Um Mecanismo de Proteção para Redes IEEE 802.11 contra a Previsibilidade de Informações em Pacotes

Bruno Gentilini D'Ambrosio[1] ; Paulo André da Silva Gonçalves[2]
[1]Estudante do Curso de Ciências da Computação - CIn – UFPE; E-mail: bgda@cin.ufpe.br,
[2]Docente/pesquisador do Depto de Informática – CIn – UFPE. E-mail: pasg@cin.ufpe.br.

Sumário: A previsibilidade de informações em alguns tipos de pacotes criptografados que são capturados por entidades maliciosas pode oferecer riscos significativos à segurança das próprias redes. Recentemente, diversos ataques que se utilizam de pacotes criptografados com tamanho e texto-plano conhecidos foram desenvolvidos. Esses ataques são explorados principalmente em redes IEEE 802.11. Este trabalho propõe um mecanismo, denominado EPP, que elimina essas vulnerabilidades inserindo bytes aleatórios nos pacotes antes dos mesmos serem criptografados.
Palavras–chave: Ataques; IEEE 802.11; Protocolos; Segurança; Vulnerabilidades

INTRODUÇÃO

A previsibilidade do texto-plano de informações criptografadas sendo transportadas em pacotes pela rede pode fornecer a uma entidade maliciosa informações necessárias para a criação de diversos ataques quando tal entidade possui acesso a esses pacotes. O reconhecimento de pacotes criptografados que podem ser usados em ataques é, em geral, baseado no tamanho do pacote e na associação desse tamanho ao conteúdo em texto-plano que o mesmo potencialmente carregava antes de ser criptografado. Tradicionalmente, o tipo de ataque onde se conhece previamente o texto-plano de mensagens cifradas para a obtenção da chave de criptografia é chamado de ataque de *puro-texto conhecido* (*Known-Plaintext Attack*). Em tese, muitos dos algoritmos de criptografia são seguros contra esse tipo de ataque, pois impedem que o acesso ao texto-plano em conjunto com o texto-cifrado revele informações sobre a chave criptográfica utilizada.

Recentemente, foram desenvolvidos diversos ataques, como em [1], [2], [3] e [4] que se utilizam de pacotes criptografados com tamanho e texto-plano conhecidos. Analisando-se esses trabalhos, observa-se que tanto protocolos de segurança que atuam em meio guiado quanto em meio não guiado ou sem fio são afetados, mas que o foco desses ataques são as redes IEEE 802.11. As vulnerabilidades são exploradas em decorrência de problemas inerentes aos algoritmos de criptografia adotados e de características dos pacotes que trafegam na rede. Este artigo propõe um mecanismo, denominado EPP (*Eliminador de Previsibilidade de Pacotes*), que visa solucionar as vulnerabilidades decorrentes da previsibilidade do tamanho e do texto-plano de pacotes criptografados. O mecanismo proposto atua antes do pacote ser criptografado, inserindo informações que alteram suas características previsíveis e, em consequência, modificando seu tamanho original.

MATERIAIS E MÉTODOS

Existem diversos exemplos na literatura de ataques que foram criados com base na previsibilidade de informações de determinados pacotes que trafegam criptografados [1], [2], [3] e [4]. Geralmente, os ataques que utilizam esse tipo de técnica são baseados em pacotes de tamanho reduzido, como pacotes do TCP (*e.g. SYN, ACK, RST e FIN*), pacotes ARP (*Address Resolution Protocol*) e pacotes DNS (*Domain Name System*). Esta seção apresenta os ataques PTW [4], Beck-Tews [1] e Ohigashi-Morii [2], os quais motivaram o

desenvolvimento do EPP, explicando como esses ataques a redes IEEE 802.11 utilizam a previsibilidade de tamanho e conteúdo de pacotes do tipo ARP.

Em [4] é apresentado o ataque mais recente contra redes IEEE 802.11 protegidas pelo WEP [6] em que se explora a previsibilidade do conteúdo e tamanho de pacotes. Para funcionar, o ataque precisa obter uma quantidade suficiente de *keystreams* do RC4 utilizados na criptografia de pacotes de interesse. Nesse ataque, os pacotes de interesse são pacotes do tipo ARP criptografados.

O reconhecimento de pacotes do tipo ARP criptografados também é possível mesmo que o protocolo WPA [8] seja utilizado para proteger a rede sem fio, o que resultou no ataque Beck-Tews [1]. O ataque Beck-Tews realiza inicialmente a captura de pacotes ARP criptografados. Como os endereços físicos nos quadros não são cifrados e um quadro contendo um pacote ARP é facilmente reconhecido pelo seu tamanho, uma parte significativa do conteúdo dos pacotes ARP torna-se previamente conhecido pelo atacante. Para decifrar o restante do pacote, é realizado um ataque do tipo *chopchop* [5] que foi originalmente inventado para se descobrir, sem a necessidade da chave criptográfica, o texto-plano de pacotes criptografados pelo WEP.

O ataque Beck-Tews leva em consideração as medidas de prevenção ao *chopchop* inseridas no WPA: renegociação imediata das chaves em caso de mais de dois erros de MIC (*Message Integrity Check*) no intervalo de 60 segundos; e descarte do quadro, caso o número de sequência TSC (*TKIP Sequence Counter*) seja menor que o TSC atual do canal [5]. Após a obtenção de todo o texto-plano do pacote ARP e dos campos de verificação de integridade criptografados do quadro que carrega o ARP, o atacante é capaz de inverter o algoritmo de integridade *Michael* utilizado, levando-o a obtenção da chave de integridade.

De posse dessa chave, o atacante tem a possibilidade de enviar aos clientes da rede um determinado número de pacotes criptografados que serão considerados legítimos e íntegros por eles. Dessa forma, explorando o conteúdo desses pacotes, é possível a criação de novos ataques.

Recentemente, Ohigashi e Morii [2] estenderam o ataque Beck-Tews. Nesse novo ataque, o atacante se posiciona fisicamente em um local onde possa se comunicar com cliente e o ponto de acesso, mas sem que tais entidades consigam se comunicar diretamente (ataque *man-in-the-middle*). Em seguida, o atacante executa um ataque Beck-Tews modificado. Esse ataque melhora o ataque Beck-Tews original ao eliminar o requisito da rede estar utilizando Qualidade de Serviço (IEEE 802.11e) no momento do ataque. Tanto esse novo ataque quanto o ataque Beck-Tews original pode explorar adicionalmente a previsibilidade de tamanho e conteúdo de pacotes DNS.

RESULTADOS

O principal resultado desse trabalho é o mecanismo denominado EPP (*Eliminador de Previsibilidade de Pacotes*) e sua ideia básica é atuar antes do pacote ser criptografado, inserindo informações que alteram as características previsíveis do pacote e, em consequência, modificam o tamanho original do mesmo. A solução utiliza um algoritmo do tipo HMAC (*Hash-based Message Authentication Code*) [7] para gerar de forma aleatória a quantidade de *dummy bytes* inseridos e a posição em que cada um deles será colocado no pacote. As Figuras 1 e 2 apresentam respectivamente os procedimentos de inserção e remoção dos *dummy bytes* do EPP, os quais serão discutidos na próxima seção.

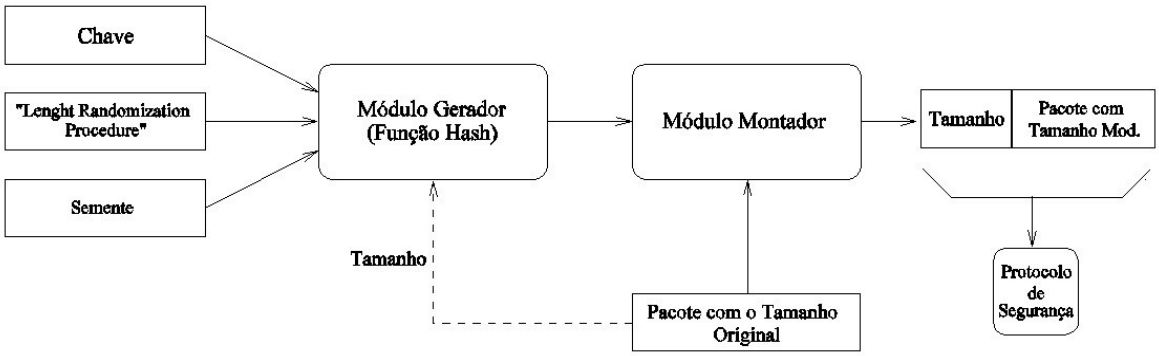

Figura 1 - Procedimento de Inserção do EPP

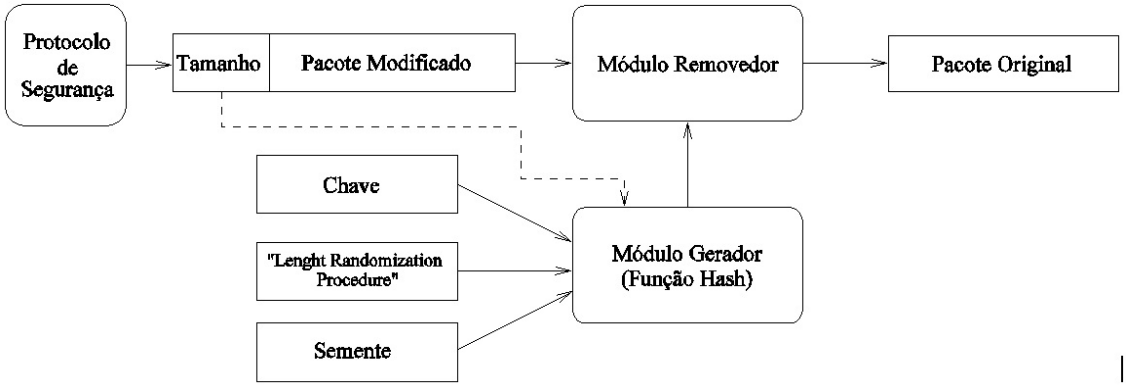

Figura 2 - Procedimento de Remoção do EPP

DISCUSSÃO

O EPP modifica o tamanho e conteúdo dos pacotes antes dos mesmos serem criptografados. Para isso, ele insere uma quantidade aleatória de *bytes* em posições também aleatórias no conteúdo dos pacotes. O mecanismo proposto é composto de dois procedimentos: procedimento de inserção de *bytes* e procedimento de remoção de *bytes*. Esses procedimentos serão detalhados abaixo.

Procedimento de Inserção: Como mostrado na Figura 1, o procedimento de inserção do EPP é composto por dois módulos: módulo gerador e módulo montador. O módulo gerador define a quantidade de *bytes* (*dummy bytes*) a ser inserida e a posição em que cada um desses *bytes* deve ser inserido no pacote. O módulo montador insere os *dummy bytes* nas posições corretas e repassa o pacote modificado para protocolo de segurança.

Procedimento de Remoção: A Figura 2 apresenta o mecanismo de remoção do EPP. Ele atua após o pacote ser decifrado pelo protocolo de criptografia. Há uma estrutura em dois módulos, semelhante ao mecanismo de inserção. O módulo gerador é utilizado novamente no mecanismo de remoção e recebe os mesmos parâmetros recebidos durante o procedimento de inserção. Assim sendo, ele obtém a mesma informação sobre a quantidade de *dummy bytes* inseridos no pacote e sobre o posicionamento deles. O módulo removedor recebe o pacote e a saída do módulo gerador e remove os *dummy bytes*, devolvendo o pacote com tamanho e conteúdo originais.

Como apresentado anteriormente, os ataques Beck-Tews e Ohigashi-Morii utilizam a previsibilidade de pacotes pequenos para descobrir a chave *MIC* e forjar pacotes que podem ser injetados como autênticos e íntegros na rede. O mecanismo, ao ser implementado com o WPA, evita os dois ataques através da inviabilização da

previsibilidade do tipo do pacote e de seu conteúdo original em texto-plano. A dificuldade de se descobrir o tipo dos pacotes criptografados capturados ocorre devido à inserção de *dummy bytes*, fazendo com que o tamanho dos pacotes varie de forma aleatória. Além disso, como os *dummy bytes* são inseridos em posições aleatórias, mesmo que o atacante ainda suponha corretamente o tipo do pacote capturado, haverá alterações significativas de conteúdo, eliminando a previsibilidade. Na prática, o uso do EPP faz com que a descoberta da chave do *MIC* se torne difícil, pois ela depende da correta avaliação do tipo do pacote capturado e do conhecimento prévio de seu conteúdo original em texto-plano. No caso específico dos dois ataques citados, sem a chave *MIC*, eles se tornam inoperantes, pois não será possível forjar e injetar pacotes na rede.

CONCLUSÕES

A previsibilidade de informações em alguns tipos de pacotes oferece riscos à segurança das próprias redes. Essa característica foi utilizada em ataques contra diversos protocolos de segurança, principalmente em redes IEEE 802.11. Com base nesse problema, esse artigo propôs um mecanismo, denominado EPP, que elimina a previsibilidade de tamanho e conteúdo de pacotes através da inserção de uma quantidade aleatória de *bytes* em posições igualmente aleatórias.

Um fator relevante sobre o EPP é o fato de sua arquitetura ser significativamente simples e a mesma poder ser adaptada para operar em conjunto com outros protocolos de segurança de redes de computadores. Quando usado em conjunto com o WPA, o EPP apresenta resultados imediatos, pois evita os ataques Beck-Tews e Ohigashi-Morii.

AGRADECIMENTOS

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

REFERÊNCIAS

[1] - Beck, M. and Tews, E. (2009). Practical Attacks Against WEP and WPA. In P*roceedings of the Second ACM Conference on Wireless Network Security -WiSec'09*, pages 79–86.

[2] - Ohigashi, T. and Morii, M. (2009). A Practical Message Falsification Attack on WPA. In *Proceedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System*.

[3] - Paterson, M. R., Watson, K. G., and Albrecht, G. J. (2009). Plaintext Recovery Attacks Against SSH. In *Procedings of IEEE Symposium on Security and Privacy*, pages 16–26.

[4] Tews, E., Weinmann, R.-P., and Pyshkin, A. (2007). Breaking 104 Bit WEP in Less Than 60 Seconds. *Lecture Notes in Computer Science - Information Security Applications*, (4867):188–202.

[5] - KoreK (2004). Chopchop (Experimental WEP Attacks).

[6] - Hayes, V. et al. (1999). IEEE Standard 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Computer Society*.

[7] - Krawczyk et al. (1997). HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Informational).

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