UMA ANÁLISE DO MECANISMO DE SEGURANÇA DE REDES IEEE 802.11: WEP

André Guedes Linhares[1]; Paulo André da S. Gonçalves[2]

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

Resumo: Este artigo apresenta uma avaliação experimental do mecanismo de segurança de redes IEEE 802.11 denominado *Wired Equivalent Privacy* (WEP). Embora diversas pesquisas tenham demonstrado problemas significativos de segurança desse mecanismo, nenhuma avaliação experimental, com base em ferramentas de domínio público, sobre a eficiência de ataques ao WEP para a recuperação da chave foi realizada. A contribuição deste trabalho reside na demonstração experimental da eficiência de ataques de recuperação de chaves em redes protegidas pelo WEP. Os resultados enfatizam a fraqueza do WEP e demonstram que o índice de sucesso dos ataques na recuperação de chaves é tão alto quanto 91,74%.

Palavras-Chave: Segurança, IEEE 802.11, WEP.

INTRODUÇÃO

A segurança de redes é freqüentemente tratada pelas camadas mais altas da pilha de protocolos e na maioria das vezes é vista apenas como um problema da camada aplicação. Com o advento das redes locais sem fio (WLANs – Wireless Local Area Networks) este paradigma de segurança sozinho se mostra inadequado. Assim, as WLANs necessitam de componentes de segurança presentes na camada enlace para proteger o acesso à rede e manter a confidência dos dados que transitam na mesma.

Com este intuito, o protocolo WEP foi proposto para uso em WLANs IEEE 802.11. Contudo, diversas pesquisas [3, 4, 5, 7] demonstraram problemas significativos de segurança neste mecanismo, sendo possível a recuperação da chave que protege a rede sem conhecimento prévio da mesma. Em 2003, o WEP foi então substituído pelo WPA (*Wi-Fi Protected Access*) que por sua vez, devido a algumas falhas de implementação, foi substituído, em 2004, pelo padrão IEEE 802.11i ou WPA2 [6].

Este trabalho apresenta uma avaliação experimental da eficiência de ataques de recuperação de chave em redes protegidas pelo WEP. A contribuição reside na demonstração da eficiência dos ataques com base no uso de ferramentas de domínio público.

Em resumo, o WEP provê dois métodos de autenticação de dispositivos, utiliza CRC-32 (Cyclic Redundancy Checks) para a verificação da integridade de dados e usa o algoritmo de criptografia RC4 (Ron´s Code #4) para prevenir a leitura de dados de usuário que transitarão na rede. Além disto, um vetor de inicialização (IV) é utilizado para garantir que um mesmo dado tenha cifras diferentes, aumentado a entropia do sistema. O IV nada mais é do que um vetor de 3 bytes que é gerado randomicamente (ou de forma incremental) pelo *firmware* da placa Wi-Fi (*Wireless Fidelity*). O IV é, então, concatenado a chave WEP que será utilizada pelo RC4. A partir desta é gerado um IV para cada pacote cifrado.

O WEP pode ser utilizado entre o Ponto de Acesso (AP – *Access Point*) e os clientes da rede (modo com infra-estrutura), assim como na comunicação direta entre clientes (modo ad-hoc).

Dentre as diversas vulnerabilidades apresentadas pelo WEP as seguintes se destacam: re-injeção de pacote, problemas no RC4 facilitando a recuperação da chave, negação de serviço, protocolo de autenticação ineficiente.

MATERIAIS E MÉTODOS

Para a realização deste trabalho, foi feito um levantamento do estado da arte da segurança em redes IEEE 802.11. Foram pesquisados os problemas que levaram a evolução dos mecanismos de segurança dessas redes, assim como os ataques de recuperação de chaves desenvolvidos até então.

Para a avaliação experimental relacionado a este trabalho, foram utilizados os seguintes equipamentos: 1) 3 PCs P4 com 1GB RAM e sistema operacional Ubuntu Linux 6.10; 2) 2 placas D-Link AirPlus G DWL-G510 *Wireless* PCI *Adapter* (rev.B); e 3) 1 Ponto de Acesso (AP) AirPlus G DWL-G700AP. A Figura 1 apresenta o cenário básico utilizado nos experimentos.

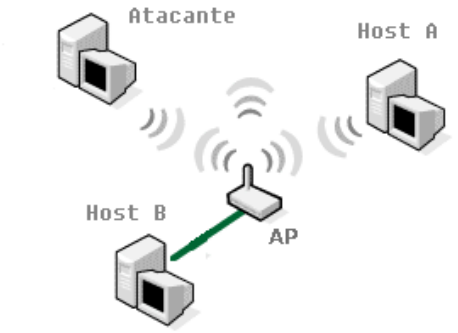

Figura 1 – Cenário dos experimentos

A geração de tráfego foi realizada utilizando-se o programa *iperf*. Foi utilizado um tráfego CBR (*Constant Bit Rate*) com pacotes UDP (*User Datagram Protocol*) sendo enviados do *host* A para o *host* B. A máquina "atacante" era responsável pela captura de pacotes sendo enviados pela rede sem fio e pelos ataques de recuperação de chave. Foram realizados ataques de recuperação de chave do tipo FMS/KoreK com o auxilio da ferramenta Aircrack-ng 0.9 configurada com os seus parâmetros padrões.

Foram realizados diversos ataques com diferentes taxas de transmissão, tamanho de pacotes e chaves WEP. Foram utilizadas as seguintes chaves WEP escolhidas aleatoriamente: 1) Chave 1 (C1): sTo4hOuh176la (apenas letras e números); 2) Chave 2 (C2): c-i*S3ia+ri2p (letras, números e caracteres especiais); 3) Chave 3 (C3): Sw6##IeCrO+2= (letras, números e caracteres especiais); e 4) Chave 4 (C4): aaaaaaaaaaaa (todos os dígitos iguais).

Foram utilizadas 3 taxas de transmissão diferentes: 1) 7 MBit/s (taxa "baixa". Experimentos com taxas menores que 7MBit/s levariam muito tempo para serem executados); 2) 15 MBit/s (taxa mediana) e 3) 20 MBit/s (taxa próxima da saturação do canal).

Foram utilizados dois tamanhos de pacotes: 1) 500 Bytes (tamanho médio dos pacotes http - HyperText Transfer Protocol) e 2) 1470 Bytes (valor máximo para evitar fragmentação de pacotes).

RESULTADOS

Ao longo da execução de todos os experimentos a taxa de perda de pacotes foi constantemente monitorada para que não fossem gerados dados não condizentes com a realidade. Com a taxa de perda elevada poucos IVs seriam capturados pelo atacante e desta

forma não seria possível quebrar a chave. Portanto, ataques que poderiam vir a ter sucesso fracassariam. A taxa média de perda observada durante os experimentos foi de aproximadamente 0,0025%.

As figuras a seguir apresentam os principais resultados alcançados. O *label* utilizado possui o seguinte significado: allM - todas as taxas de transmissão;, Pall – todos os tamanhos de pacotes; FMS – tipo do ataque utilizado; Call – todas as chaves.

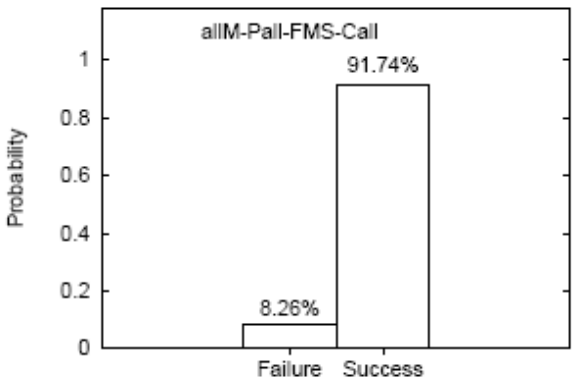

Figura 2 - Probabilidade de ataques realizados com sucesso e fracasso

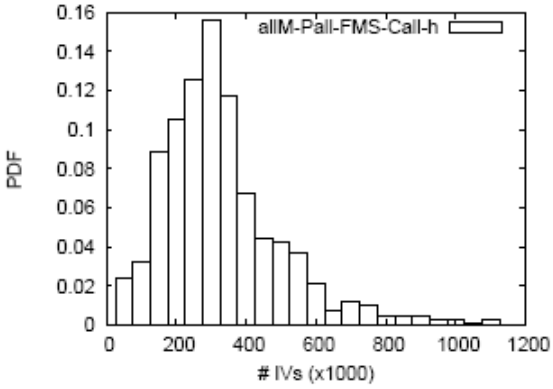

Figura 3 - Probabilidade do ataque ser bem sucedido com a captura do número de IVs indicado

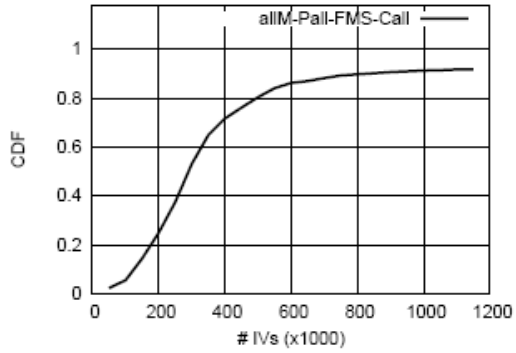

Figura 4 - Distribuição da probabilidade acumulada de um ataque ser bem sucedido dado o número de IVs já capturados

DISCUSSÃO

Durante a execução dos experimentos foram monitorados os ataques que falharam, ou seja, ataques que não foram capazes de recuperar a chave WEP. A Figura 2 mostra que a grande maioria dos ataques foram realizados com sucesso (91,74%), em contraste com os poucos que falharam (8.26%). Isto demonstra que uma investida de um atacante contra uma rede Wi-Fi protegida pelo protocolo WEP tem uma altíssima probabilidade de sucesso. Dado que qualquer pessoa com certo conhecimento das ferramentas existentes pode atacar uma rede Wi-Fi protegida por WEP, mesmo que não saiba como realmente funciona o ataque e que um atacante tem 91.74% de chance de obter sucesso no seu ataque, as redes protegidas por WEP, na verdade, são bastante vulneráveis, causando um grande risco para os seus usuários.

A Figura 3 apresenta a distribuição do número de IVs necessário para a recuperação da chave. Observa-se que a distribuição é do tipo cauda longa, onde poucos ataques precisaram de mais de 800 mil IVs para recuperar com sucesso a chave WEP. Assim, capturar mais de 800 mil IVs não aumenta em quase nada a probabilidade de sucesso para recuperação da chave.

A Figura 4 apresenta a probabilidade acumulada de obtenção de sucesso na recuperação da chave WEP dado que determinada quantidade de IVs já foram capturados. Com um pouco mais de 200 mil IVs a probabilidade de recuperar a chave foi de aproximadamente 23%. Porém, com 600 mil IVs a probabilidade de sucesso cresce significativamente chegando a aproximadamente 83%. E finalmente, observa-se que após 800 mil IVs capturados, a probabilidade de sucesso para recuperar a chave não aumenta significativamente.

CONCLUSÕES

As vulnerabilidades do WEP são muito fáceis de serem exploradas. Qualquer pessoa com certo conhecimento das ferramentas existentes pode atacar uma rede IEEE 802.11 protegida pelo WEP, mesmo que não saiba como realmente funciona o ataque. Desta forma, a segurança da maioria dessas redes pode ser comprometida. Com base nos taxa de transmissão de dados na rede, a recuperação da chave WEP pode ser realizada em questão de minutos ou até mesmo dezenas de segundos. Isso se deve ao fato que redes com altas taxas de transmissão geram mais pacotes por segundo e, conseqüentemente, mais IVs.

AGRADECIMENTOS

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

REFERÊNCIAS

[1] - Shafi, M et al, 1997. “Wireless communications in the twenty-first century: a perspective”. *Proceedings of the IEEE*. Vol 85, No 10, pp 1622 – 1638.

[2] - IEEE 802.11 WG, 1999. “Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specification”. *IEEE Computer Society.*

[3] - Borsc, M.e Shinde, H., 2005. “Wireless security & privacy”. *Conference on Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International*. pp 424 – 428.

[4] - Boland, H.e Mousavi, H., 2004. “Security issues of the IEEE 802.11b wireless LAN”. *Canadian Conference on Electrical and Computer Engineering*. Vol 1, pp 333 – 336.

[5] - Fluhrer, S., Mantin, I. e Shamir, A., 2001. “Weaknesses in the key scheduling algorithm of RC4”. *Eighth Annual Workshop on Selected Areas in Cryptography*.

[6] - IEEE 802.11i WG, 2004. “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements”. *IEEE Computer Society.*

[7] - Shunman, W., 2003. “WLAN and its security problems”. *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'2003)*. pp 241 – 244.