SEGURANÇA NO PROCESSO DE AUTENTICAÇÃO DE REDES IEEE 802.11

Ivan Luiz de França Neto[1]; Eduardo Ferreira de Souza[2]; Paulo André da Silva Gonçalves[3]

[1]Estudante do Curso de Ciência da Computação – CIn – UFPE; E-mail: ilfn@cin.ufpe.br,
[2]Estudante do Curso de Ciência da Computação – CIn – UFPE; E-mail: efs@cin.ufpe.br,
[3]Docente/pesquisador do Depto de Informática – CIn – UFPE. E-mail: pasg@cin.ufpe.br.

Sumário: 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 trabalho apresenta 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.

Palavras-chave: 4-way handshake; autenticação; IEEE 802.11; protocolos de segurança

INTRODUÇÃO

Tanto o protocolo WPA quanto o WPA2 possuem dois métodos de autenticação de usuários à rede: autenticação corporativa e autenticação pessoal. No primeiro método, um servidor de autenticação (padrão IEEE 802.1X) é utilizado para realizar a autenticação de usuários na rede, tal arquitetura é utilizada em ambientes de médio e grande porte. O segundo método é utilizado em ambientes de pequeno porte, onde a autenticação é realizada pelo próprio ponto de acesso, através de uma chave pré-compartilhada (PSK), que 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. Parte do processo de autenticação é realizada durante o 4-Way Handshake entre o cliente e o ponto de acesso e tem por objetivo permitir que cliente e o ponto de acesso da rede verifiquem se ambos possuem a mesma chave mestra *Pairwise Master Key* (PMK). Ao término do 4-Way Handshake as entidades comunicantes derivam um conjunto de chaves PTK (Pairwise Transient Key) que são comuns e exclusivas entre o cliente e o ponto de acesso, tal conjunto é temporário. Uma das funções da PTK é prover a criptografia de quadros e a verificação da integridade dos mesmos. Apesar de esse processo ser realizado sem que chaves sejam transmitidas pelo canal de comunicação, temos que a derivação de chaves pode simplesmente ser reproduzida [2] [5] por entidades maliciosas. Para isso, basta ao atacante conhecer a chave pré-compartilhada e ter capturado as duas primeiras mensagens trocadas durante o 4-Way Handshake do cliente-alvo. Notamos, portanto, que o processo de derivação da PTK é vulnerável em redes que usam os métodos de autenticação WPA-PSK, WPA2-PSK. Com essas informações em mãos, um

atacante 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. Primeiramente, este trabalho apresenta 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 apresentada se baseia no protocolo Diffie-Hellman sobre Curvas Elípticas (Elliptic Curve Diffie–Hellman – ECDH). Em seguida, é apresentada uma adaptação nova adaptação no 4-Way Handshake para prover autenticação automática em redes abertas, permitindo a troca de informações criptografadas sem a necessidade do fornecimento de chaves pelos usuários.

MATERIAIS E MÉTODOS

Para os testes das vulnerabilidades dos protocolos foi utilizada uma plataforma formada por 3 computadores com placas wireless utilizando redes IEEE 802.11 e um ponto de acesso. Foram executados os testes através dos sistemas operacionais Ubuntu 8.04 e Windows XP. As ferramentas utilizadas foram os programas de captura de tráfego e análise de pacotes Wireshark, Aircrack-ng e Kismet. Os softwares do cliente e do ponto de acesso dos testes foram do projeto Host AP [3], onde o cliente (wpa_supplicant) deste projeto é o padrão para sistema operacional Ubuntu.

RESULTADOS

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. Em particular, o Improved Handshake propõe a utilização das chaves públicas do ECDH também como Nonces. 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:

PTK = PRF(PMK, Ke, “Elliptic pairwise key expansion”, Min(AA, SA) || Max(AA, SA) || Min(Apub, Spub) || Max(Apub, Spub)).

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:

PTK = PRF(Ke, "Elliptic pairwise key expansion", Min(AA, SA) || Max(AA, SA) || Min(Apub, Spub) || Max(Apub, Spub)).

O Improved Handshake foi avaliado 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.

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

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

Tabela 1. (a) Aumento Médio (em *bytes*) do tamanho das mensagens com o *Improved Handshake* (IH). (b) Duração Total Média (em milisegundos) do Improved Handshake (IH) e do 4-Way Handshake.

A Tabela 1a 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 37,5% quando comparado ao 4-Way Handshake tradicional. Ao se analisar o aumento médio na proposta em [7], observa-se que o mesmo seria maior do que 85%. Já ao se analisar a proposta em [5], observa-se que o aumento médio seria maior do que 164%. Assim sendo, o Improved Handshake se mostra melhor em termos do overhead introduzido. A Tabela 1b 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.

DISCUSSÃO

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. 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.

CONCLUSÕES

Esse trabalho apresentou 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. Além disso, foi mostrada uma adaptação para prover autenticação automática em redes abertas, permitindo a criptografia de informações sem a necessidade do fornecimento de chaves pelos usuários. Experimentos realizados em ambientes reais mostraram 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.

AGRADECIMENTOS

Agradecemos ao PIBIC, à UFPE e ao CNPq pelo apoio para a realização das pesquisas.

REFERÊNCIAS

[1] – Diffie, W. and Hellman, M. E. (1976). New Directions in Cryptography. *In Proceedings of IEEE Transactions on Information Theory*, volume 22, pages 644–654.

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

[3] – Host AP. driver for Intersil Prism2/2.5/3, hostapd, and WPA Supplicant – http://hostap.epitest.fi/

[4] – Shihab, A. and Langhammer, M. (2003). Implementing IKE Capabilities in FPGA Designs. http://www.eetimes.com/story/OEG20031205S0005.

[5] – 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*, Campinas.

[6] – National Institute of Standards and Technology (2009). FIPS PUB 186-3. In Digital Signature Standard.

[7] – 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.