Segurança em redes Wi-FI

Wardriving

- Termo escolhido para batizar a atividade de dirigir um automóvel à procura de redes sem fio abertas, passíveis de invasão.
- Para efetuar a prática do wardriving, são necessários um automóvel, um computador, uma placa Ethernet configurada no modo "promíscuo" (o dispositivo efetua a interceptação e leitura dos pacotes de comunicação de maneira completa), e um tipo de antena, que pode ser posicionada dentro ou fora do veículo.

Wardriving

- Tal atividade não é danosa em si, pois alguns se contentam em encontrar a rede wireless desprotegida, enquanto outros efetuam login e uso destas redes, o que já ultrapassa o escopo da atividade

Warchalking

- É a prática de escrever símbolos indicando a existência de redes wireless e informando sobre suas configurações. As marcas usualmente feitas em giz em calçadas indicam a posição de redes sem fio, facilitando a localização para uso de conexões alheias pelos simpatizantes da idéia.

Warchalking

Formas de Segurança

- O padrão IEEE 802.11 fornece o serviço de segurança dos dados através de dois métodos: autenticação e criptografia.
- Este padrão 802.11 define duas formas de autenticação: **aberta** e **chave compartilhada**.
- Independente da forma escolhida, qualquer autenticação deve ser realizada entre pares de estações. Em sistemas BSS as estações devem se autenticar e realizar a troca de informações através do Access Point (AP).

Formas de segurança

- As formas de autenticação previstas definem:

- **Autenticação aberta** - é o sistema de autenticação padrão. Neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo.

- **Autenticação chave compartilhada** – neste sistema de autenticação, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo

Autenticação aberta

- A autenticação Aberta foi desenvolvida focando redes que não precisam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção.

Autenticação chave compartilhada

- A autenticação Chave Compartilhada utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos. Um segredo é utilizado como semente para o algoritmo de criptografia do WEP na cifragem dos quadros. A forma de obter esta autenticação é a seguinte:

  1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
  2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudorandômicas.
  3.A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
  4.O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

A natureza dos problemas

- O sinal pode se propagar além dos limites físicos desejáveis
  - acessível a qualquer um que esteja dentro da cobertura do sinal
  - riscos:
    - captura de dados privativos
    - roubo de largura de banda da conexão com a Internet
- Não se pode confiar na técnica de modulação e transmissão por espalhamento de sinal
  - qualquer receptor padrão é capaz de decodificar

Principais ameaças

- Negação de Serviço (DoS)
  - inundar os APs com pedidos de associação e autenticação
- Jamming
  - inundar a faixa de RF com interferência (DoS no nível físico)
- Ataques de Inserção
  - conectar estações não-autorizadas a um AP
- Ataque de Replay
  - interceptar tráfego de autorização (como chaves ou senhas) e depois usá-lo para ganhar acesso não autorizado
- Monitoramento de Broadcast

Principais ameaças

- ARP Spoofing
  - corromper as tabelas ARP para que tráfego seja direcionado para a estação intrusa
- Seqüestro de Sessão (man-in-the-middle)
  - faz-se passar por uma estação sem fio e requisita sua desassociação do AP
  - faz-se passar pelo AP e reassocia a mesma estação consigo
- Rogue Access Point (ataque do gêmeo mau)
  - instala um AP não-autorizado com o mesmo SSID
  - aumenta a potência do sinal desse AP para fazer com que os clientes se associem com ele
- Ataque Criptoanalítico

Principais ameaças

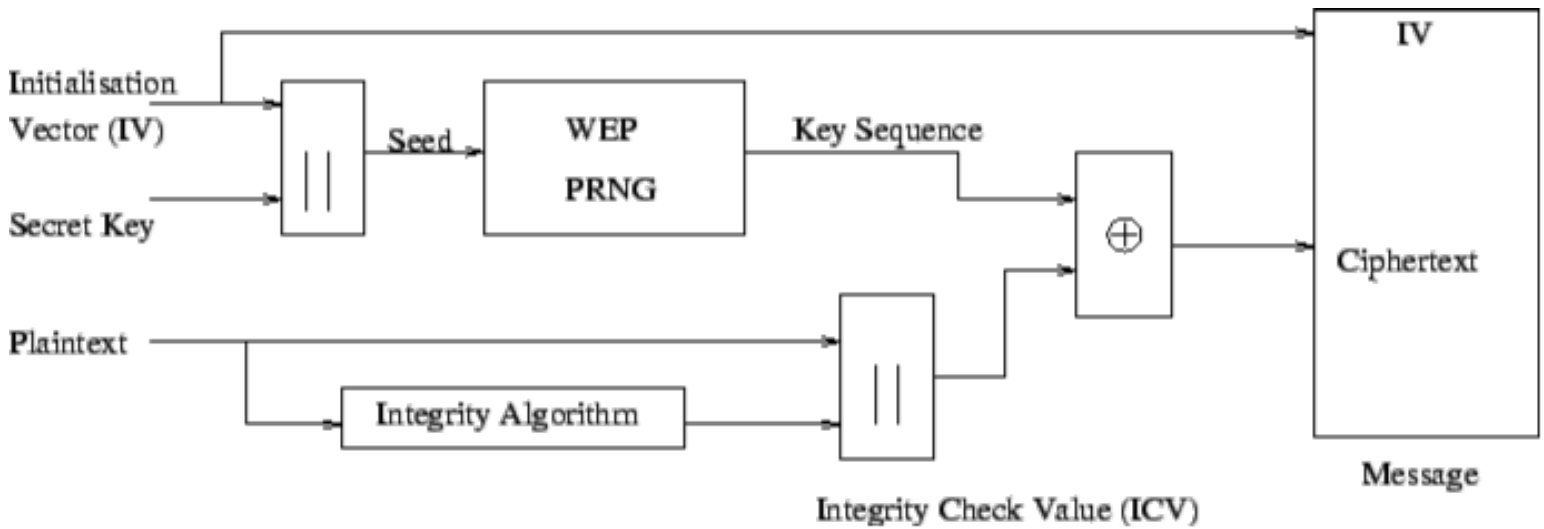
- Ataques no Canal
  - uso de informações do nível físico
    - consumo de energia, temporizações, emissões eletromagnéticas
  - para obter informações sobre o sistema criptográfico
  - permite obter a chave de criptografia diretamente ou uma mensagem em plain text a partir da qual a chave pode ser computada

WEP

- Uso de chave secreta
  - configurada no AP
  - distribuída (por meios externos, na maioria das vezes, manual) para estações autorizadas
  - usada par encriptar os dados
- Chaves secretas de 40 ou 104 bits
  - combinada com vetor de inicialização de 24 bits para gerar chaves de criptografia de 64 e 128 bits
  - independente do tamanho da chave, pode-se derivar a chave a partir da análise de cerca de 4 milhões de quadros!
- Encriptação

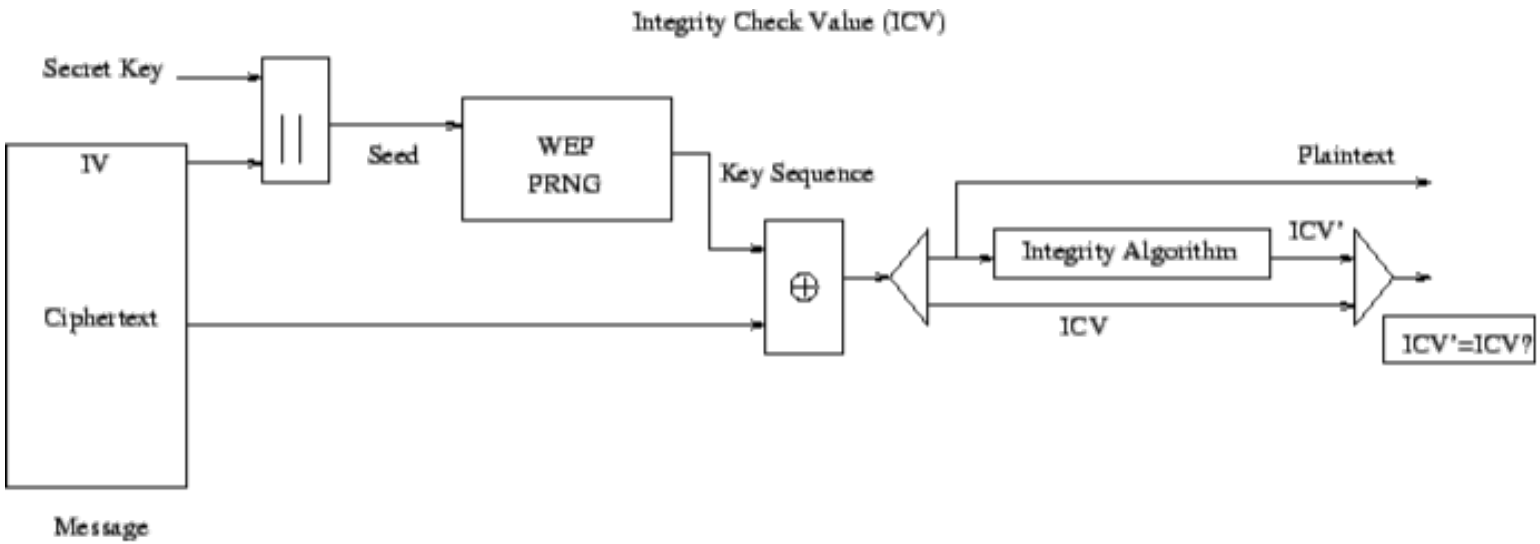
WEP

- Encriptação



WEP

- Decriptação



WEP

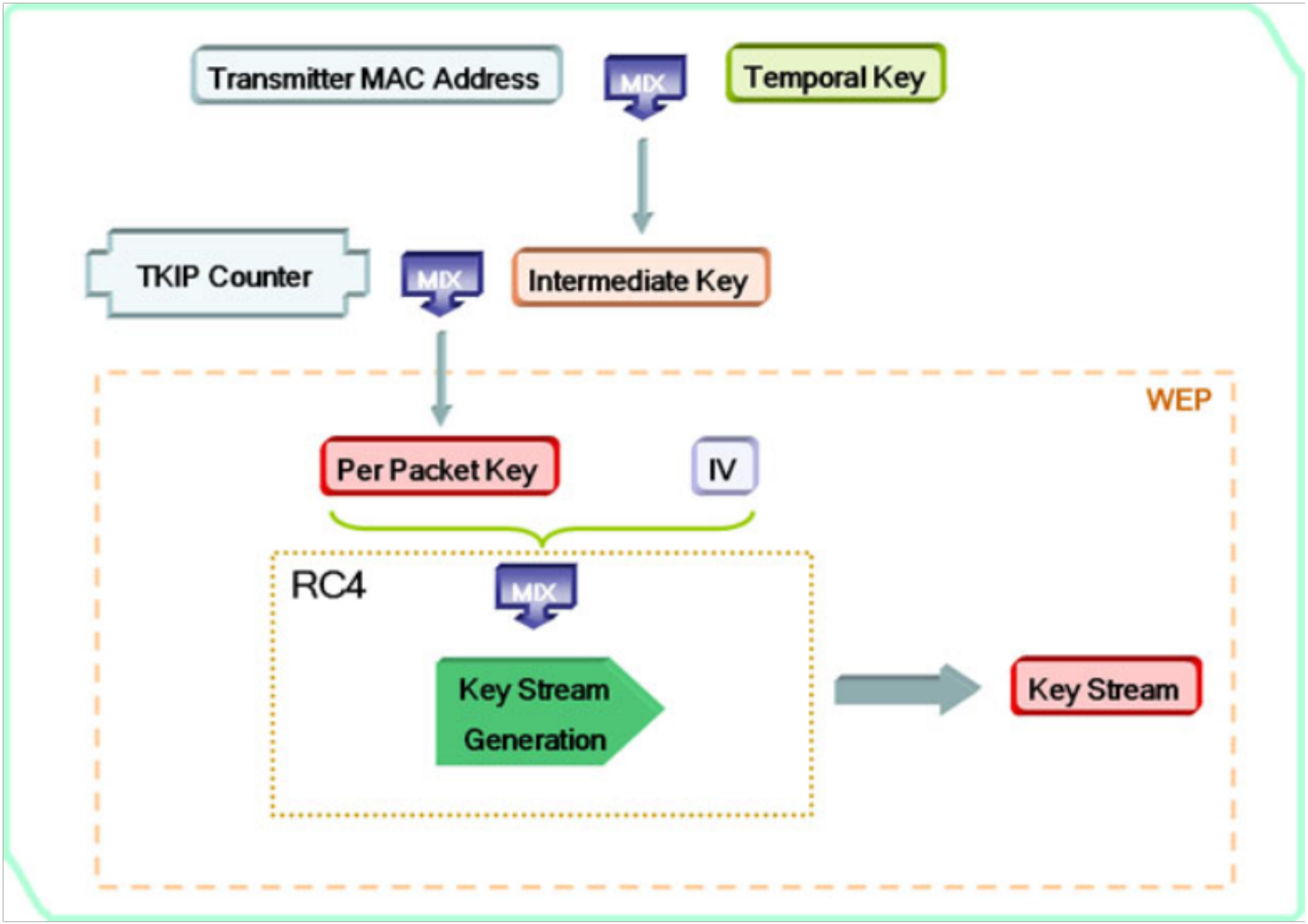
- Crítica
  - IV (vetor de inicialização) muito curto: 24 bits, independentemente do tamanho da chave: repetido com freqüência e incluso no ciphertext
    - pode ser utilizado para extrair a chave de criptografia após um número “não muito grande” de tentativas
  - Não há um mecanismo para troca dinâmica da chave
    - a mesma chave permanece em uso por tempo suficiente para dar a oportunidade de quebrá-la (o que não demora mais do que alguns minutos!)

- Solução intermediária
  - Reforçar o uso de WEP
    - algum mecanismo para troca (distribuição) de chaves com freqüência (em 802.1X)
  - Utilizar filtragem de endereços MAC

WPA

- Procura eliminar a vulnerabilidade de WEP
  - Chaves dinâmicas (de 128 bits)
    - Protocolo para criação e distribuição de chaves: TKIP
    - Chave
      - criada para cada sessão (estação-AP)
      - pelo protocolo de autenticação ou manualmente
  - Vetor de inicialização maior (48 bits)
  - Função de checagem da integridade das mensagens
  - Pode ser considerado um WEP dinâmico (usa RC4)
- TKIP (Temporal Key Integrity Protocol)
  - cálculo da chave:
    - chave temporal + end. MAC + contador TKIP + IV de 48 bits
  - distribui chaves periodicamente
    - intervalos de 1 a 10.000 pacotes
  - MIC (message integrity code)
    - código de verificação de erros: detectar msgs forjadas

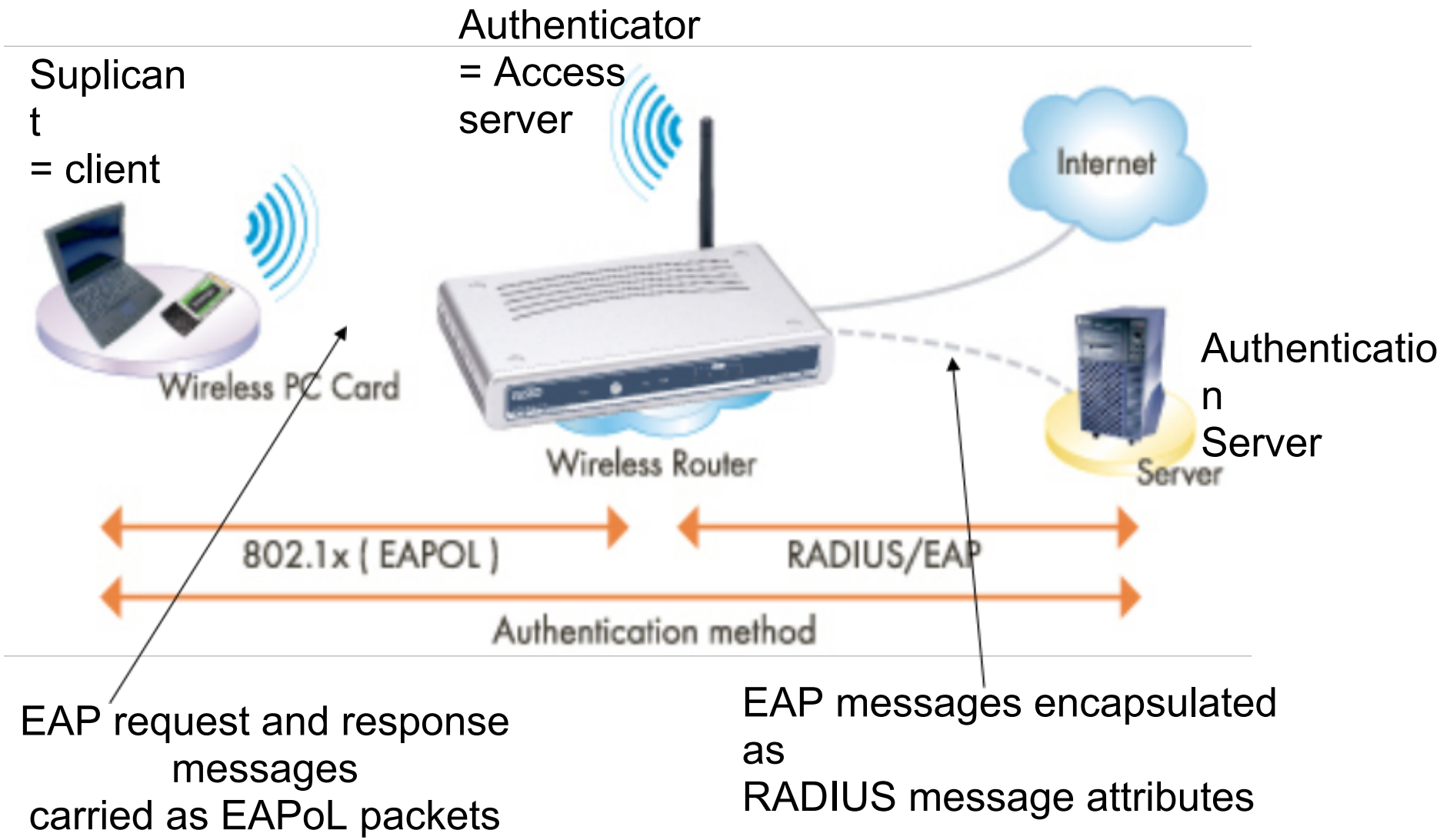
WPA = TKIP + WEP


Transmitter MAC Address
MIX
Temporal Key
TKIP Counter
MIX
Intermediate Key
WEP
Per Packet Key
IV
RC4
MIX
Key Stream Generation
Key Stream

WPA

- Medidas de segurança adicionais
  - Se uma violação é detectada através do cálculo do MIC
    - o que pode significar que uma chave foi quebrada
  - Todas as chaves são resetadas
  - Aumenta-se a taxa de atualização de chaves
  - Envia alerta para o administrador da rede
  - Opcional:
    - desautentica todas as estações
    - shutdown do BSS por 1 minuto caso o AP receba uma sucessão de pacotes forjados
- Autenticação
  - Primeiro passo na associação: não associa se não autenticar
  - 802.1X
  - Configuração mais comum: servidor de autenticação

Autenticação com RADIUS



802.1X

- EAP (Extensible Authentication Protocol)
  - usado na camada de enlace para passar informação de autenticação entre o suplicante e o servidor de autenticação
  - tanto para redes cabeadas quanto para redes sem fio
  - em redes sem fio, o AP funciona como um autenticador, mas desempenha esta função fazendo uso do servidor de autenticação propriamente dito
    - um intermediário entre o suplicante e o servidor de autenticação
  - Vários tipos de EAP são permitidos
    - EAP-TLS: utiliza certificados de cliente e servidor
    - EAP-TTLS e PEAP: apenas certificado do servidor – dados de autenticação do cliente (ex.: usuário e senha) são passados para o servidor encriptados com sua chave pública
  - Requer uma PKI (Public Key Infrastructure) para validar os certificados

802.11i e WPA2

- 802.11i
  - criptografia mais forte (AES)
  - autenticação
  - gerenciamento de chaves
  - conceito de RSNs (*Robust Security Network*)
    - negociação do protocolo de confidencialidade durante associação do dispositivo
    - sistema de chaves: chaves unicast e chaves de grupo
    - TKIP e AES
  - cache de chaves e pré-autenticação: *roaming* mais rápido
- WPA2
  - implementação do padrão 802.11i pela Wi-Fi Alliance

WPA e WPA2: Modos de autenticação

- Enterprise Mode
  - autenticação automática via 802.1X / EAP

- Personal Mode
  - PSK – Private Shared Key
    - configuração manual de chaves
    - cliente autentica se possuir a chave correta
  - apenas viável em redes de pequeno porte (SOHO)

- Discutir a aplicabilidade de cada um

WPA

- A despeito do WPA ter características de segurança superiores ás do WEP, ainda assim apresenta algumas vulnerabilidades já reportadas e que devem ser conhecidas para que o seu impacto possa ser minimizado.

WPA – Uso de senha pequenas ou fáceis

- Apesar de não ser específicas do protocolo, este também está sujeito a ataques de força bruta ou dicionário de palavras, onde o atacante testa senha em sequência e/ou palavras comuns.

WPA – Uso de senha pequenas ou fáceis

- Senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque. É muito comum fabricantes usarem senhas pequenas (de 8 a 10 dígitos) imaginando que o administrador irá trocá-las quando o equipamento entrar em produção.

Crackers de WPA

- Linux
  - WPACrack
    - De posse de um tráfego capturado, permite ataques combinados usando um dicionário e técnicas de força bruta.

Medidas Gerais de Segurança I

- Política de segurança
  - requisitos de controle de acesso, uso de senhas, encriptação, controle da instalação de equipamentos etc
- Avaliação dos riscos
  - qual o valor dos dados/acesso e as potenciais conseqüências de acesso não-autorizado?
- Inventariar todos os APs e dispositivos sem fio
  - por varredura do espaço de RF e análise de logs
- Colocação dos APs no interior do prédio
  - reduzir “vazamento” de RF para fora
- Colocar os APs em locais seguros
  - e desabilitar gerenciamento a partir da própria rede sem fio

Medidas Gerais de Segurança II

- Trocar o SSID default e desabilitar SSID broadcast
- Desabilitar protocolos de gerenciamento não essenciais nos APs
- Troca periódica de chaves compartilhadas
- Listas de controle de acesso de endereços MAC
- Na administração dos APs
  - habilitar autenticação de usuário e usar senhas fortes
- Implantar Autenticação de usuários
- Detecção de Intrusão
- Manter o firmware atualizado (APs e NICs)
- Manter e examinar os logs com freqüência
- Quando dispositivos são descartados
  - resetar (zerar) a configuração