Relatório Ataques a Redes Wi-Fi

João Fiuza de Alencastro 15/0131933

***Abstract*—Relatório destinado à matéria de Segurança de Redes do Departamento de engenharia Elétrica da Universidade de Brasília. Experimento realizado a fim de explorar falhas físicas em redes que utilizam o protocolo IEEE 802.11.**

***Index Terms*—Segurança, redes, wifi, 802.11, WEP, WPA, aircrack-ng.**

I. Introdução

ATAQUES podem não ser somente a nível de aplicação. Muitas vezes ataques são feitos ao meio físico, um atacante pode conseguir um acesso a um cabo de rede mal posicionado, ou pode ter acesso a uma rede wireless pública. Esses são chamados de ataques infra-estruturados, os quais se utilizam de falhas físicas ou da camada de enlace para executar *exploits*.

Ataques infra-estruturados à redes wifi podem representar um enorme risco à sociedade, já que, atualmente, todos estão conectados a uma rede móvel 24 horas por dia. Talvez nem sempre a uma rede que utiliza o protocolo 802.11, porém em grande parte do tempo, com certeza, e é onde reside o problema que será abordado.

II. Desenvolvimento

A. Algoritmos de senha

Esses são os algoritmos e protocolos utilizados pelo equipamento wifi para realizar a verificação de senhas dos usuários. Dois algoritmos foram desenvolvidos para o protocolo IEEE 802.11, o **WEP** (Wired Equivalent Privacy) e o **WPA** (Wi-Fi Protected Access).

1) WEP: Algoritmo considerado desatualizado e simples, ainda é uma opção que pode ser escolhida em pontos de acesso. Apesar, de que a Wi-Fi Alliance já anunciou que o WEP foi substituído pelo WPA. O WEP era o único protocolo de criptografia disponível nos dispositivos configurados em 802.11a e 802.11b, dipositivos criados posteriormente ao protocolo 802.11g já possuiam segurança WPA.

Na figura 1, que se encontra logo abaixo, pode-se verificar um simples esquema de cifragem de mensagens utilizado pelo protocolo WEP.

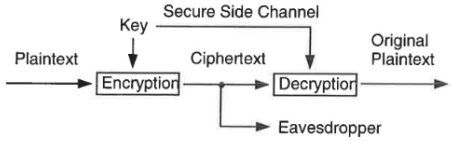

Fig. 1. Simples esquema de cifragem da mensagem utilizado pelo WEP. Fonte [1].

As especificações mais detalhadas e sua implementação podem ser encontradas em [1].

2) WPA: WPA era uma solução intermediária para a melhoria dos padrões de segurança estabelecidos anteriormente. Porém, WPA demonstrou vulnerabilidades significativas e foi posteriormente substituído pela sua segunda versão, WPA2.

Ambos WPA e WPA2 utilizam o mesmo método de autenticação, porém utilizam diferentes métodos de criptografia e algoritmos de integridade de dados. Redes corporativas utilizam frameworks **802.1 X/EAP** para sistemas centralizados de autenticação mútua, enquanto que redes pequenas e domésticas utilizam o **PSK** (Pré-Shared Key).

Na figura 2, vista abaixo, pode-se verificar uma comparação entre os *Throughputs* de redes que utilizam nenhum método de segurança, WPA e WPA2, respectivamente.

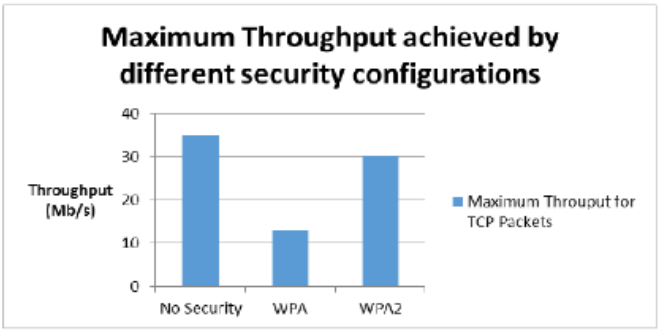

Fig. 2. Comparativo de 'throughput' de diferentes métodos de segurança. Fonte [2].

B. Ataques à redes Wi-Fi usando o aircrack-ng

Foi providenciado um dispositivo de ponto de acesso para a parte prática desse experimento, dispositivo no qual foi configurado com SSID 'seguranca' e método de segurança WEP, como mostra a figura 3 abaixo.

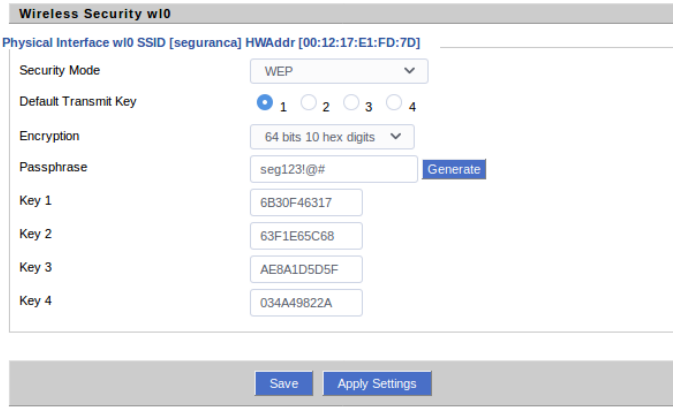

Fig. 3. Configuração feita no AP e demonstração de como funciona o WEP.

1) Descobrindo o SSID: Simulando um atacante, que de antemão não tem conhecimento algum sobre as redes wi-fi que estão ali presentes, deve-se descobrir o SSID da rede que será atacada, é utilizado então o wireshark (ou qualquer outro software '*sniffer*') e espera-se pacotes de '*Beacon*', que são pacotes de varredura e possuem informações sobre a rede 802.11.

Na figura 5, no final do relatório, é mostrado um exemplo de um pacote capturado quando é utilizada a interface de rede em modo 'monitor', ou promíscuo. Nele se encontram informações valiosas que qualquer um pode ver, tais como, endereço MAC dos dispositivos envolvidos e seus respectivos fabricantes, SSID da rede, banda de frequência utilizada, taxas de transmissão, entre outras.

2) Captura de pacotes: Agora, utilizando o modo promíscuo e a ferramenta airocrack-ng, capturam-se os pacotes trafegados no meio que contenham endereço MAC do AP que já é sabido pelo atacante. Foi utilizado o comando como super usuário:

```
# airodump-ng -c 6 --bssid
> 00:12:17:e1:fd:7d -w capture mon0
```

Dessa maneira, foi possível entrar em um modo onde o programa está rodando e é possível verificar várias informações sobre a captura, como mostra a figura 4 abaixo.

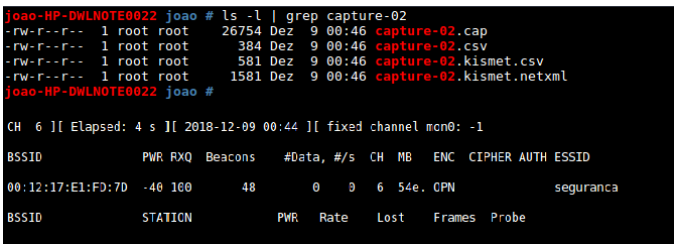

Fig. 4. Airodump rodando e seus arquivos de saída.

III. Conclusão

Primeiramente, o mais importante a se ressaltar é que deve-se tomar um cuidado extra ao se conectar em redes wifi públicas, já que seu dispositivos ficará exposto, e por consequência, suas informações mais valiosas e privadas.

Caso seja de extrema importância se conectar a uma rede pública e insegura - como, a de um aeroporto, por exemplo - uma boa escolha seria a utilização de uma VPN, fazendo com que o seu tráfego de rede seja totalmente cifrado, e assim, seguro.

References

[1] http://www.ieee802.org/11/Documents/DocumentArchives/1994_docs/1194249_scan.pdf
[2] A comparative study of WLAN security protocols: WPA, WPA2 https://ieeexplore.ieee.org/document/7506822

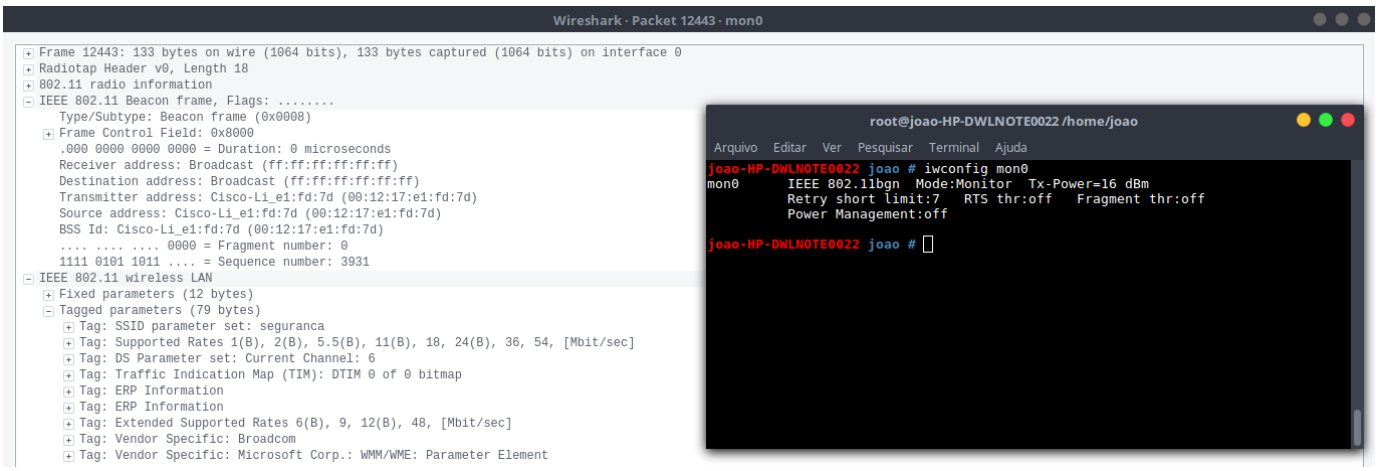

Fig. 5. Exemplo de pacote capturado e modo monitor ativado.