NextiraOne Portugal

Segurança em Rede Wireless

Novembro 2005

nextiraOne
A PLATINUM EQUITY COMPANY

Porquê o Wireless ?

- Quais os motivos para rápida vulgarização das REDES WIRELESS ?
  - Não necessita de infra-estrutura de cabos
    - Baixo custo
    - Rápida implementação
    - Necessidades específicas (Museus, Igrejas, etc)
  - Maior Mobilidade

Standards

	802.11a	802.11b	802.11g
Frequência	5Ghz	2,4Ghz	2,4Ghz
Distribuição Geográfica	EUA	Mundo	Mundo
Modulação	OFDM	DSSS	OFDM
Largura de Banda	54Mbps	11Mbps	54Mbps
Data rates	54M;48M;36M;24M; 18M;12M;9M;6M;	11M; 5,5M; 2M; 1M	54M;48M;36M;24M; 18M;12M;9M;6M;

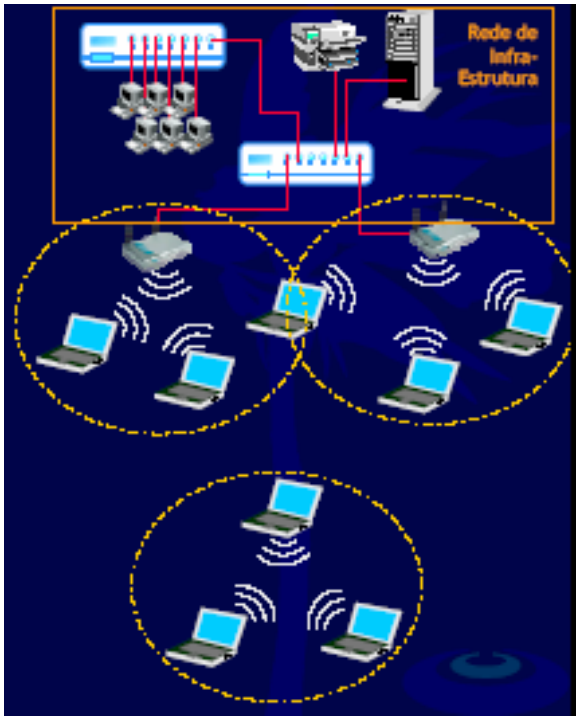
OFDM - Orthogonal Frequency-division Multiplexing
DSSS - Direct Sequence Spread Spectrum

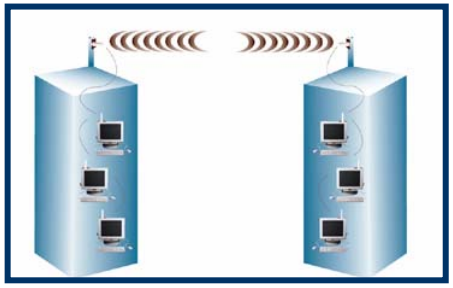
Distâncias

- Em ambientes indoor:
  - Tipicamente 50 metros
- Outdoor :
  - Tipicamente 400 metros
- Configurações especiais para Outdoor:
  - Recorrendo a amplificadores e antenas apropriadas, podemos alcançar alguns Kilometros
  - Tipicamente em ligações ponto a ponto, com antenas direccionais atinge-se distâncias até 7 KM, indo a 20KM em casos especiais.

Topologias Tipo

- Modo Ad-hoc
  - Não necessita de infra-estrutura
  - Utiliza apenas placa de wi-fi para interligações (peer-to-peer)
- Modo Infra-estrutura
  - Necessita de Access Point (AP) para interligar a LAN com os PC's
  - Tirando partido das facilidades existentes na LAN
- Modo Bridge (ponto a ponto)
  - Utilizado para a ligação de edifícios





Mecanismos de Segurança no wireless

- Sem Encriptação
  - Apenas mecanismos de Autenticação e Controlo de Acesso
    - Autenticação baseada no SSID
    - Inibição de Broadcast de SSID
    - ACL's Baseadas no Mac Address
- Com Encriptação
  - Utilizando WEP

Mecanismos de Segurança no wireless

Problemas Autenticação e Controlo de Acesso :

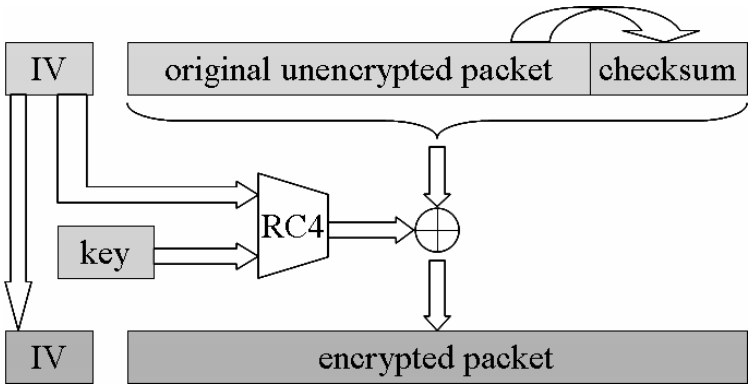
- Autenticação baseada no SSID
  - O SSID não é encriptado e é transmitido pelo ar
- Inibição de Broadcast de SSID
  - Não Resulta as frames de autenticação do cliente revelam o SSID
- ACL’s Baseadas no Mac Address
  - Os MAC address são facilmente forjados

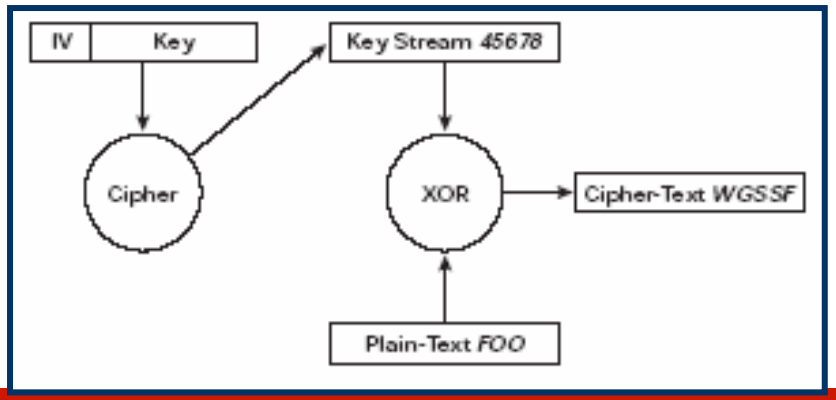
Solução:

- Utilizar WEP

WEP – Wired Equivalent Privacy

- Foi criado com o objectivo de garantir:
  - Confidencialidade
  - Integridade
  - Autenticidade
- É baseado no algoritmo RC4
- O tamanho das chaves pode ser de 64 bits (40 +24 IV) ou 128 (104 + 24 IV)
- O Initialization Vector (IV) é utilizado durante a encriptação para evitar a repetição da chave (IV 24 Bits - 16777216)





Demo

Live WEP Crack Tutorial

Problemas WEP / Wireless

- Autenticação
  - Autenticação num só sentido (Apenas o AP valida o utilizador)
    - Possibilita ataques de MIM
  - A chave é partilhada entre o AP e todos os clientes
    - Basta comprometer uma ligação para termos acesso a tudo
  - Distribuição manual das chaves
    - Mudar as chave é uma tarefa difícil, regularmente quase impossível.
- Integridade
  - Apenas um mecanismo de Checksum (CRC 32) e não garante qualquer integridade
    - Permite Ataques de Replay e Bit Flapping que aceleram a descoberta da chave
- Confidencialidade
  - Má implementação do algoritmo RC4
    - Reutilização de IV (24 Bits é pouco), IV enviado em claro, IV utilizado na construção da Chave, Mecanismo de Scheduling Defeituoso
  - FMS Attack – Weak IV's relevam partes da PSK (requer de 1 a 5 Milhões de Pacotes)
  - KoreK Attack - IV Unicos permitem a descobrir a chave de PSK através de estatística (250 Mil Pacotes)

Exemplos de Ataques

- Dos
- Eavesdropping
- Man in the midle
- Rogue AP

Denial of Service

- Objectivo: Negar o acesso à rede a um utilizador legítimo.
- Nível Físico
  - Interferência - Jamming
    - Sinais mais fortes sobrepõem-se ocasionando a disrupção do serviço

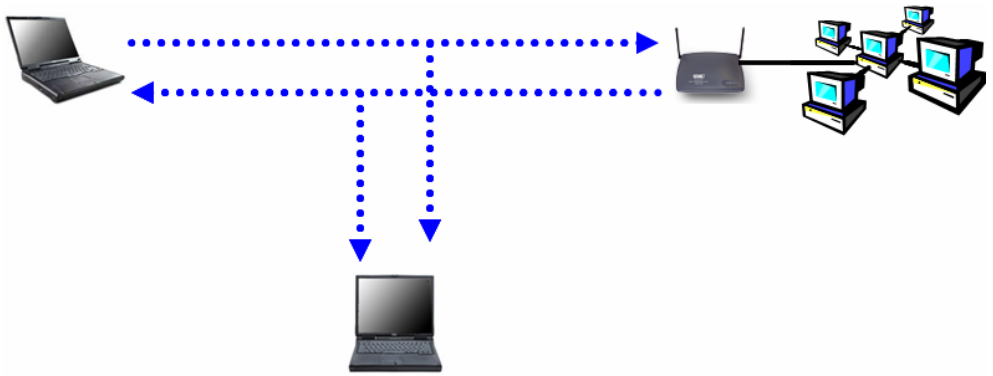
      Melhor Antena

      Mais Perto

- Nível 2 - Data Link Layer
  - Envio de Pacotes de autenticação falsos
    - O envio de pacotes falsos de-associação provoca a quebra de ligação entre o utilizador legítimo e o AP

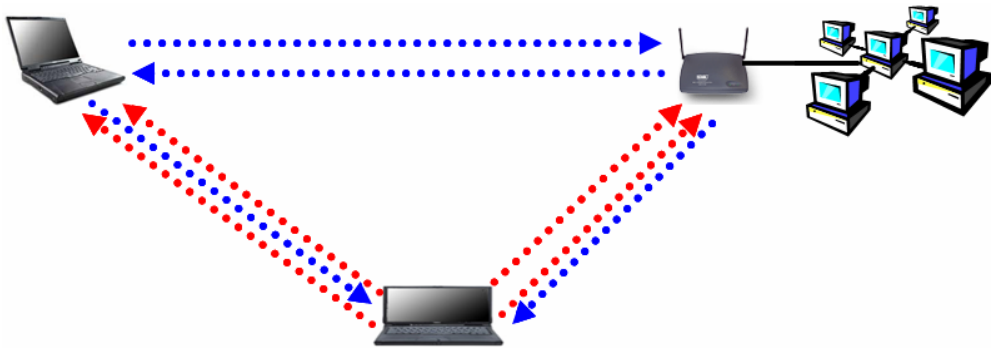
Eavesdropping

- Objectivo: Capturar informação que circula na rede (passwords, etc)
  - Sem encriptação
    - Toda a informação circula sem ser encriptada pelo ar
    - Basta uma carta wireless e um programa de sniffing para ter acesso à Informação
  - Com encriptação
    - Procura-se explorar alguns problemas do WEP de modo a descobrir a chave de encriptação
    - Com a chave é possivel desencriptar o tráfego e ter acesso a toda a informação



Man-in-the-Midle

- Objectivo: Introduzir-se no meio de uma comunicação de modo a capturar e alterar a informação entre dois utilizadores legítimos.
  - São utilizadas técnicas comuns como Arp Spoofing, IP Spoofing e Rogue AP's

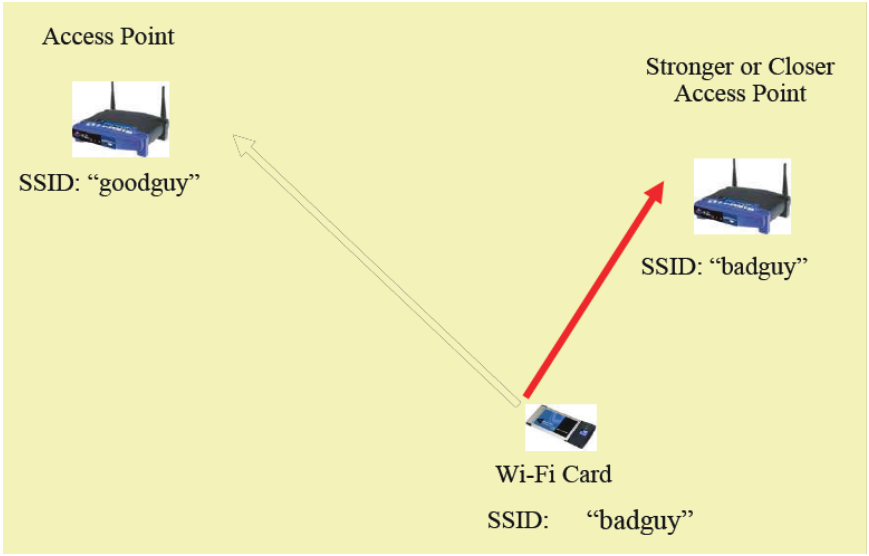


Rogue AP's

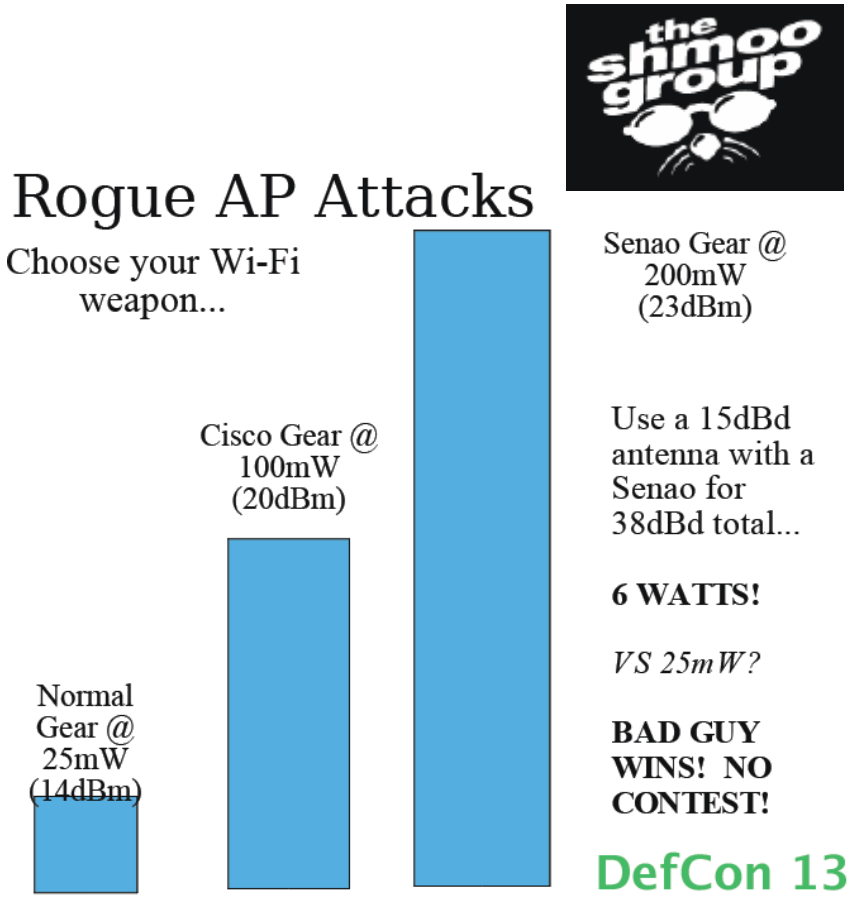
- São AP's não autorizados.
  - Utilizadores legítimos e/ou ilegítimos podem ligar um Access Point
  - Utilizador Inconsciente
    - Ao ligar um AP desprotegido à rede dá acesso imediato as todos os recursos existentes nessa mesma rede
  - Utilizador Malicioso
    - Utiliza o Rogue AP para efectuar ataques de MAN in The Midle, com o objectivo de recuperar passwords, Injectar tráfego, alterar dados em transito etc.
    - Através do MIM é possivel fazer phishing (Apresentar paginas falsas que se parecem com os sites originais ex: www.cgd.pt, www.bcp.pt)

Rogue AP's

- Como Funciona ?



Basicamente o cliente escolhe o AP com o sinal mais forte



Soluções

- WPA
  - Solução Intermédia, disponível desde 2002
- 802.11i (WPA2)
  - Standard IEE Rectificada em 2004

WPA – Wi-fi Protected Access

- WPA , solução intermédia até à definição do 802.11i (WPA2)
- Facilmente implementável em dispositivos com suporte WEP, requerendo apenas upgrade de firmware
- Combina várias tecnologias :
  - TKIP
  - 802.1X
  - EAP

Demo

Live WAP Crack Tutorial

WPA – Modos

- Enterprise
  - Requer Servidor RADIUS
  - Utiliza o RADIUS/EAP e 802.1x para autenticação e distribuição das chaves
  - Providência gestão central
- Personal
  - Pensado para Home/SOHO
  - Não requer servidor RADIUS
  - Utiliza Pre Shared Key (PSK)
  - Gestão feita no AP
  - Vulnerável a ataques de dicionário

WPA – Vantagens sobre WEP

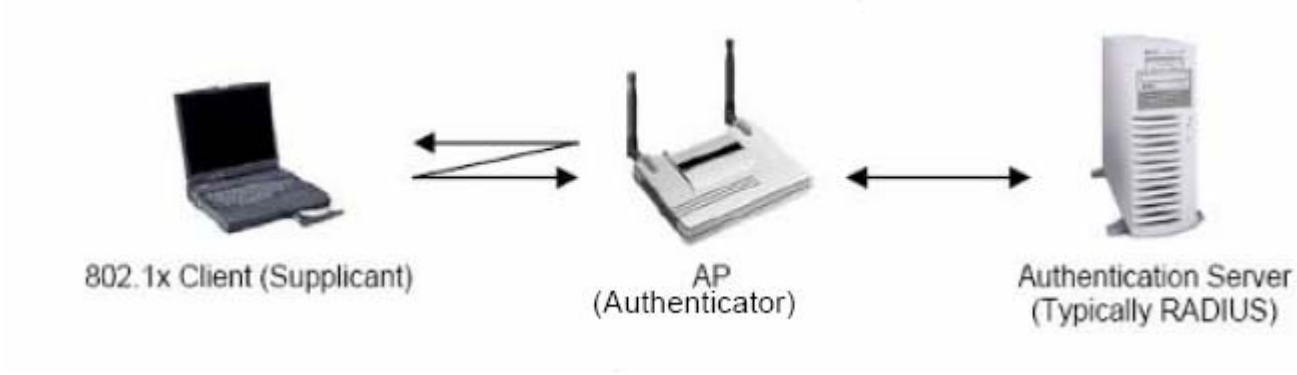
- Melhor método de autenticação e Gestão de Chaves
  - 802.1X e EAP – Extensible Authentication Protocol (Modo Enterprise)
- Melhor método de encriptação ou confidencialidade
  - TKIP – Temporal Key Integrity Protocol
- Melhor método de Integridade
  - MIC

TKIP – Temporal Key Integrity Protocol

- Substituto do WEP
- Resolve os problemas de segurança ao WEP, sem necessitar de novo hardware
- Mantém o algoritmo de encriptação (RC4) e adiciona novas funcionalidades:
  - Message Integrity code (previne a alteração da informação em transito/ Bit flapping attacks e Replay Attacks)
  - Aumenta o tamanho do IV (para 48 bits), reduzindo a reutilização do mesmo IV
  - Melhor Scheduling - Impõe regras para escolha do IV e sua reutilização caso necessário

802.1x

- Desenvolvido para redes LAN wired, permite o controlo de acesso na porta do Switch
- Análogo a um interruptor:
  - Autenticação com sucesso = Porta Aberta
  - Autenticação sem sucesso = Porta Fechada
- Possui três componentes:
  - Suplicante/cliente
  - Autenticador (Switch/AP)
  - Servidor de Autenticação (Radius)



EAP (Extensible Authentication Protocol)

- O 802.1x não define modo de como as mensagens de autenticação são trocadas entre os vários componentes, recorrendo-se do EAP para tal.
- Com o EAP actualmente podem ser utilizados quatro tipos de autenticação
  - EAP- MD5
    - Baseado em passwords
  - EAP – TLS (Transport Layer Security)
    - Baseado em certificados (Cliente/Servidor)
  - EAP - TTLS (Tunneled TLS)
    - Certificados apenas no Servidor
  - EAP- PEAP (Protected EAP)
    - Permite dois tipos de autenticação

      Microsoft CHAPV2 (Certificados apenas no Servidor)

      TLS (Certificados Cliente / Servidor)

Comparação

	EAP MD5	EAP TLS	PEAP	TTLS
Autenticação Mutua	Não	Sim	Sim	Sim
Certificados no Servidor	Não	Sim	Sim	Sim
Certificados no Cliente	Não	Sim	Não	Não
Segurança	Fraca	Super Forte	Forte	Forte
Requer PKI	Não	Sim	Não	Não
Dynamic Key Exchange (WAP Key)	Não	Sim	Sim	Sim

WPA2

- WPA2 (802.11i)
- A alteração mais significativa é a substituição do algoritmo RC4/TKIP pelo AES (Advanced Encryption Standard)
  - Este algoritmo é complexo e requer equipamentos com maior capacidade de processamento
- Utiliza as tecnologias do WPA
  - 802.1X
  - EAP

Comparação

TABLE 1 Comparing WEP, WPA And WPA2

	WEP	WPA	WPA2
Confidentiality	RC4 with WEP 24-bit IV 40/104-bit Key	RC4 with TKIP 48-bit IV 128-bit Key	AES-CCMP 48-bit IV 128-bit Key
Integrity	CRC	Michael 64-bit Key	CBC-MAC 128-bit Key
Authentication	Optional Shared Key	PSK (Personal) 802.1X (Enterprise)	PSK (Personal) 802.1X (Enterprise)
Dynamic Key Delivery	None	EAP-based	EAP-based

Comparação - Detalhes

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Per Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael (MIC)	CCM
Header Integrity	None	Michael (MIC)	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

Que outras soluções os fabricantes nos oferecem?

- Gestão centralizada
  - Gestão do espectro
  - Gestão de interferências
    - Detecção das interferências – Reacção :mudança de canal
  - Detecção e o bloqueio de Rogue AP's
    - As antenas na vizinhança aumentam o sinal para impedir o AP Malicioso
    - Detecção da localização física do AP
- AP's com Segurança Integrada
  - Sistemas de IDS Wireless
    - Detecção de ataques MIM, ARP Spoofing, DOS, etc
  - Firewall

Criticas ao 802.11i (WPA2) e WPA

- Continua sem fornecer segurança às mensagens de gestão
  - Permite a ocorrência de ataques de negação de serviço
- Factor humano
  - Chaves fracas possibilitam ataques de dicionário (Modo Personal PSK)

Questões ?

Obrigado pela sua atenção.

paulo.rosa@nextiraone.pt