dispositivos com baixa capacidade computacional como *smartphones* e PDAs.

4. Diffie-Hellman sobre Curvas Elípticas

Fundamentalmente, os criptossistemas de chaves públicas são baseados em problemas da matemática classificados como NP, incluindo o Diffie-Hellman e o Diffie-Hellman sobre Curvas Elípticas. Este último protocolo tem sua segurança baseada na dificuldade de se resolver o problema do logaritmo discreto sobre curvas elípticas. Uma curva elíptica sobre um campo finito F é o conjunto de pontos P(x, y) juntamente com um ponto no infinito, onde as variáveis x e y satisfazem uma equação de *Weierstrass* [Tate 1973] dada por:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \quad (1)$$

As variáveis e os coeficientes pertencem ao campo finito F. Para curvas elípticas sobre campos finitos gerados por números primos, a Equação (1) pode ser simplificada, desde que não possua raízes múltiplas, tomando a forma da Equação (2). A inexistência de raízes múltiplas é garantida para $4a_4^3 + 27a_5^2 \neq 0$.

$$y^2 = x^3 + a_4x + a_5 \quad (2)$$

A Figura 2 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.

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

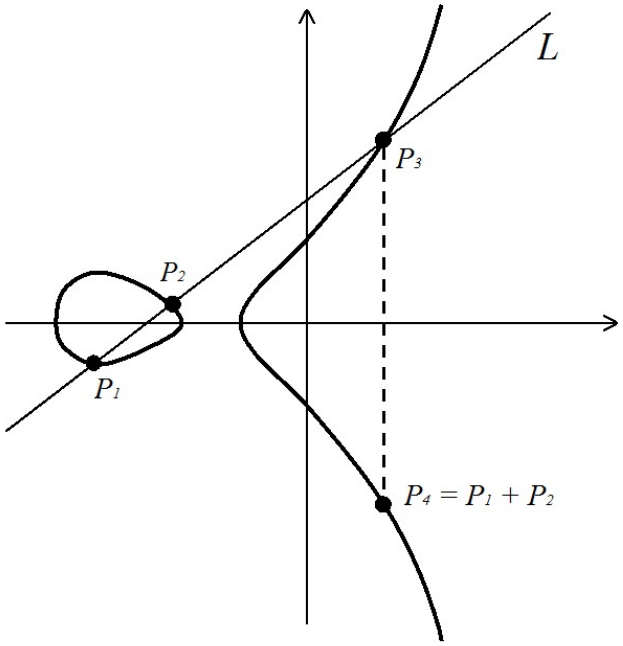

Figura 2. Adição entre pontos sobre curvas elípticas

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 $Q \in E$. Desse modo, a resolução do problema do logaritmo discreto sobre curvas elípticas 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. 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 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 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. Isso ocorre porque para uma entidade maliciosa calcular K, é necessário que ela conheça ao menos uma das chaves privadas k_A ou k_S. Como essa

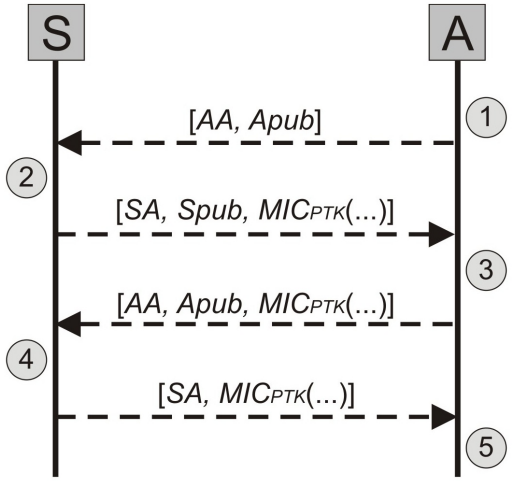

Figura 3. *Improved Handshake*

informação é mantida em sigilo, o cálculo de K em função apenas das chaves públicas P_A e P_S torna-se inviável.

5. O Mecanismo de Autenticação Proposto

O mecanismo proposto neste trabalho consiste em uma adaptação do *4-Way Handshake* para uso do protocolo de acordo de chaves Diffie-Hellman sobre Curvas Elípticas. Doravante, o *4-Way Handshake* adaptado será denominado *Improved Handshake*. Nessa proposta, o cliente e o ponto de acesso inicialmente já conhecem os parâmetros de domínio, os quais definem a curva elíptica a ser utilizada. A escolha de uma curva elíptica adequada para o *Improved Handshake* é apresentada na Seção 6. Em particular, o *Improved Handshake* propõe a utilização das chaves públicas do ECDH também como *Nonces*. Os detalhes dessa proposta serão apresentados ainda nesta seção.

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. A chave elíptica (Ke) é utilizada juntamente com a PMK para derivação da PTK. Ke representa a coordenada x da chave K obtida através do protocolo ECDH. Além do cálculo de Ke, as chaves públicas $Spub$ e $Apub$ são utilizadas como *Nonces* (respectivamente, $SNonce$ e $ANonce$ do *4-Way Handshake*). Como $Spub$ e $Apub$ são geradas aleatoriamente e substituem os *Nonces*, o objetivo de permitir a geração de diferentes chaves PTK a cada *handshake* é mantido. SA e AA são os endereços físicos do cliente e do ponto de acesso, respectivamente.

A Figura 3 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_{PTK} e verifica a integridade da mensagem de S;
   O ponto de acesso A calcula Ke com base em $Spub$, $Apub$ e $Apriv$;
   O ponto de acesso A deriva a PTK;

4. O cliente S calcula o MIC_{PTK} 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 artigo, a função pseudo-aleatória recebe os argumentos PMK, Ke, AA, SA, $Apub$, $Spub$ e uma *string* de modo que:

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

Para um atacante que conheça *a priori* 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.

Com uma pequena modificação no cálculo da PTK, o *Improved Handshake* também pode ser utilizado para prover autenticação automática em redes abertas sem a necessidade do fornecimento de chaves pelos usuários. O *Improved Handshake* para redes abertas possui a mesma estrutura de mensagens anteriormente proposta, no entanto difere nos argumentos da função de derivação da PTK. Nesse caso, a PTK é derivada de modo que:

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

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 do fato da derivação da chave Ke ser baseada no problema do logaritmo discreto sobre curvas elípticas e cujas soluções executam atualmente em tempo exponencial. Até hoje, não são conhecidos problemas que levem a 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. Isso ocorre sem a necessidade de configurações adicionais, visto que o processo de *handshake* é independente da forma de obtenção da PMK.

6. Avaliação Experimental

Esta seção 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* [IEEE Standard 802.11i 2004] 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*.

Tabela 2. 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

Para a avaliação experimental, o *Improved Handshake* foi adicionado aos *softwares open source wpa_supplicant 0.71* e *hostapd 0.71* [Malinen and contributors 2010] que são utilizados em sistemas operacionais, como o *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* [OpenSSL 2010]. 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 [National Institute of Standards and Technology 2009]. 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 2 mostra que o *Improved Handshake* com as curvas de índices 1, 2, 6 e 7 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

Tabela 3. 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

37,5% quando comparado ao *4-Way Handshake* tradicional. Ao se analisar o aumento médio na proposta em [Mano and Striegel 2006], observa-se que o mesmo seria maior do que 85%. Já ao se analisar a proposta em [Souza and Gonçalves 2009], observa-se que o aumento médio seria maior do que 164%. Assim sendo, o *Improved Handshake* se mostra melhor em termos do *overhead* introduzido. 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 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 [Ahmad et al. 2009]. Assim sendo, uma chave ECDH com pelo menos 328 bits pode ser potencialmente utilizada com segurança por mais tempo.

A Tabela 3 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*.

7. Conclusões

Esse trabalho propôs uma adaptação no *4-Way Handshake* como solução ao problema de derivação indevida da PTK em redes que usam o método de autenticação pessoal dos padrões de segurança WPA, WPA2 e desses dois padrões com a emenda IEEE 802.11w. A solução proposta se baseou no protocolo Diffie-Hellman sobre Curvas Elípticas. Além disso, a solução proposta foi adaptada para prover autenticação automática em redes abertas, permitindo a criptografia de informações sem a necessidade do fornecimento de chaves pelos usuários. A proposta apresentada foi avaliada através de experimentos realizados em ambientes reais, mostrando que com o uso da curva elíptica P-192 definida pelo NIST 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 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

Ahmad, T., Hu, J., and Han, S. (2009). An Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography. In *Proceedings of Third International Conference on Network and System Security*, pages 474–479, Australia.

Diffie, W. and Hellman, M. E. (1976). New Directions in Cryptography.

Fogie, S. (2005). Cracking Wi-Fi Protected Access (WPA), Part 2. `http://www.fermentas.com/techinfo/nucleicacids/maplambda.htm`.

Gupta, V., Gupta, S., and Chang, S. (2002). Performance Analysis of Elliptic Curve Cryptography for SSL. In *Proceedings of Workshop on Wireless Security 2002*, pages 87–94.

Hankerson, D., Menezes, A., and Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer Verlag.

IEEE 802.1X (2004). IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control.

IEEE Standard 802.11 (1999). 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.

IEEE Standard 802.11i (2004). 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.

IEEE Standard 802.11w (2009). 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.

Lederer, C., Mader, R., Koschuch, M., Groszschaedl, J., Szekely, A., and Tillich, S. (2009). Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks. In *Proceedings of Workshop on Information Security Theory and Practices*, pages 112–127.

Lehembre, G. (2005). Wi-Fi security – WEP, WPA and WPA2. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*.

Malinen, J. and contributors (2010). Host AP driver for Intersil Prism2/2.5/3, hostapd, and WPA Supplicant. `http://hostap.epitest.fi/`.

Mano, C. D. and Striegel, A. (2006). Resolving WPA Limitations in SOHO and Open Public Wireless Networks. In *Proceedings of IEEE Wireless Communications and Networking Conference 2006*, Las Vegas.

Moskowitz, R. (2003). Weakness in Passphrase Choice in WPA Interface. `http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html`.

National Institute of Standards and Technology (2009). FIPS PUB 186-3. In *Digital Signature Standard*.

OpenSSL (2010). The OpenSSL Project. `http://www.openssl.org/`.

Souza, E. F. and Gonçalves, P. A. S. (2009). Um Mecanismo de Proteção de Nonces para a Melhoria da Segurança de Redes IEEE 802.11i. In *Proceedings of WTICG/SBSeg*, pages 291–300, Campinas.

Tate, J. T. (1973). The Arithmetic of Elliptic Curves. In *Inventiones Mathematicae*, volume 23, pages 179–206.

Tews, E. (2007). Attacks on the WEP Protocol. Cryptology ePrint Archive, Report 2007/471.

Vanstone, S. A. (2003). Next Generation Security for Wireless: Elliptic Curve Cryptography. In *Computers and Security*, volume 22.

Wi-Fi Alliance (2003). Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for Today's Wi-Fi Networks.