ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Chave:

2444666668888888

Segurança WiFi

ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

Porquê abordar o wireless?

- Ponto de entrada na rede que ultrapassa as fronteiras físicas
  - Mas o atacante precisa de ser local
- Serviço quase obrigatório
  - A ser disponibilizado aos utilizadores
- Os utilizadores cada vez mais trazem os seus dispositivos para aceder à rede
- A segurança em Wireless precisa de também ser endereçada

Formas de autenticação/cifra

- WEP
  - Descontinuada
- WPA/WPA2
  - Mais atualizada
- WPS
  - Criada para facilitar a vida aos utilizadores residenciais
  - Vulnerabilidades recentes em múltiplos fabricantes
    - Ataque pixie-dust

WEP

- Forma original de segurança, com as vertentes de autenticação e cifra de dados
- Baseada no algoritmo RC4
- Chave de 40bit concatenados com 24bit de Initialization Vector (IV)
- Evoluiu para 104bit fornecidos pelo utilizador mais os 24bit de IV
- Introduzidas nos dispositivos como sequencias de 10 ou 26 caracteres hexadecimal
- Outras variantes não normalizadas usando 152bit e 256bit (chave+IV)

WEP – Autenticação

- *Open*
  - Sem qualquer validação
  - Todos os equipamentos se podem ligar à rede
  - Por vezes validada com listas de acesso dos endereços MAC permitidos
- *Shared Key*
  - Cliente pede ao AP para se autenticar
  - AP responde com um "desafio" (valor aleatório em claro)
  - Cliente responde com o "desafio" cifrado com a chave configurada para o WEP
  - AP decifra a mensagem e se conferir com a original aceita o cliente
- *Open* é a forma mais segura!!!
- *Shared* permite deduzir facilmente a chave através de iterações ao AP

WEP – Cifra de dados

- A chave não deve ser repetida
  - Para evitar que duas tramas iguais produzam o mesmo conteúdo cifrado
- No envio de cada trama cifrada
  - É gerado um valor para o IV (de forma aleatória ou outra)
  - Chave do utilizador+IV são usados como chave da cifra
  - No cabeçalho da trama cifrada o IV é incluído em claro
- Problemas
  - Com somente 24bit o IV repete-se ao longo de grandes transferências de dados
  - Investigadores identificaram inseguranças no RC4
  - Possibilidade de replay de tramas facilita geração de múltiplas tramas com o mesmo conteúdo mas cifradas com IVs distintos
    - Do processamento matemático/estatístico é possível derivar os 40/104 bit de chave!!!

WPA/WPA2 (802.11i)

- WPA/TKIP deve ser usado somente quando estritamente necessário
  - Reutiliza o algoritmo de cifra RC4 em dispositivos que o hardware não suporte cifra AES
  - Chaves distintas de 128bit são usadas para cada trama e não somente o IV
- Incluem proteções para evitar a retransmissão (replay) de mensagens
- WPA2 usa cifra CCMP, uma cifra robusta baseada em AES

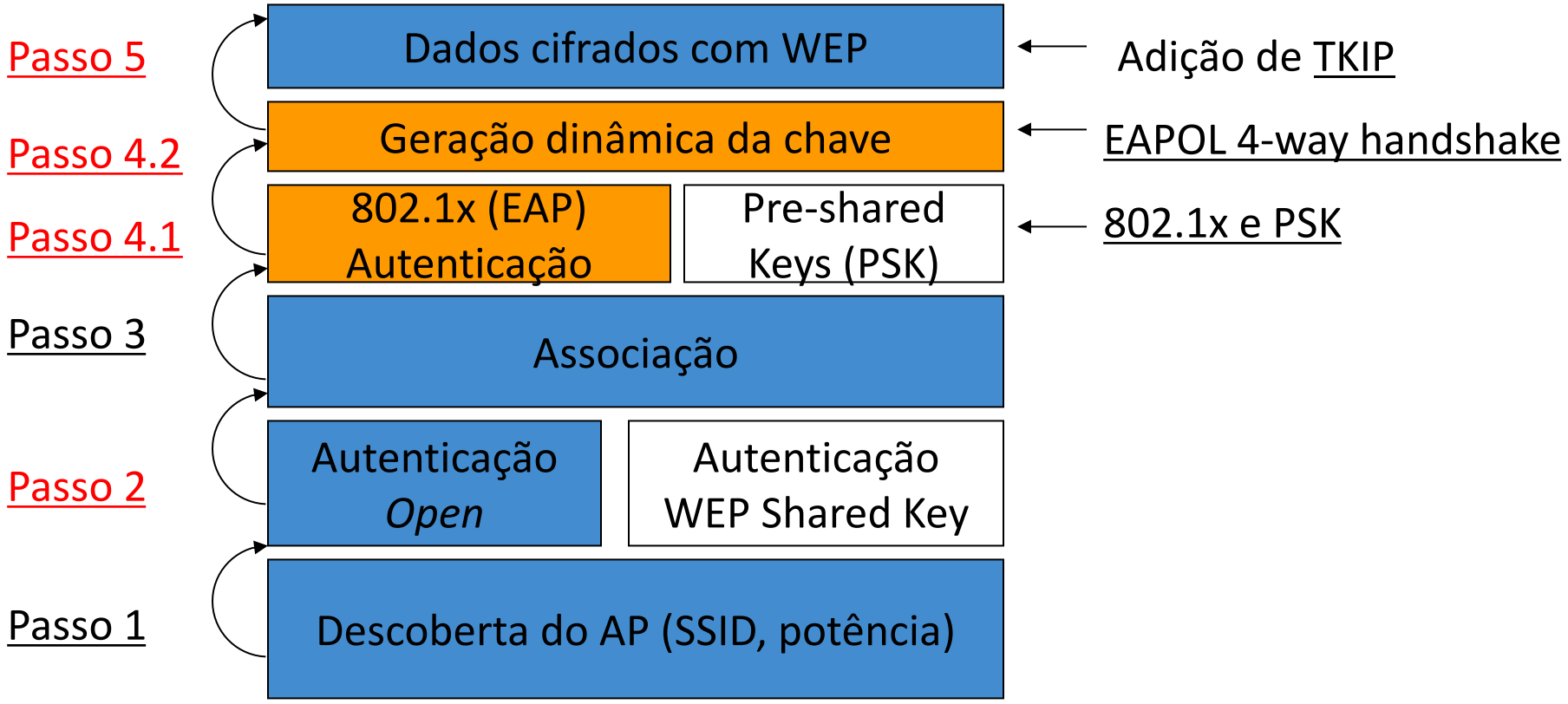
WPA/WPA2 (802.11i) - Distribuição de chaves

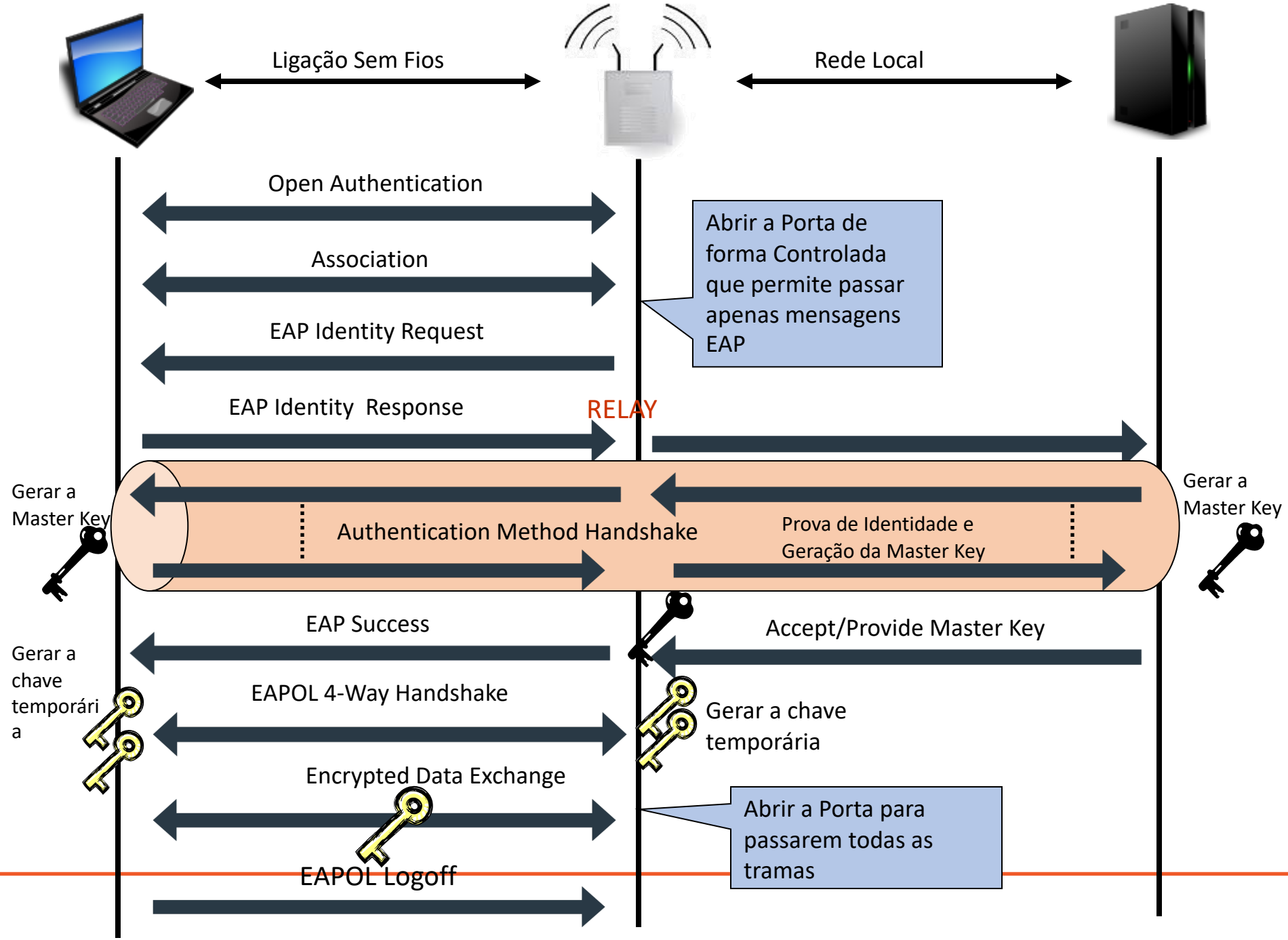
- WPA-Personal
  - Também conhecido por WPA-PSK (Pre-shared key)
  - Cifra com chaves de 256bit
    - 64 caracteres hexadecimal
    - Derivada de uma frase-chave de 8 a 63 caracteres ASCII (imprimíveis)
      - Chave derivada usando a função PBKDF2
      - Usando SSID como salt e 4094 iterações de HMAC-SHA1
  - Disponível no WPA e WPA2
- WPA-Enterprise
  - Também conhecido como WPA-802.1X
  - Chaves são geradas dinamicamente, por acesso
  - Necessita do suporte de um servidor RADIUS para validação de acessos e geração de chaves
  - Várias formas de EAP podem ser usadas na autenticação e distribuição de chaves
    - Formas mais seguras apoiam-se em TLS/SSL e PKI (certificados digitais)
  - Usada na e-U/eduroam

WPA/WPA2 (802.11i) - Distribuição de chaves

- WiFi Protected Setup (WPS)
  - Forma facilitadora da configuração de equipamentos em ambientes PSK
  - Uso de PINs numéricos de 4 ou 8 dígitos
  - Utilizador prime um botão no AP e durante alguns segundos ele permite que qualquer cliente obtenha a frase-senha
  - Maioria dos AP domésticos possui WPS ligado e com uma chave por omissão
  - Com no máximo 10^8 tentativas obtém-se a palavra-passe!

Estabelecimento da ligação com WPA




Ligação Sem Fios
Rede Local
Open Authentication
Association
EAP Identity Request
Abrir a Porta de forma Controlada que permite passar apenas mensagens EAP
EAP Identity Response
RELAY
Gerar a Master Key
Authentication Method Handshake
Prova de Identidade e Geração da Master Key
Gerar a Master Key
EAP Success
Accept/Provide Master Key
Gerar a chave temporária
EAPOL 4-Way Handshake
Gerar a chave temporária
Encrypted Data Exchange
Abrir a Porta para passarem todas as tramas
EAPOL Logoff

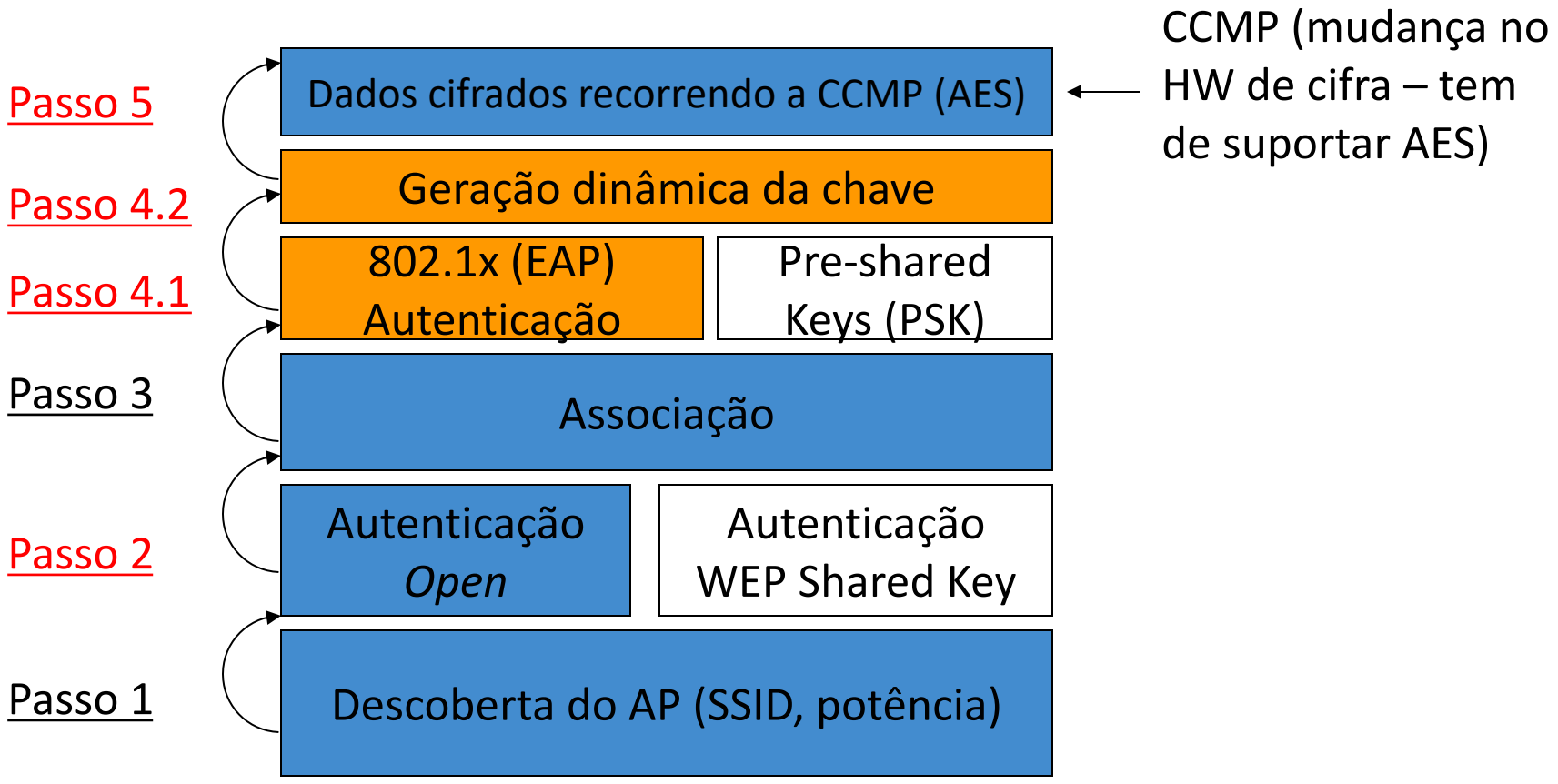
Vantagens do 802.1x

- Liberdade de escolha do algoritmo de autenticação
  - O 802.1x é apenas um protocolo de transporte
  - TLS, TTLS, LEAP, PEAP, GTC, MSCHAPv2, Kerberos, SIM, e algoritmos futuros podem ser transportados sobre 802.1x, sendo os únicos requisitos
    - Suporte de autenticação mútua
    - Suporte de derivação de *master keys*
  - As chaves e os algoritmos de autenticação pode ser específicos a cada sessão
- Facilidade de gestão de credenciais num servidor central de autenticação
- Facilidade de integração com sistemas de segurança empresariais (autenticação da rede)

TKIP

- O TKIP usa IVs maiores (48 bits) – o dobro do WEP
- Evita IVs fracos
- Previne a reutilização de IVs para uma chave
  - O IV começa sempre em 0 e é incrementado
- A geração da *master key* é feita para cada tentativa de ligação – ao contrário das chaves WEP estáticas
  - As chaves temporárias são geradas a partir da *master key* e são utilizadas para cifra – renovadas em intervalos regulares

Estabelecimento de uma ligação baseada no 802.11i – WPA2



Considerações erradas sobre o WiFi

- “Escondemos o SSID e assim não encontram a nossa rede”
- “Usamos controlos de acesso baseados em endereços MAC e permite-nos autorizar dispositivo a dispositivo”
- “Os ataques a redes WiFi necessitam de hardware caro e que não está facilmente disponível”
- ”Segregamos todo o tráfego da rede WiFi e por isso estamos seguros”

Riscos de uma rede WiFi

- Eavesdropping (escuta)
- Masquerading (disfarce)
- Denial of Service (negação de serviço)
- Rogue Access Points (pontos de acesso maliciosos)

WEP – O ataque do aircrack-ng - Captura

- Colocar a placa de rede sem fios em modo "monitor"
  - airmon-ng start <wlanX>
  - Acesso ao tráfego ao nível MAC
  - Injeção de tramas
- Identificar a rede alvo e as características base da mesma
  - airodump-ng <monIf>
  - SSID, BSSID (MACAP) e canal
- Confirmar que a placa de rede sem fios em uso permite a injeção de tramas
  - aireplay-ng -9 –e <SSID> -a <MACAP> <monif>
  - Teste deve concluir indicando 100% ou próximo para que se possa prosseguir
- Iniciar a captura de IVs
  - airodump-ng –c <canal> --bssid <MACAP> -w <ficheiro> <monif>

WEP – O ataque do aircrack-ng – Gerar IVs

- Sem parar a captura de IVs!
- Simular a autenticação no AP (para ele aceitar o trafego que iremos gerar)
  - aireplay-ng -1 0 -e <SSID> -a <MACAP> <monIf>
  - Se o anterior não funcionar testar com:
    - aireplay-ng -1 6000 -o 1 -q 10 -e <SSID> -a <MACAP> <monIf>
- Iniciar o ARP replay
  - aireplay-ng -3 –b <MACAP> <monIf>
  - Aplicação aguarda a receção de uma trama que deduza ser um ARP request
    - Pela dimensão da trama
    - Por ser destinada a broadcast
  - AP irá aceitar a retransmissão da trama que enviou por usar uma chave válida
  - Sendo um broadcast irá reenviar a trama mas usando um IV distinto na nova cifra

WEP – O ataque do aircrack-ng – Chave!

- Periodicamente verificar se já foram recolhidos IVs suficientes para deduzir a chave
  - aircrack-ng -b <MACAP> <ficheiro*.cap>
  - Para o algoritmo alternativo de pesquisa (FSM/Korek) correr o comando com o parâmetro adicional –K
- Como funciona
  - O aircrack-ng sabe acerca da trama
    - Conteúdo da quase totalidade dos bytes da mensagem original
      - Muitos são fixos, outros facilmente inferidos
    - Conteúdo da trama cifrada sempre com a mesma chave de utilizador mas com os diferentes IV, incluídos na trama
    - Usando as fragilidades identificadas no RC4, deduzidos os bit da chave do utilizador
- Recomendação: Não usar

WPA/WPA2-Personal – Ataque aircrack-ng (1)

- Colocar a placa de rede sem fios em modo "monitor"
  - airmon-ng start <wlanX>
  - Acesso ao tráfego ao nível MAC
  - Injeção de tramas
- Identificar a rede alvo e as características base da mesma
  - airodump-ng <monIf>
  - SSID, BSSID (MACAP) e canal
- Iniciar a captura de tráfego (handshakes)
  - airodump-ng –c <canal> --bssid <MACAP> -w <ficheiro> <monif>

WPA/WPA2-Personal – Ataque aircrack-ng (2)

- Sem parar a captura
- Ir verificando se já foi registado algum handshake (troca de dados que ocorre no momento da autenticação de um cliente na rede)
  - aircrack-ng -w <ficheiro com dicionário> -b <MACAP> <ficheiro*.cap>

- Provocar o "handshake" (se necessário)
  - Validar primeiro se a placa suporta injeção de tramas (ver slides sobre o ataque ao WEP)
  - Forjar uma mensagem do AP desautenticando um cliente ativo
    - Usando informações sobre os clientes ativos no AP, listados no airodump-ng
    - aireplay-ng -0 1 -a <MACAP> -c <MACCLIENTE> <monIf>

WPA/WPA2-Personal – Ataque aircrack-ng (3)

- Como funciona
  - Quando um cliente entra numa rede WPA/WPA2-PSK são trocadas mensagens em que este prova saber a frase-chave e é derivada a chave a usar na cifra
  - airodump-ng irá capturar esta troca de mensagens
  - Com recurso a um dicionário (ficheiro com uma palavra por linha)
    - Nos sistemas Linux costumam estar em /usr/share/dict/ ,podem ser instalados dicionários adicionais
  - Sabendo que o algoritmo PBKDF2, tal como usado tem um universo reduzido de bits à entrada e salt (caracteres imprimíveis)
  - São testadas cada uma das palavras do dicionário procurando uma que corresponda ao handshake registado
- Recomendação: Usar uma frase-chave longa inexistente em dicionário ou 64 caracteres hexadecimal aleatórios (ex: openssl rand -hex 64)

WPA/WPA2 com WPS – Ataque reaver

- Fases iniciais semelhantes às dos ataques anteriores
  - Colocar a placa de rede em modo monitor
  - Confirmar o suporte de injeção de tramas da placa/driver
  - Identificar os parâmetros da rede a atacar

- Ataque em modo pixie-dust (mais eficiente)
  - Falha frequentemente devido a limitações do hardware
  - reaver -i <monIf> -b <MACAP> -vvv -K 1
- Ataque WPS base
  - reaver -i <monIf> -b <MACAP> -vvv
- Recomendação: Desactivar o WPS no equipamento (AP)