Segurança em Redes IEEE 802.11: Um Estudo de Caso

Bruno Gentilini D'Ambrosio[1] ; Paulo André da Silva Gonçalves[2]

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

Resumo: Este artigo apresenta uma avaliação sobre a força das chaves *Wired Equivalent Privacy* (WEP), protocolo de segurança da camada enlace para redes IEEE 802.11. Foram feitos ataques a uma rede configurada com duas chaves diferentes, uma intuitivamente simples, sem caracteres especiais e outra complexa, apenas com caracteres especiais, com o objetivo de descobrir se a complexidade da chave influencia na segurança do protocolo. Os resultados mostram que ao contrário do que se pode imaginar a complexidade da chave não influencia na segurança do protocolo, sendo essa a maior contribuição desse artigo.

Palavras–chave: chaves; segurança; WEP;

INTRODUÇÃO

O WEP foi criado por necessidade em 1999, visto a falta de segurança existente nas redes IEEE 802.11[1,6,7] na época. Seu objetivo inicial era tentar simular a segurança das redes cabeadas, no entanto foi desenvolvido por uma equipe de profissionais não especializados na área de segurança, os quais cometeram erros que acarretaram em falhas de segurança[2,3,4,5]. Devido a essas falhas o WEP não é recomendado nem mesmo para usuários domésticos.

Nos últimos anos, o maior desafio tem sido convencer os usuários a adotar protocolos de segurança mais modernos que o WEP, pois os mesmos possuem uma configuração menos intuitiva. Devido a essa simplicidade de configuração o WEP ainda é o protocolo mais utilizado nas redes IEEE 802.11.

Este artigo compara o comportamento de duas chaves, uma intuivamente simples e outra complexa, com a finalidade de verificar se a complexidade da chave influencia no nível de segurança do protocolo WEP, melhorando ou piorando o seu desempenho na proteção da rede. Para isso foram realizados experimentos em um ambiente simulado.

MATERIAIS E MÉTODOS

As chaves de segurança: O protocolo *WEP* utiliza uma chave de segurança que deve ser inserida tanto no ponto de acesso, no momento da configuração do protocolo de segurança, como no computador que deseja se conectar a rede. Ambas as chaves utilizadas possuiam 13 caracteres *ASCII*, no entanto a primeira, tida como mais simples, era composta apenas por caracteres alfanuméricos, já a segunda, tida como mais complexa, era composta somente por caracteres especiais. As chaves utilizadas foram denominadas C5 e C6, sendo a C5 a complexa composta pelos 13 caracteres !@#$%¨&*!@#$% e a C6 a simples composta pelos 13 caracteres filippo1234ti.

A plataforma: A plataforma base para os experimentos foi a mesma utilizada na etapa anterior composta por três computadores. O primeiro deles estava conectado ao ponto de acesso (AP - *Access Point*) via conexão com fio. O segundo estava conectado ao ponto de acesso pela rede sem fio. O terceiro computador foi o responsável pelos ataques, para isso

ele foi colocado em modo monitor, *i.e*, modo em que a interface de rede sem fio apenas captura os pacotes gerados por outras interfaces.

As Configurações: Os experimentos para cada chave foram divididos em dois grupos. No primeiro grupo , o segundo computador utilizava um *driver linux* para gerar tráfego e no segundo ele utilizava um *driver windows* com a mesma finalidade. A diferença básica entre os dois é que no *driver linux* os IVs mais sucetiveis a ataques são excluidos, já no windows somente o IV zero é excluido.

Dentro dos dois grupos foram usadas três configurações diferentes para geração de tráfego, feita através do programa *Iperf*. Na primeira e na segunda, a velocidade de transmissão utilizada foi de 20 *Mbits* e os tamanhos dos pacotes utilizados foram de 1470 e 500 *bytes*, respectivamente. Na terceira a velocidade foi de 7 *Mbits* e o tamanho de 500 *bytes*.

Os Experimentos: No total foram 12 experimentos realizados, 6 para cada chave. Em média cada experimento levava de 5 a 8 horas para ser concluído. As etapas para a realização dos mesmos são descritas abaixo:

Primeiramente a rede era configurada com uma das duas chaves selecionadas para o experimento. O *Iperf* recebia uma das três configurações e era executado tanto no primeiro computador, no modo servidor, como no segundo, no modo cliente, iniciando assim a transmissão de dados pela rede. No terceiro computador, previamente configurado em modo monitor, o *script* responsável pela realização dos ataques era executado. Esse *script* realizava sussecivos ataques a rede até que a senha fosse recuperada com sucesso 50 vezes, armazenando tanto os sucessos como os fracassos em arquivos individuais. Após os 50 sucessos o *script* era automaticamente encerrado.

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. A taxa média de perda nos experimentos não foi superior a 0,001%.

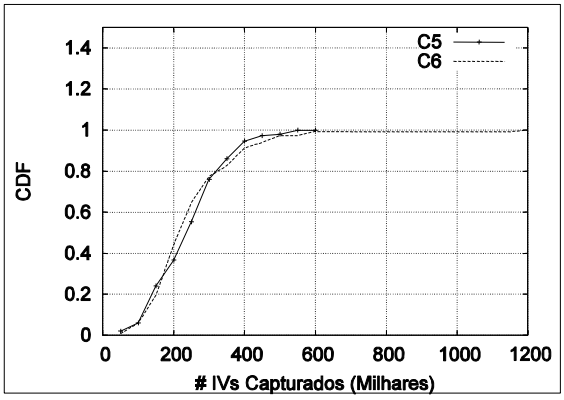

Figura 1 - CDF comparando as duas chaves

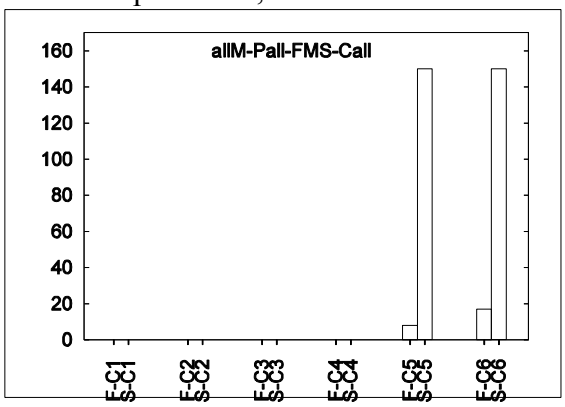

Figura 2 - Comparação de fracassos e sucessos de ambas as chaves

DISCUSSÃO

Os resultados dos experimentos foram surpreendentes, já que ao contrário do que se poderia imaginar o desempenho dos ataques a ambas as chaves não apresentou grandes diferenças, indicando que mesmo que a chave de segurança possua um maior nível de complexidade o protocolo WEP se mantém frágil.

Na Figura 1 temos o gráfico CDF com a comparação da probabilidade de que as chaves tenham sido quebradas dado que uma quantidade de IVs tenha sido capturada. Claramente,

o desempenho das duas chaves foi muito próximo e as variações ocorridas são desprezíveis.
Na Figura 2 temos a comparação do número de fracassos e sucessos na quebra das duas chaves. A diferença novamente é muito pequena para ser considerada e a chave que teve um pouco mais de fracassos era justamente a tida como mais simples, demonstrando que a complexidade da chave realmente não influencia na eficiência do protocolo WEP.

CONCLUSÕES

O WEP é um protocolo frágil independentemente da complexidade da senha. 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. O foco das pesquisas no momento deve ser em um modo de facilitar a configuração de protocolos de segurança mais atualizados.

AGRADECIMENTOS

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

REFERÊNCIAS

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

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

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

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

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

[6] - S. J. Kerry et al., “802.11g Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specification. Amendment 4: Further Higher Data Rate Extensionin the 2.4 GHz Band”, *IEEE Computer Society*. 2003.

[7] - S. J. Kerry et al., “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements”, *IEEE Computer Society*, 2004.