Segurança Informática e nas Organizações

Guiões das Aulas Práticas

João Paulo Barraca[1] e Hélder Gomes[2]

[1]Departamento de Eletrónica, Telecomunicações e Informática
[2]Escola Superior de Tecnologia e Gestão de Águeda
Universidade de Aveiro

2015–2016

Conteúdo

2

Ataques ao WEP: Falsificação da autenticação e descoberta da chave de rede

Resumo:

- Exploração prática das vulnerabilidades do WEP

2.1 Introdução

Com este trabalho pretende-se demonstrar na prática a insegurança total de uma rede protegida com WEP (*Wireless Equivalente Privacy*). Adicionalmente são também demonstradas algumas fragilidades do WPA/WPA2. Para esse fim, deve usar um sistema Linux que possua as ferramentas de ataque necessárias. Na aula haverá uma rede WEP alvo e uma rede WPA2 alvo, cujos identificadores (SSID) serão divulgados na hora. Não use este guião contra outras redes para as quais não tenha autorização.

2.2 Instalação e configuração

Arranque o seu computador da PEN USB fornecida pelo docente. Se porventura tiver um sistema Windows 8 ainda não preparado para arrancar de dispositivos alternativos, terá que alterar as configurações da BIOS.

O sistema operativo fornecido possui a ferramenta `aircrack-ng`, que é fundamental para realizar o ataque ao WEP. O sistema possui ainda a ferramenta `iw` para configuração de vários modos de operação da interface WiFi.

2.3 Ataques ao WEP

2.3.1 Modo monitor

O ataque requer que o atacante trabalhe com a interface WiFi em modo monitor. Neste modo o atacante consegue receber e enviar tramas 802.11 sem estar associado a um AP (*Access Point*). Isto tem de ser feito porque o atacante tem de interferir com a rede (receber e enviar tramas) mas, no início do ataque, não dispõe de credenciais para se associar à rede (falta-lhe conhecer a chave da rede, que no final do ataque irá conseguir obter).

Execute o comando

```
iwconfig
```

e observe as interfaces WiFi existentes, nomeadamente o seu modo (deverá ser `Managed`). Seguidamente execute o comando

```
airmon-ng start wlanX
```

onde `wlanX` deverá ser o nome de uma interface WiFi detetada com o comando anterior ou, caso possua várias, aquela que pretende usar para este trabalho. Execute novamente o comando `iwconfig` e verifique o resultado.

Deverá observar a presença de uma nova interface (`mon0`) e de a mesma estar a operar em `Monitor Mode`. Esta é a interface que deverá ser usada daqui em diante para realizar o ataque.

Nota: Poderão aparecer mensagens referentes a eventuais incompatibilidades com outros programas. Caso um destes programas seja o **Network-Manager** é conveniente desáctivá-lo, o que pode fazer usando o seguinte comando:

```
service network-manager stop
```

2.3.2 Captura de tráfego wireless com Wireshark

O Wireshark pode ser usado para capturar e analisar o tráfego de uma rede sem fios. Para analisar o tráfego de todas as redes, a captura deve incidir sobre a intreface `mon0`. Numa rede sem fios existem três tipos de tramas: de gestão, de controlo e de dados. Através da aplicação de filtros podemos seleccionar o tipo de tramas que se pretende observar.

Inicie uma captura na interface `mon0`. Todas as tramas que são recebidas pela interface são capturadas e apresentadas no ecrã. Assim, se aplicarmos no wireshark o filtro `wlan.fc.type == 0` iremos observar apenas tramas de gestão. Se aplicarmos o filtro `wlan.fc.type == 1` iremos observar apenas tramas de controlo e se aplicarmos o filtro `wlan.fc.type == 2` iremos observar apenas tramas de dados. Aplique os vários filtros e analise as tramas capturadas.

2.3.3 Deteção do AP (ou rede) vítima

O passo seguinte do ataque consiste em identificar as características operacionais da vítima. Esta será em primeira instância um determinado AP, mas o resultado final será o comprometimento da rede a que o AP dá acesso (logo, a vítima última será a rede). Por outras palavras, o AP não sofre qualquer dano durante o ataque, o atacante ficará apenas na posse de elementos que lhe permitem, daí em diante, aceder à rede, quer através do AP atacado, quer através de qualquer outro AP da rede que use a mesma configuração de segurança WEP no acesso à rede.

Execute o comando

```
airodump-ng mon0
```

e procure os AP de serviço a uma rede com um derminado nome (ou ESSID, *Extended Service Set IDentifier*). Neste passo deverá procurar os AP que servem a rede que pretende atacar. Confirme que os mesmos usam WEP

e tome noma do seu endereço MAC (sequência de 6 números hexadecimais separados por ´:´ e do seu canal (número entre 1 e 11 ou 13, tipicamente). Estes dois elementos serão usados mais adiante. Feito isto, aborte o comando em curso.

2.3.4 Análise da capacidade de interação com um AP

Uma vez escolhido o AP vítima, é preciso averiguar se se consegue injetar tramas destinadas ao mesmo. Tal injeção pode ser rejeitada caso o AP concretize políticas de filtragem de endereços MAC.

A injeção de tramas pode ser experimentada com tramas insuspeitas, como é o caso das do tipo *Probe Request*; a resposta às mesmas com tramas *Probe Response* é uma evidência de que não está a ser concretizada qualquer política de filtragem do endereço MAC do atacante, logo o atacante poderá prosseguir com o seu ataque usando o seu endereço MAC.

Antes de testar a injeção de tramas, é necessário fixar no canal do AP vítima a interface `mon0`, que opera em modo monitor varrendo os vários canais. Isto é necessário porque a interface não pode operar simultanamente em todos os canais. Para ficar a interface no canal do AP vítima, execute o seguinte comando:

```
airmon-ng stop mon0
airmon-ng start wlanX channel
```

onde `channel` deverá ser substituído pelo canal usado pelo AP. Seguidamente execute o comando

```
aireplay-ng -9 -e target mon0
```

onde a opção `-9` significa, precisamente, teste de injeção e **target** deve ser substituído pelo SSID do AP vítima. Como resultado deverá receber indicações sobre o sucesso ou insucesso das injeções de tramas que estão a ser testadas.

Exercício adicional: verifique o que acontece quando realiza o teste de injeção sem a interface `mon0` sintonizada no canal do AP vítima.

2.3.5 Captura de tramas

Para descobrir a chave de rede é fundamental capturar tramas cifradas. Para tal é preciso observar tráfego envolvendo um endereço MAC que participe numa associação WEP entre um AP e um terminal. O endereço MAC poderá pertencer a qualquer dos dois (terminal ou AP), uma vez que a mesma chave

de rede é usada nos dois sentidos. No entanto, para facilitar o ataque, vamos usar o endereço MAC do AP, que anotámos anteriormente.

Execute o comando

```
airodump-ng --bssid <mac> -c XX -w captura mon0.
```

Este comando procura por tramas contendo o endereço MAC indicado em `<mac>`, enviadas através do canal `XX` e guarda-as num conjunto de ficheiros cujo nome possui o prefixo `captura`. Daqui em diante este guião considerará apenas este prefixo, mas quem realizar este guião pode usar outros.

Na parte inferior do ecrã produzido pelo comando acima, são identificados (através dos respectivos endereços MAC na coluna STATION) os vários terminais que estão associados a um AP, cujo endereço MAC é identificado na coluna BSSID.

2.3.6 Aceleração do ataque

Caso haja pouca atividade no AP vítima (i.e., pouco tráfego legítimo cifrado) o processo de descoberta da chave de rede pode ser muito demorado, porque é preciso capturar um determinado número de tramas cifradas com recurso a alguns valores de IV (*Initialization Vector*) especiais.

No entanto, este problema pode ser contornado através da injeção de pacotes (cifrados) capturados que irão provocar respostas legítima igualmente cifradas. Desta forma podemos acelerar a geração de tráfego cifrado genuíno, o qual poderá então ser útil para ajudar ao ataque em curso.

Para que se possa provocar a aceleração da captura é necessário que exista algum terminal associado com o AP. A partir das tramas trocadas entre um desses terminais e o AP pode ser extraída a chave contínua usada e depois reutilizá-la na produção das tramas forjadas, que terão como origem esse terminal associado, para que estas sejam aceites pelo AP. Assim, caso exista algum terminal associado com o AP, abra um novo terminal e use o seguinte comando para fazer a aceleração do ataque,

```
aireplay-ng -3 -b <macAP> -h <macTerminal> mon0
```

em que <**macAP**> é o endereço MAC do AP vítima e <**macTerminal**> é o endereço MAC de um terminal que esteja presentemente associado ao AP vítima.

Este comando esperará por um pedido ARP e depois injectá-lo-á repetida e continuamente. Por causa disto, deverá constatar um aumento significativo do número de tramas de dados (não *Beacons*) capturadas pelo `airodump-ng` no outro terminal. Tal significa mais dados cifrados capturados, logo mais valores de IV usados, logo mais possibilidades de descobrir a chave de rede.

Caso não exista nenhum terminal associado ao AP vítima, é possível usar uma chave contínua previamente capturada para que o atacante se possa associar, mas tal não é coberto neste guião.

2.3.7 Descoberta da chave de rede

Neste momento temos tudo configurado para começar a descobrir a chave de rede a partir de algumas das tramas cifradas capturadas. Numa outra consola (terceira) execute o comando

```
aircrack-ng captura*.cap
```

onde `captura` é o prefixo dos ficheiros onde estão a ser guardadas as tramas cifradas capturadas. Este comando irá processar as tramas cifradas capturadas e descobrir a chave de rede. A segurança da rede foi quebrada; a rede ficou acessível ao atacante.

Após esse facto, pode experimentar entrar na rede atacada usando a sua interface de rede da forma convencional e essa mesma chave.

2.4 Ataque ao WPA2

Como vimos atrás, uma redes sem fios WEP não tem segurança nenhuma, uma vez que facilmente se obtem a chave partilhada. Para substituir o WEP surgiram primeiro o WPA e depois o WPA2. Apesar das difemrenças entre eles, ambos permitem autenticação baseada em EAP (usando um servidor Radius) ou autenticação baseada em chave pré-partilhada (PSK - *Pre-Shared Key*). Esta última (WPA/WPA2 PSK) é vulnerável a ataques com dicionário para a descoberta da chave partilhada.

Para realizar este ataque é necessária a captura dos pacotes trocados durante a autenticação entre o cliente e o AP, o designado *four-way handshake*, e um ficheiro com um conjunto de chaves comuns, o dicionário. Para realizar a captura do *four-way handshake*, siga os três primeiros passos realizados para o WEP, i.e., a "Detecção do AP vítima", a "Análise da capacidade de interação com um AP"e a "Captura de tramas", tendo em conta que a vítima agora é um AP com WPA2 PSK.

Quando ocorre uma captura dos pacotes de autenticação, o airodump-ng sinaliza-o com uma mensagem no campo superior direito, semelhante à seguinte: `WPA handshake: 00:14:6C:7E:40:80`. Depois de capturados esses pacotes, podemos terminar a captura.

Caso não pretenda esperar por uma atenticação, o que pode demorar, é possível forçar o desassociar de clientes associados ao AP, o que faz com que

estes se reautentiquem, o que nos permite realizar a captura de imediato. Para desassociar um cliente use o seguinte comando.

```
aireplay-ng -0 1 -a <macAP> -c  <macClient> mon0
```

em que **macAP** é o endereço MAC do AP vítima e **macClient** é o endereço MAC do terminal que se pretende desautenticar. Note que a desautenticação é enviada diretamente pelo seu terminal para o terminal a desassociar, pelo que estes devem estar ao alcance um do outro.

Para realizar o ataque à chave é necessário um ficheiro com o dicionário de chaves. Pode descarregar um da página da disciplina no elearning. A chave apenas será descoberta se for uma das contidas no ficheiro. Para realizar o ataque use o seguinte comando:

```
aircrack-ng -w chaves.lst -b <macAP> captura*.cap
```

Caso a chave partilhada conste na lista de chaves ela será apresentada.

O sucesso deste tipo de ataque depende da qualidade da chave partilhada e da lista de chaves. A chave foi obtida porque consta na lista de chaves. Este ataque não resulta se a chave partilhada for uma chave forte, que não conste em nenhuma lista de chaves. A qualidade da lista de chaves também influi, porque quanto mais chaves lá estiverem, maior a probabilidade de sucesso. No entanto, quanto maior o ficheiro de chaves, mais pesado e demorado é o ataque. Pesquise formas mais eficientes de atacar a chave partilhada de uma rede WPA/WPA2.

2.5 Bibliografia

`http://www.aircrack-ng.org`