Previsibilidade de Dados e Impactos na Segurança das Redes IEEE 802.11

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: Este trabalho apresenta um conjunto de estudos sobre a previsibilidade dos dados de pacotes que trafegam em redes de computadores e sobre possíveis impactos na segurança das redes IEEE 802.11. Primeiramente, foi realizada a coleta de pacotes na rede do Centro de Informática. Em segundo lugar, experimentos analisam a previsibilidade do tamanho dos pacotes do tipo ARP, DNS e requisições HTTP. Por fim, um experimento analisa o conteúdo dos pacotes do tipo ARP utilizando uma técnica conhecida como *(p,n)-grams*. Os resultados obtidos mostram que existem previsibilidades em determinados tipos de pacotes, principalmente nos do tipo ARP, e que os impactos das mesmas na segurança das redes IEEE 802.11 são bastante significativos.

Palavras–chave: IEEE 802.11; Pacotes; Previsibilidade

INTRODUÇÃO

As redes sem fio abrangem uma diversidade de tecnologias cujas diferenças incluem, por exemplo, a freqüência utilizada, o alcance e os protocolos envolvidos. Dentre as tecnologias mais promissoras para redes públicas de acesso sem fio à Internet (hotspots) e redes locais sem fio internas de prédios, casas, aeroportos e escritórios encontra-se o IEEE 802.11 ou Wi-Fi (***Wi***reless ***Fi***delity). Atualmente, a segurança é o maior problema relacionado ao uso dessas redes [1,2,3,4]. Os principais padrões de segurança do IEEE 802.11 são o *Wired Equivalent Privacy* (WEP), o *Wi-Fi Protected Acess* (WPA) e o IEEE 802.11i (WPA2). Existe ainda o padrão IEEE 802.11w que ainda se encontra em desenvolvimento.

O protocolo WEP é reconhecidamente fraco por ser vulnerável a uma série de ataques estatísticos [1,2,3]. O ataque mais recente ao WEP conhecido como PTW [4] utiliza a previsibilidade dos dados contidos em pacotes que trafegam pela rede para recuperar, em poucos minutos, a chave de segurança utilizada pelo protocolo.

O WPA possui correções para a grande maioria das vulnerabilidades presentes no WEP, no entanto recentemente foi desenvolvido um ataque [4] capaz de injetar pacotes falsos em uma rede protegida pelo WPA. Para conseguir burlar o algoritmo Michael, responsável por evitar esse tipo de ataque, é utilizada uma combinação de pequenas falhas na configuração padrão do WPA com a previsibilidade dos dados contidos nos pacotes do tipo ARP.

Os dois ataques citados anteriormente são conhecidos em criptografia como k*nown-plaintext attacks*, ou seja, ataques nos quais é possível estabelecer uma relação entre o texto cifrado e o texto puro devido a algum tipo de previsibilidade. Portanto, o estudo da previsibilidade do conteúdo de pacotes que trafegam na rede é necessário para que fique claro quais tipos de pacotes possuem conteúdo previsível e até que ponto essa previsibilidade pode ter impacto nos protocolos de segurança que protegem as redes IEEE 802.11. Além disso, o estudo proposto neste artigo serve de base para a proposição de mecanismos de defesa e prevenção contra esse tipo de vulnerabilidade.

MATERIAIS E MÉTODOS

Coleta de pacotes: Os quatro tipos de pacotes coletados foram: ARP, requisições DNS, respostas DNS e requisições HTTP. Os do tipo ARP foram selecionados por terem sido utilizados em dois ataques aos protocolos de segurança das redes IEEE 802.11. Os outros três tipos foram escolhidos por serem pacotes muito utilizados pelos navegadores da Internet e por terem partes dos cabeçalhos intuitivamente previsíveis. Essa coleta foi realizada na rede do Centro de Informática através dos programas W*ireshark* e *TCPdump.*

Experimentos com o tamanho dos pacotes: O primeiro experimento realizado analisa a previsibilidade do tamanho dos pacotes capturados. Essa análise é muito importante, já que a maioria dos protocolos de segurança não modifica o tamanho de um pacote ao cifrar os dados contidos no mesmo.

Os *scripts* desenvolvidos para esse experimento coletam o tamanho de cada pacote e organizam os dados em tabelas. Estas tabelas são usadas na construção de quatro tipos de gráficos (*PDF*, *scatterplot*, *CDF* e *CCDF*), que apresentam a distribuição de tamanho de cada tipo de pacote.

Experimentos com o conteúdo dos pacotes do tipo ARP: O objetivo desse experimento foi comparar todos os bytes dos pacotes ARP utilizando a técnica dos *(p,n)-grams*[5,6], identificando os *(p,n)-grams* mais freqüentes e conseqüentemente as partes mais previsíveis desse tipo de pacote. Essa técnica realiza a detecção de pacotes em uma rede de alta velocidade. Para que isso seja possível é feita uma pré-analise do tipo de pacote a ser detectado com o intuito de encontrar o(s) *(p,n)-grams* mais relevantes para aquele tipo.

Um ***(p,n)-gram*** relevante é um conjunto ***n*** bytes (em geral o ***n*** utilizado é 2) que se repetem freqüentemente num determinado tipo de pacote com um deslocamento ***p*** em relação ao início do mesmo. Quanto maior a quantidade de *(p,n)-grams* um tipo de pacote possui mais fácil se torna sua identificação. Vale ressaltar que quanto mais freqüente for um determinado *(p,n)-gram*, mais previsível aquele conjunto de ***n*** bytes se torna.

Para esse experimento todos os ARPs utilizados possuíam 60 *bytes* de dados e o **n** foi fixado em 2, resultando num total de trinta *(p,n)-grams* por pacote. Os *scripts* desenvolvidos realizam a captura dos trinta *(p,n)-grams* de cada pacote, armazenando-os em arquivos separados. Em seguida esses arquivos são comparados e os *(p,n)-grams* contidos nos mesmos são organizados do mais para o menos freqüente.

RESULTADOS

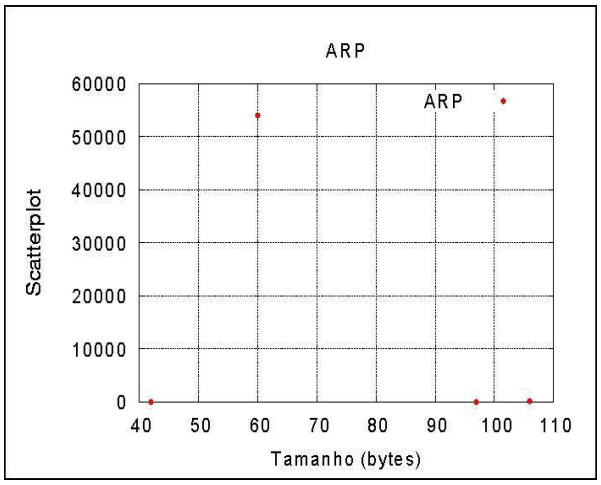

Figura 1 – *Scatterplot* do tamanho dos ARPs

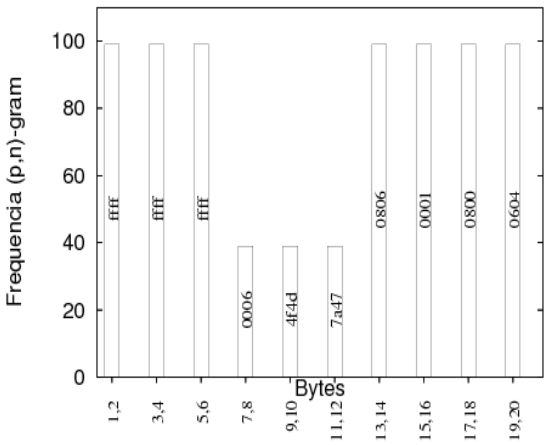

Figura 2 – Freqüência dos (p,n)-grams 1 a 10

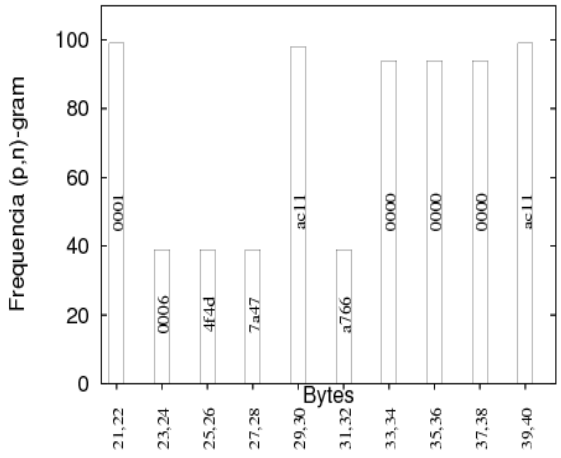

Figura 3 – Freqüência dos (p,n)-grams 11 a 20

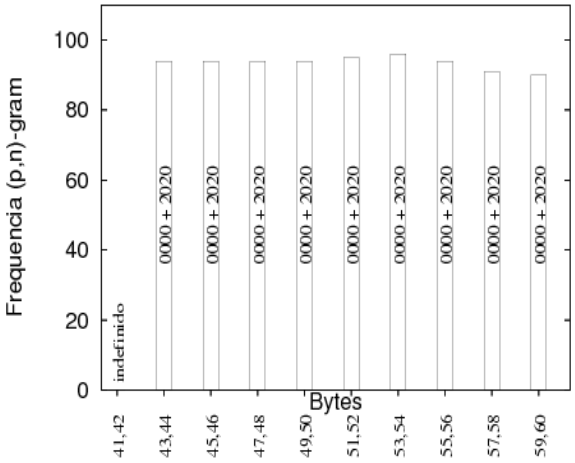

Figura 4 - Freqüência dos (p,n)-grams 21 a 30

DISCUSSÃO

A Figura 1 apresenta o *scatterplot* do tamanho dos ARPs. Este resultado mostra que mais de 99% dos 54347 pacotes utilizados no experimento possuem 60 *bytes* de tamanho, o que deixa claro que os ARPs possuem tamanho previsível.

Os resultados do primeiro experimento para os demais tipos de pacote mostram que o tamanho dos mesmos não é previsível como o dos pacotes do tipo ARP. No caso das Requisições DNS o tamanho varia entre 65 e 95 *bytes*. Nas Respostas DNS ele é ainda menos previsível, variando entre 50 e 600 *bytes*. Nas Requisições HTTP ocorreu a maior desigualdade, com uma variação de 200 a 1500 *bytes*.

A Figura 2 apresenta os *(p,n)-grams* mais relevantes para as dez primeiras duplas de *bytes* consecutivos. Nessa figura é importante ressaltar que a freqüência superior a 98% dos *(p,n)-grams* nos conjuntos de *bytes* 1 a 6, 13 a 14, 15 a 16, 17 a 18 e 19 a 20 mostra que existe previsibilidade nos campos representados pelos conjuntos (respectivamente: endereço MAC de destino (camada enlace), tipo de pacote (camada enlace), tipo de *hardware* (ARP), tipo de protocolo (ARP) e tamanho do *hardware* e do protocolo (ARP)).

A Figura 3 apresenta os *(p,n)-grams* mais relevantes para as dez duplas de *bytes* consecutivos subseqüentes. Nessa figura é importante ressaltar que a freqüência superior a 94% dos *(p,n)-grams* nos conjuntos de *bytes* 21 a 22 e 33 a 38 mostra que existe previsibilidade nos campos representados pelos mesmos (respectivamente: *Opcode*(ARP) e endereço MAC de destino (ARP)).

A Figura 4 apresenta os *(p,n)-grams* mais relevantes para as dez últimas duplas de *bytes* consecutivos. Nessa figura é importante ressaltar que a freqüência superior a 90% dos dois *(p,n)-grams* mais relevantes cominados (“0000” e “2020”) no conjunto de *bytes* 43 a 60 mostra que existe previsibilidade no campo *trail* (camada enlace), que é representado pelos mesmos.

É importante ressaltar que os resultados dos *bytes* 7 a 12, 23 a 28, 29 a 32 e 39 a 42 sofrem grandes variações dependendo das configurações da rede. Isso ocorre porque essas configurações influenciam diretamente os campos representados por esses conjuntos de *bytes* (respectivamente: endereço MAC de origem (camada enlace), endereço MAC de origem (ARP), endereço IP de origem (ARP) e endereço IP de destino (ARP)).

Os resultados do segundo experimento deixam claro que dos 60 *bytes* de dados presentes em um ARP pelo menos 40 são previsíveis. Além disso, se for possível obter algum conhecimento prévio sobre a configuração do IP da rede e se a rede que estiver transportando

esses dados for IEEE 802.11, nas quais os endereços MAC de destino e de origem não são protegidos por criptografia, o número de *bytes* previsíveis sobe de 40 para 56.

CONCLUSÕES

Neste artigo foram realizados estudos sobre a previsibilidade dos dados de pacotes que trafegam em redes de computadores e sobre possíveis impactos na segurança das redes IEEE 802.11. Os experimentos realizados demonstraram que os pacotes do tipo ARP possuem tamanho e conteúdo previsíveis. Esse tipo de previsibilidade auxilia no desenvolvimento de k*nown-plaintext attacks,* assim sendo mais pesquisas devem ser feitas para que mecanismos e técnicas de defesa possam ser desenvolvidos, evitando que novos ataques desse tipo sejam usados contra os protocolos de segurança das redes IEEE 802.11

AGRADECIMENTOS

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

REFERÊNCIAS [centralizado, negrito]

[1] - A. Vladimirov, K. V. Gavrilenko, e A. A. Mikhailovsky, "*Wi-Foo: The Secrets of Wireless Hacking,"* Addison Wesley, 1ª Edição, 2004.

[2] - S. Fluhrer, I. Mantin, e A. Shamir, "*Weaknesses in the key scheduling algorithm of RC4,"* Lecture Notes in Computer Science, 2001.

[3] - D. Hulton, "*Practical Exploitation of RC4 Weaknesses in WEP Environments,"* Dachb0den Labs, 2002.

[4] - Tews, E. and Beck, M. 2009. Practical attacks against WEP and WPA. In *Proceedings of the Second ACM Conference on Wireless Network Security* (Zurich, Switzerland, March 16 - 19, 2009). WiSec '09. ACM, New York, NY, 79-86. DOI= http://doi.acm.org/10.1145/1514274.1514286

[5] – Matrawy, A.; van Oorschot, P.C.; Somayaji, A., "Mitigating network denial-of-service through diversity-based traffic management," In Applied Cryptography and Network Security (ACNS'05), pages 104–121. Springer Science+Business, Media,2005.

[6] – Hijazi, A.; Inoue, H.; Matrawy, A.; van Oorschot, P.C.; Somayaji, A., "Discovering Packet Structure through Lightweight Hierarchical Clustering," Communications, 2008. ICC '08. IEEE International Conference on, vol., no., pp.33-39, 19-23 May 2008.