SEGURANÇA EM REDES IEEE 802.11: INTEGRIDADE DE DADOS, AUTENTICAÇÃO E CONFIDÊNCIA

Eduardo Ferreira de Souza[1] ; Paulo André da Silva Gonçalves [2]

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

Sumário: Este artigo apresenta uma análise dos protocolos de segurança que atuam na proteção das redes IEEE 802.11. Inicialmente foi estudado o funcionamento dos protocolos WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), IEEE 802.11i e da emenda IEEE 802.11w. Em seguida foram realizados testes de segurança sobre tais protocolos visando identificar suas vulnerabilidades. Com base nas vulnerabilidades identificadas, o trabalho se focou em propor uma solução para o problema de captura indevida de chaves, existente no processo de autenticação dos protocolos WPA e IEEE 802.11i. Essa vulnerabilidade permite que um atacante capture as chaves temporárias PTK (*Pairwise Transient Key*) dos clientes autenticados na rede, permitindo-o decifrar e adulterar os pacotes enviados e recebidos por tais clientes. A proposta desse artigo soluciona tal vulnerabilidade através da utilização do protocolo Diffie-Hellman adaptado ao processo troca de mensagens para derivação da PTK. Por fim, foi realizada uma análise da implantação da proposta sobre tais protocolos, demonstrando sua viabilidade.

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

INTRODUÇÃO

O crescimento na utilização de tecnologias de comunicação sem fio entre dispositivos tem permitido aos usuários grande praticidade e mobilidade. Atualmente a principal tecnologia de rede sem fio utilizada para acesso à Internet e criação de redes locais é a IEEE 802.11, conhecida como *Wi-Fi*. O IEEE 802.11 é um conjunto de especificações que envolve uma família de protocolos voltados para a comunicação segura entre hosts sem fio. Os principais protocolos de segurança para tais redes são: WEP, WPA, IEEE 802.11i e a emenda IEEE 802.11w.

Apesar dos objetivos de garantia de segurança aos clientes da rede, os protocolos de proteção às redes IEEE 802.11 ainda apresentam significativas vulnerabilidades. Os problemas, em geral, são derivados do meio não guiado e sem controle por onde trafegam as informações. Este tipo de propagação de informações se mostra inerentemente inseguro, visto que os dados podem ser capturados por dispositivos indevidos.

Protocolos de Segurança

Wired Equivalent Privacy (WEP): Primeiro padrão desenvolvido para prover segurança em redes IEEE 802.11. Tal protocolo é considerado inseguro e obsoleto devido às suas várias vulnerabilidades.

Wi-Fi Protected Access (WPA): Protocolo criado para corrigir as vulnerabilidades encontradas no WEP. O WPA possui problemas em seu mecanismo de checagem de integridade, não sendo considerado tão seguro quanto IEEE 802.11i.

IEEE 802.11i (ou WPA2): Possui significativas semelhanças com WPA, visto que o WPA foi desenvolvido com base em uma versão preliminar do IEEE 802.11i. Seus principais avanços estão nos mecanismos de integridade e confidência dos dados. A autenticação no IEEE 802.11i funciona de modo análogo ao WPA.

IEEE 802.11w: É uma emenda aos protocolos WPA e IEEE 802.11i e tem como objetivo corrigir as vulnerabilidades encontradas nos pacotes de gerenciamento das redes IEEE 802.11. Foi criado visando evitar ataques de negação de serviço durante a etapa de autenticação dos clientes.

Autenticação e *4-way handshake*

Como exceção do WEP, os protocolos de segurança citados possuem dois possíveis mecanismos de autenticação: um baseado na arquitetura IEEE 802.1X, onde há um servidor dedicado para a verificação da autenticidade dos clientes; e um baseado em chaves pré-compartilhadas (*Pre-Shared Key* – PSK), com todo processo de autenticação dos clientes sendo realizado no ponto de acesso.

Em ambos os modos de autenticação é utilizada uma chave mestra (*Pairwise Master Key* - PMK) para a derivação das chaves temporárias, utilizadas pelos clientes para cifragem e checagem de integridade das mensagens trocadas. No modo baseado na arquitetura IEEE 802.1X, a PMK é enviada pelo servidor de autenticação ao cliente, porém no modo baseado em chaves pré-compartilhadas, a PMK é a própria chaves pré-compartilhada PSK da rede.

O *4-way handshake* é parte do processo de autenticação e tem por objetivo permitir que cliente e o ponto de acesso se autentiquem mutualmente. Ao término desse processo, ambas as entidades compartilham um mesmo conjunto de chaves temporárias PTK. Nesse processo o cliente e o ponto de acesso trocam quatro mensagens. O cliente e o ponto de acesso derivam a PTK através de uma função pseudo-aleatória (*Pseudo Random Function* – PRF), onde *PTK = PRF(PMK, Min(AA, SA)* || *Max(AA, SA)* || *Min(ANonce, SNonce)* || *Max(ANonce, SNonce))*. Os campos SA, AA, SNonce e ANonce representam os endereços físicos e *nonces* do cliente e ponto de acesso, respectivamente. O objetivo dos *nonces* é permitir que cada nova PTK gerada seja diferente das chaves já derivadas anteriormente, visto que eles são gerados de forma aleatória pelas entidades comunicantes.

Vulnerabilidade no *4-way handshake*

O problema de segurança referente ao *4-way handshake* está relacionado com o fato que o processo de derivação de chaves pode ser reproduzido [2,5]. Isso só é possível porque as mensagens trafegam em texto-claro sobre um canal de comunicação sem fio, de modo que qualquer entidade maliciosa pode capturá-las.

Para que a derivação da PTK possa ser reproduzida por um atacante, é necessário que se conheçam todos os parâmetros da função PRF, ou seja, os endereços físicos e os *nonces* do cliente e do ponto de acesso, bem como a PMK. Porém, destes parâmetros apenas a PMK não é trocada em texto-claro durante o *4-way handshake*. Em ambientes baseados em chaves pré-compartilhadas, ou seja, onde a PMK é a própria chave pré-compartilhada PSK, caso um dos clientes autênticos à rede seja um atacante, a rede apresenta-se vulnerável. Isto ocorre porque a PMK é a mesma para todos os clientes, e o atacante, por ser um cliente, possui a PMK.

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

A proposta deste artigo é um novo mecanismo de troca de mensagens para derivação de chaves PTK, nomeado de *6-way handshake*. O *6-way handshake* consiste na troca de seis mensagens entre o cliente (S) e o ponto de acesso (A), das quais as duas primeiras possuem a finalidade de estabelecer uma chave K para proteção dos *nonces* e as quatro mensagens posteriores visam à derivação da PTK. Os valores *p* e *g* são definidos pelo ponto de acesso para o cálculo da chave K seguindo a definição do protocolo Diffie-Hellman [1]; SA, AA, SNonce e ANonce são os endereços MAC e *nonces* do cliente e do ponto de acesso; ANK e SNK representam respectivamente os valores cifrados, através da chave K, dos campos ANonce e SNonce; os campos msg_x representam os tipos de mensagem, onde x é o número da mensagem em questão e SN; SN + 1 e SN + 2 são seus números de sequência; MIC_{PTK} consiste no MIC da mensagem enviada, calculado com base na chave PTK derivada.

A Figura 1 apresenta as mensagens trocadas durante o *6-way handshake*. Inicialmente o ponto de acesso define os valores de *p* e *g*. Os valores de y_1 e y_2 a serem computados pelas entidades comunicantes ocorrem de mesmo modo que no protocolo Diffie-Hellman [1], bem como o cálculo da chave K.

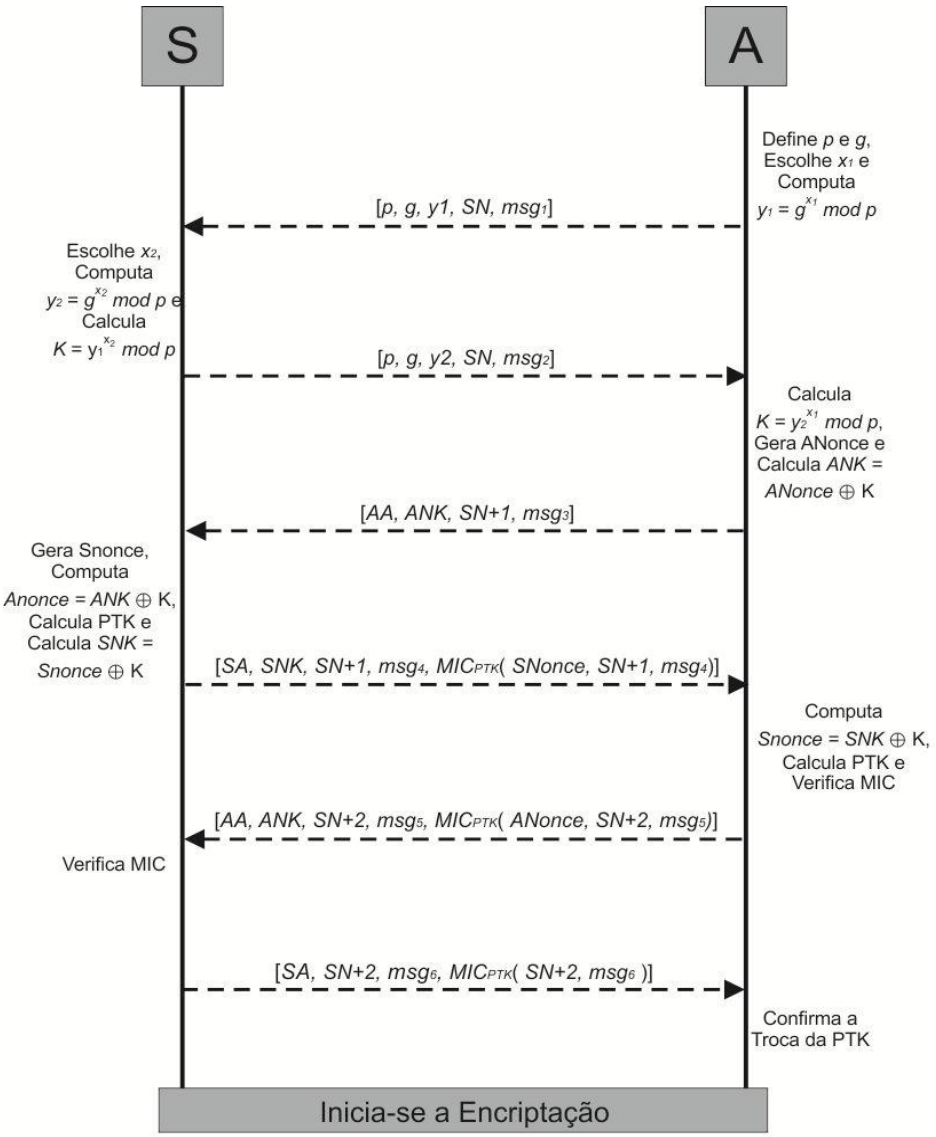

Figura 1: *6-way handshake*

A derivação da chave PTK no *6-way handshake* ocorre do mesmo modo que no *4-way handshake*, de maneira que tal chave é obtida a partir da função pseudo-aleatória PRF, onde *PTK = PRF(PMK, Min(AA, SA) || Max(AA, SA) || Min(ANonce, SNonce) || Max(ANonce, SNonce))*. No entanto, ambas as entidades devem computar uma operação de *ou exclusivo* entre o *nonce* cifrado (ANK e SNK) e a chave K para obter o valor plano do *nonce* contido na mensagem recebida para que tal valor possa ser aplicado como parâmetro à função PRF.

DISCUSSÃO

O protocolo Diffie-Hellman, utilizado como base para o *6-way handshake*, possui sua segurança fundamentada na dificuldade de se resolver o problema do logaritmo discreto, que é situado na classe de problemas NP da matemática. De modo que para se quebrar a segurança da chave K, utilizada para cifrar os *nonces* no *6-way handshake*, é necessário descobrir um algoritmo que resolva em tempo hábil qualquer instância do problema do logaritmo discreto.

Foi realizado um estudo sobre a viabilidade computacional da implementação do mecanismo proposto. Em [4] é utilizada uma abordagem de implementação do protocolo Diffie-Hellman para dispositivos FPGA (*Field Programmable Gate Array*), onde foi obtida uma taxa de até 640 trocas de chaves por segundo. Essas trocas de chaves conseguidas correspondem ao custo computacional de trocas de chaves K entre cliente e o ponto de acesso. Isso demonstra que o custo computacional adicionado ao sistema através do protocolo Diffie-Hellman é baixo, tornando viável a implementação do *6-way handshake* nos diversos dispositivos que utilizam os padrões WPA e IEEE 802.11i.

CONCLUSÕES

Neste trabalho foi desenvolvida uma pesquisa aprofundada sobre os protocolos de segurança de redes IEEE 802.11. Com base em uma vulnerabilidade existente no processo de autenticação dos protocolos WPA e IEEE 802.11i e na emenda IEEE 802.11w, foi um proposto um novo mecanismo de troca de mensagens, nomeado de *6-way handshake*, para derivação segura da chave PTK. O *6-way handshake* se mostrou uma solução eficaz e viável ao problema abordado, visto que o custo computacional adicionado à etapa de autenticação é significativamente baixo. Isso ocorre porque a utilização do protocolo Diffie-Hellman na implementação do mecanismo não acrescenta expressivos esforços computacionais ao sistema.

AGRADECIMENTOS

Agradecemos ao PIBIC, a 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.