GTS/GTER

2003

Rio de Janeiro - RJ

Redes Wireless: Princípios Básicos de Segurança.

André Ricardo Abed Grégio
ACME! Researcher

Luiz Otávio Duarte
ACME! Researcher

Marcelo Carvalho Sacchetin
ACME! Researcher

Adriano Mauro Cansian
ACME! Coordinator

ACME! Quem Somos:

- ACME! – Advanced Counter-measures Environment
- Localizado na UNESP – Campus de São José do Rio Preto.
- Coordenado pelo Prof. Dr. Adriano Mauro Cansian que é assessor chefe de informática na reitoria da UNESP.
- Atualmente conta com uma equipe também formada por alunos cursando graduação em Ciência da Computação.

Áreas de Pesquisas

- **Áreas de pesquisa:**
  - Detecção de Intrusão;
  - Segurança em redes *wireless*;
  - Análise de artefatos e códigos maliciosos (perícia forense computacional);
  - Honeynet e honeypots.
- **Projetos assistenciais:**
  - PROCED (Programa de Combate à Exclusão Digital) http://www.acmesecurity.org/proced
  - Forum de discussões ACME! – https://forum.acmesecurity.org.

Agenda

- Introdução às redes *wireless*
- Protocolo 802.11
- WEP
- Vulnerabilidades, ferramentas e ataques
- Segurança em redes *wireless*

Introdução

- O que são redes *wireless?*
- Como funcionam?
- Onde são utilizadas?
- Dispositivos e equipamentos;
- Problemas na transmissão.

Redes wireless, necessidades

- Nas últimas décadas as LANs (*Local Area Networks*) sofreram um crescimento explosivo.
  - As LANs cabeadas se tornaram ingrediente indispensável para o mundo dos negócios.
- Surge uma indústria multi-bilionária para suprir a necessidade das LANs cabeadas.
- Necessidades de redes *wireless*:
  - Computação cada vez mais pessoal;
  - Necessidade do homem em se manter em movimento;
  - Barateamento de equipamentos de tecnologia celular.
- Redes *wireless* podem ser obtidas via rádio freqüência, IrDA ou laser.

GTS 27/11/2003 7

LAN's nas Instituições (1/3)

- LANs estão presentes na infra-estrutura interna das instituições;
- Crescimento da utilização destas LANs é acelerado e lembra a internet no início dos anos 90;
- Indispensável para o funcionamento das empresas;
- Alto custo da infra-estrutura cabeada para interconectar pontos da rede;
- Solução: não usar cabos.

GTS 27/11/2003 8

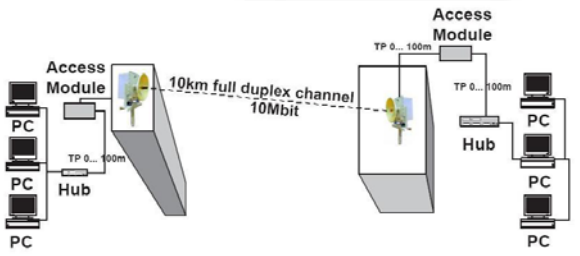
LAN's nas Instituições (2/3)

- WLANs (*Wireless Local Area Networks*) são mais baratas e com desempenho comparável às redes cabeadas;
- Tecnologia *spread spectrum* nas redes *wireless* por rádio frequência (RF) visando diminuir interferências;
- Assim como no início da internet, existem problemas de segurança devido à falta de preocupação efetiva por parte das instituições.

GTS 27/11/2003 9

LAN's nas Instituições (3/3)

- ***Radio bridges*** **são amplamente utilizados para interligar LAN's localizadas em diferentes construções.**



Desenvolvimento

- **A tecnologia *wireless* cresce ao longo dos anos**
  - **Crescimento devido ao ganho de performance dos semicontutores, o barateamento da tecnologia e também pela necessidade de maiores taxas de transferência, bem como, de bandas com poucos ruídos.**
- **As 4 gerações de produtos *Wireless*:**
  - **1ª. Opera na banda ISM (Industrial Scientifc and Medical) que abrange de 902 a 928 MHz. Consegue taxas de 500 Kbps;**
  - **2ª. Opera na ISM que abrange de 2.40 a 2.48 GHz. Consegue taxas de 2 Mbps;**
  - **3ª. Opera na ISM de 2.4 Ghz. Conseguindo taxas de 11Mbps;**
  - **4ª. Opera na ISM que abrange de 5.775 a 5.850 GHz. Conseguindo 10 Mbps de início.**

Equipamentos

Existe uma quantidade muito grande de equipamentos para redes *wireless*. Estes equipamentos podem ser agrupados nas categorias:

- ***Access Points***
- **Antenas**
- **Placas de Rede**
  - **PCI**
  - **PCMCIA**
  - **Compact Flash**

Access Points

- AP – *Access Point*:
  - Pode operar como *switch/gateway/bridge/router*;
  - É o dispositivo que provê o acesso à rede *wireless*;
  - Uma estação comum pode trabalhar como um AP através de softwares como o *HostAP* (http://hostap.epitest.fi);
  - Um AP é identificado dentro da rede através de seu SSID (*Service Set Identifier*);
  - Também utilizado como portal para interligar a rede *wireless* à guiada.

Access points

- AP – Netgear 11 Mbps, WEP 128, padrão 802.11b

Access points

- AP – U.S. Robotics 22 Mbps

Access points

- AP – Belkin SOHO Access Point

GTS 27/11/2003 16

Access points

- AP – Action Tec 54 Mbps, 802.11g

GTS 27/11/2003 17

Access points

- AP – D-Link 11 Mbps

GTS 27/11/2003 18

Access points

- AP – D-Link Outdoor Access Point 11 Mbps

Access points

- AP – Linksys 2.4GHz, 802.11b, 11Mbps

Antenas

- Extensão de um transmissor ou receptor de rádio utilizadas para aumentar a área de cobertura da rede *wireless*.
- Tipos de antena:
  - Direcional;
  - Omni-Direcional;
  - Grade Parabólica;
  - Setorial.

Antena Radome-Enclosed Yagi

- Antena direcional de alta qualidade;
- Leve, fácil de instalar e capaz de suportar condições extremas;
- Aumenta em cerca de três vezes a distância da capacidade de conexão.

Antena Radome-Enclosed Yagi

- Especificações técnicas:
- Freqüência: 2.4 – 2.5 GHz
- Ganho: 14.5 dBi
- Potência Máxima de Entrada: 50 Watts
- Polarização: Vertical

Antena com grade parabólica

- Alta performance, minimiza interferência e maximiza a potência.
- Excelente para montar em telhados (conexão *building-to-building*)

Antena com grade parabólica

- Especificações técnicas:

- Freqüência: 2.4 – 2.5 GHz
- Ganho: 19 dBi
- Potência Máxima de Entrada: 50 Watts
- Polarização: Vertical ou Horizontal

Antena feita com pote de batata

- Montando uma antena direcional apartir de um pote de batatas: (http://www.turnpoint.net/wireless/has.html)

(http://www.oreillynet.com/cs/weblog/view/wlg/448http://www.oreillynet.com/cs/weblog/view/wlg/448)

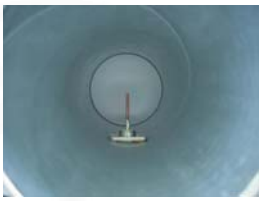
Antena feita com pote de batata

- Comparação entre antenas comerciais e uma caseira

Antenna	Signal	Noise
10db A:	-83db	-92db
10db B:	-83db	-92db
11db:	-82db	-95db
24db:	-67db	-102db
Pote batata:	-78db	-99db

Antena feita com pote de batata

- Parte Interna



GTS 27/11/2003 28

SigMax Omni-Direcional

- Aplicações multiponto de médio a longo alcance;
- Adequada para estender a cobertura de *access points* corporativos.

GTS 27/11/2003 29

SigMax Omni-Direcional

- Especificações técnicas:

- Freqüência: 2.4 – 2.5 GHz
- Ganho: 10 dBi
- Potência Máxima de Entrada: 50 Watts
- Polarização: Vertical

GTS 27/11/2003 30

SigMax Circular Yagi

- Altas taxas de performance;
- Própria para uso em ambientes internos;
- Direcional.

SigMax Circular Yagi

- Especificações técnicas:
- Freqüência: 2.4 – 2.5 GHz
- Ganho: 12 dBi
- Potência Máxima de Entrada: 50 Watts
- Polarização: Vertical e Horizontal

Technolab Log Periodic Yagi

- Antena direcional adequada para atividades "indoor";
- Útil no perímetro externo para criação de links building-to-building;
- Permite utilização em outras aplicações além de redes *wireless*.

Technolab Log Periodic Yagi

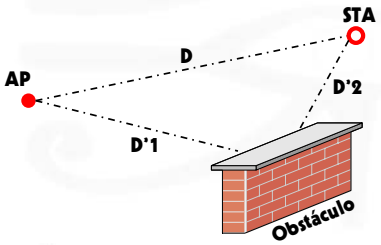
- Especificações técnicas:
- Freqüência: 0.9 – 2.6 GHz
- Ganho: 12 dBi
- Potência Máxima de Entrada: 10 Watts

Problemas na Transmissão

- **Refração**: ocorre quando uma onda eletromagnética se propaga e se depara com um objeto que é muito grande em relação ao comprimento de onda. Ocorre na superfície da terra, muros e paredes;
- **Dispersão**: ocorre quando a onda atravessa um meio composto por uma porção de objetos pequenos em relação ao comprimento de onda. Ocorre em superfícies rugosas e folhas de árvores;
- **Difração**: é o fenômeno que ocorre quando o caminho entre o emissor e o receptor é obstruído distorcendo a onda;

Problemas na Transmissão

- Multipath (multicaminho) é um fenômeno causado principalmente devido ao problema da refração, além da difração e dispersão;



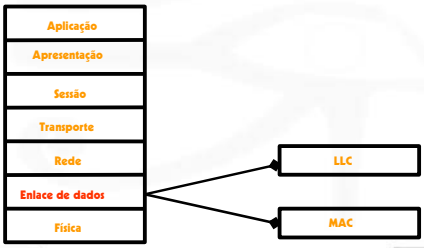
D' = D'1 + D'2
D < D'

Agenda

- Introdução às redes *wireless*
- Protocolo 802.11
- WEP
- Vulnerabilidades, ferramentas e ataques
- Segurança em redes *wireless*

Ethernet X Wireless

- Redes *wireless* são compatíveis com redes cabeadas.
  - As únicas mudanças para produtos *wireless* repousa sobre as duas primeiras camadas do modelo OSI. Mais especificamente na camada física e metade inferior da camada de enlace de dados, conhecida como MAC (*Media Access Control*).

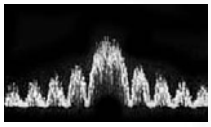


Camada Física (PHY)

- Diferentes PHYs são definidas como parte do padrão IEEE 802.11, tais como:
  - FHSS (*Frequency-Hoping spread spectrum*);
  - DSSS (*Direct sequence spread spectrum*);
  - IR (infravermelho).

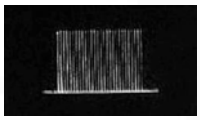
DSSS

- Auxilia na prevenção da interferência espalhando o sinal por diversas freqüências ao mesmo tempo;
- Aumenta a banda, permite múltiplos dispositivos operando.



FHSS

- Combinado com uma freqüência de 2.4 GHz, um sinal pode trocar canais 50 vezes por segundo;
- Provê serviço confiável: múltiplas redes podem operar na mesma área sem medo de colisão.

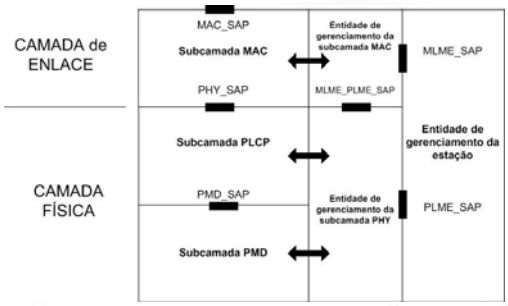


Funções da PHY

- A implementação da PHY apresenta 3 entidades funcionais:
  - PLCP (*physical layer convergence procedure)*: mapeamento das unidades na camada MAC;
  - PMD (*physical medium dependent)*: define as características e o método de transmissão e recebimento de dados através de um WM (meio sem fio) entre duas ou mais estações;
  - Entidade de gerenciamento.

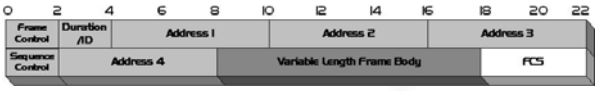
Funções da PHY

- **Relação entre as 3 entidades da camada física (PHY):**



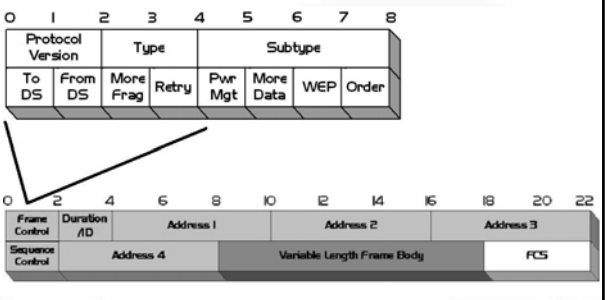
Camada de Enlace

- **O MAC *frame* é formado por 3 componentes básicos:**
  - **Cabeçalho MAC;**
  - **Corpo do frame;**
  - **FCS: *Frame Check Sequence.***



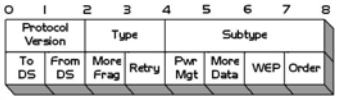
Camada de Enlace

- ***Frame Control*: representado pelos 2 primeiros *bytes* do MAC *frame*.**



Camada de Enlace

- Campos do *Frame Control:*
  - *Protocol Version* (Versão do Protocolo), com tamanho fixo de 2 bits e possui valor 0 (zero) para o padrão corrente;
  - *Type* (Tipo), com comprimento de 2 bits, identifica a função do *frame* e pode ser de controle, de dado ou de gerenciamento;
  - *Subtype* (Subtipo), com comprimento de 4 bits, identifica a função do *frame* em conjunto com o tipo, podendo haver diversas combinações entre os mesmos;



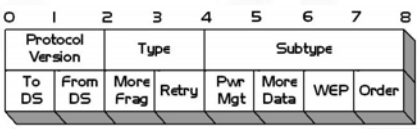
Camada de Enlace

- Campos do *Frame Control: Subtype*

Type value b3 b2	Type Description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1011	Authentication
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment(ACK)
10	Data	0000	Data

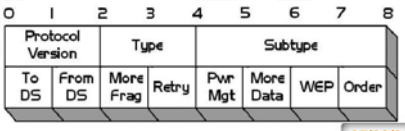
Camada de Enlace

- Campos do *Frame Control:*
  - *To DS* e *From DS*, cada qual sendo de 1 bit e tendo a função de identificar se o *frame* está sendo enviado, se está chegando, se a comunicação é entre dois *access points* ou estações;
  - *More Fragments* (Mais Fragmentos), com tamanho de 1 bit, contendo valor um ou zero, de forma a indicar a existência de mais fragmentos ou não;



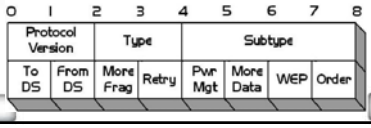
Camada de Enlace

- **Campos do *Frame Control:***
  - ***Retry*** **(Nova Tentativa), de comprimento de 1 bit, serve para controle de retransmissões e *frames* duplicados;**
  - ***Power Management*** **(Gerenciamento de Energia), que indica o modo de gerenciamento de energia de uma estação, sendo que o valor designado um significa que esta estará em modo de economia de energia e zero em modo ativo. Seu comprimento é de 1 bit;**



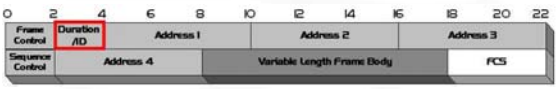
Camada de Enlace

- **Campos do *Frame Control:***
  - ***More Data*** **(Mais Dados), com tamanho de 1 bit, usado para indicar a existência de unidades de dados em registro no *access point* para a estação;**
  - **WEP, bit utilizado para indicar a presença ou não de WEP;**
  - ***Order*** **(Ordem), de 1 bit de comprimento, utilizado para classificar se o fragmento usa a classe de serviço *StrictlyOrdered*** **(estritamente ordenado) ou não.**



Camada de Enlace

- **O campo *Duration/ID*** **(Duração/ID), cujo comprimento é 16 bits, carrega o ID de associação da estação que transmitiu o *frame*, além do valor de duração definido para cada tipo de *frame*.**

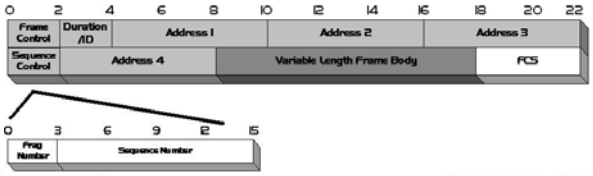


Camada de Enlace

- Os quatro campos de ***Address*** (Endereço), são usados para indicar os endereços de origem e de destino, os endereços da estação transmissora e da receptora.
- 48 bits para cada endereço.

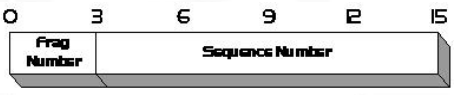
Camada de Enlace

- ***Sequence Control***: representado pelos *bytes 22 até 24* do MAC *frame*. é utilizado na manutenção dos *frames* em fluxo, possui 16 bits de comprimento e consiste dos subcampos ***Sequence Number*** (Número de Seqüência), de 12 bits e ***Fragment*** Number (Número do Fragmento), de 4 bits.



Camada de Enlace

- ***Sequence Control***
  - O campo ***Sequence Number*** (Número de Seqüência) é um campo de 12 bits e indica o número de seqüência de um MSDU (***MAC Service Data Unit***) enviado por uma estação. Este número é atribuído pelo módulo de 4096, começando em 0 e sendo incrementado de 1 a cada MSDU.
  - O campo ***Fragment Number*** (Número do Fragmento) é o campo que indica o número de cada fragmento de um MSDU enviado. Este campo é atribuído com 0 no primeiro ou único fragmento e é acrescido de 1 para cada um dos fragmentos remanescentes.



Camada de Enlace

- ***Frame Body Field***
  - Tem tamanho variável e contém informações específicas para cada tipo e subtipo de *frame*.

Camada de Enlace

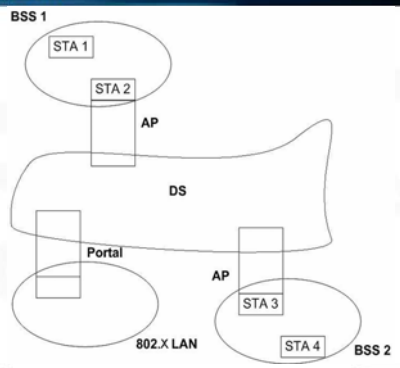
- ***Frame Check Sequence (FCS)***
  - O FCS é calculado sobre todos os campos do cabeçalho MAC e do corpo do *frame*. Apresenta 32 bits de tamanho.
  - É calculado usando gerador polinomial de grau 32:

- $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1$

Nomenclaturas IEEE 802.11

- **STA** – ***Wireless Station.***
  - Qualquer estação de trabalho que possua dispositivo *wireless*.
- **WLAN** – ***Wireless Local Area Network.***
  - Rede local de computadores interligados por uma infra-estrutura *wireless*.
- **BSS** – ***Basic Service Set.***
  - É o componente básico de uma rede local *wireless*.
- **DS** – ***Distribution System.***
  - É formado pela interligação de vários BSSs.

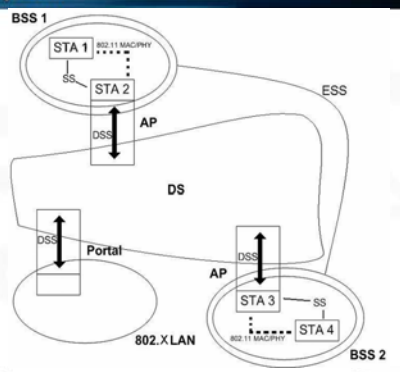
Estrutura lógica IEEE 802.11



Tipos de Serviço

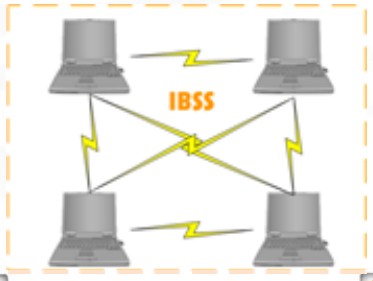
- O padrão IEEE 802.11 divide os serviços da rede *wireless* em duas categorias: SS *station service* e DSS *distribution system service*
- SS *station service*:
  - Autenticação / desautenticação
  - Distribuição de MSDU (unidade de dados trocadas por serviços)
  - Privacidade
- DSS *distribution system service:*
  - Associação / desassociação / reassociação
  - Distribuição / integração

Estrutura lógica completa IEEE 802.11



Modos de operação

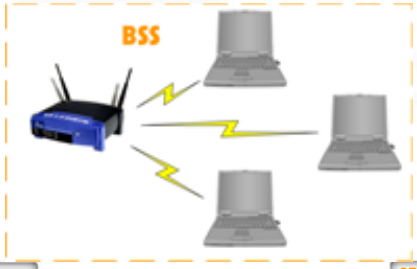
- **Redes Independentes (*Ad Hoc*)**
  - São redes que possuem somente STAs que se comunicam mutuamente. Todas possuem o mesmo BSSID (identificador de BSS). O termo mais correto para redes *Ad Hoc* é IBSS (*Independent BSS*).



GTS 27/11/2003 61

Modos de operação

- **Redes de Infra-estrutura básica (BSS)**
  - Um conjunto de STAs controlados por um AP. Toda conexão é realizada através deste AP. O termo mais correto para uma rede de infra-estrutura básica é BSS.



GTS 27/11/2003 62

Modos de operação

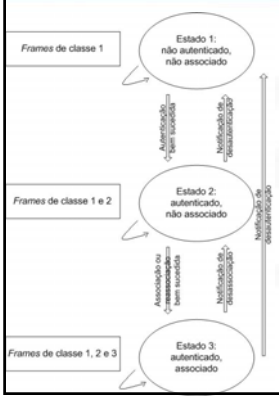
- **Rede infra-estruturada (ESS)**
  - Um número de BSSs conectadas com a finalidade de que as STAs aparentem estar em uma rede única. Este esquema é tecnicamente chamado de ESS (*Extended Service Set*)

GTS 27/11/2003 63

Autenticação e Associação

- Uma estação mantém duas variáveis de estado para cada estação com a qual se estabelece uma comunicação direta via meio *wireless* (WM - *wireless medium*)
  - estado de autenticação: os valores são autenticado e não autenticado;
  - estado de associação: os valores são associado e não associado.
- Dessa forma, uma estação pode assumir três estados locais:
  - estado 1 (estado inicial): não autenticado e não associado;
  - estado 2: autenticado e não associado;
  - estado 3: autenticado e associado;

Autenticação e Associação



- Os frames trocados pelas estações são agrupados em três classes de acordo com o estado atual de cada estação.
- No estado 1 são permitidos somente *frames* de classe 1. No estado 2 são permitido *frames* de classe 1 e 2. No estado 3 todos os *frames* são permitidos (classe 1, 2 e 3).

Autenticação em redes wireless

- Quando um cliente pretende entrar em uma rede *wireless* específica ele precisa se autenticar.
- Esta autenticação pode ser feita de duas formas, na camada 2 ou na camada 3 do modelo OSI.
  - A autenticação e privacidade na camada 3 seria baseado em endereços IPs um exemplo comum seria o uso de autenticação com servidores RADIUS.
- O padrão IEEE 802.11-1997, apenas define o WEP (*Wired Equivalent Privacity*) como opção de segurança, feita em camada 2.
- O grupo de trabalho do IEEE 802.11, bem como a aliança WiFi estudam formas de autenticação e privacidade alternativas ao WEP.

WEP (Wired Equivalent Privacy)

- Nas redes IEEE 802.11b o tráfego é criptografado utilizando-se o WEP.
  - Este algoritmo é simétrico e as chaves são compartilhadas.
- As chaves WEP possuem vulnerabilidades.
  - Os tamanhos das chaves criptográficas variam de 64-128 bits.
  - Quando foi proposto, este algoritmo se tornou alvo de estudos e uma série de vulnerabilidades foram encontradas.
- Ataques ao WEP
  - Já existem ferramentas que conseguem quebrar facilmente este tipo de criptografia.
  - Uma forma de se prevenir destes ataques é fazer a troca da chave de criptografia periodicamente, como de 10 em 10 minutos. Isto não é implementado no IEEE 802.11b.

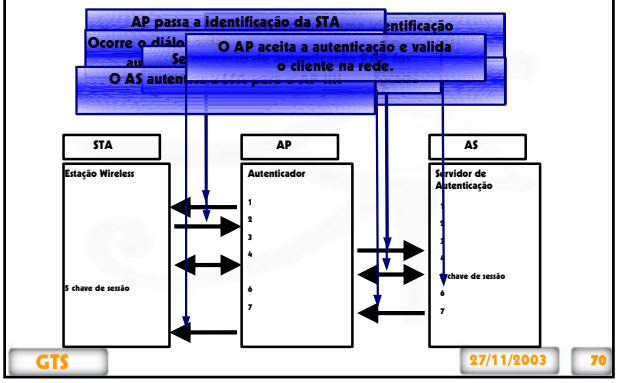
Configuração de autenticação

- Quando se configura um AP, existem três formas de autenticação possíveis:
  - *Open Authentication* (Autenticação Aberta) – Qualquer estação *wireless* pode se associar ao *access point* e obter acesso a rede.
  - *Shared Authentication* (Autenticação Compartilhada) – Onde chaves WEP são previamente compartilhadas. Estas são utilizadas para autenticar uma estação *wireless* a um *access point*.
  - *Network-EAP* – Baseado em algoritmos EAP (*Extensible Authorization Protocol*) que operam sobre o padrão IEEE-802.1x

Autenticação 802.1x

- Um padrão mais robusto que utilizaremos para ilustrar o processo de autenticação de acesso entre uma estação cliente e um ponto de acesso é o especificado no 802.1x;
- Um servidor RADIUS é utilizado para prover esta autenticação;
- O diálogo de autenticação entre a estação e o servidor RADIUS é feita através de frames EAP.

Exemplo de autenticação 802.1x



Alguns padrões para redes wireless

- **IEEE 802.11**
  - Primeiro padrão utilizado para redes *wireless*.
  - Este padrão inclui suporte para WEP para proteger as mensagens trocadas entre os hosts.
- **IEEE 802.11b**
  - Opera em 2.4 Ghz atingindo 11 Mbps e provê WEP.
  - É o padrão mais utilizado atualmente.
- **IEEE 802.11g**
  - Padrão para prover 54 Mbps em 2.4 GHz.
  - Este, ganhou aprovação do grupo de trabalho da IEEE 802.11 em junho de 2003.
- **IEEE 802.11i**
  - Padrão para prover maior nível de segurança.
  - Ainda não ratificado pelo grupo de trabalho da IEEE 802.11.

O padrão 802.11

- Define os protocolos que governam todo o tráfego *wireless* baseado em *ethernet*;
- Composto de diversos sub-padrões (a, b, g).

O padrão 802.11a

- Primeiro padrão *wireless* oficialmente ratificado;
- Baseado em novas tecnologias, utiliza diferente tipo de transmissão de dados;
- Freqüência: 5GHz;
- Velocidade: 54Mbps;
- OFDM – *Orthogonal Frequency Division Multiplexing*.

O padrão 802.11b

- Utilizado pela grande maioria das redes *wireless*;
- Suporta a velocidade baixa (1-2 Mbps) das WLANs mais antigas;
- Freqüência: 2.4 GHz;
- Velocidade: 5.5 – 11 Mbps;
- DSSS – *Direct-Sequence Spread Spectrum*.

802.11a X 802.11b

- 802.11a:
  - Mais veloz, maior transferência de dados ao mesmo tempo;
  - Custoso, incompatível com o padrão dominante (802.11b), maior freqüência diminuindo a área de cobertura da rede.
- 802.11b:
  - Mais difundido, mais barato, alcance maior do sinal.

O padrão 802.11g

- Funde as boas características dos padrões 802.11a e 802.11b:
  - Compatibilidade (2.4 GHz);
  - Velocidade (24 – 54 Mbps);
  - OFDM (maior velocidade de transmissão, redução de colisão).

O padrão 802.11i

- Padrão proposto para solucionar os problemas de segurança devido as vulnerabilidades encontradas nos padrões anteriores:
  - TKIP (Temporal Key Integrity Protocol);
  - AES (Advanced Encryption Standard);
- WPA (Wifi Protect Access): é um pré-padrão utilizado temporariamente até a ratificação do IEEE 802.11i.
  - Provê chaveamento por TKIP, que diz resolver os problemas do WEP

HomeRF

- Padrão vida curta:
  - Voz e dados ao mesmo tempo;
  - Sem necessidade de *access point* para conversão de sinais;
  - FHSS – *Frequency Hopping Spread Spectrum*;
  - 2.4 GHz / 1.6 Mbps;
  - Serviço confiável;

Agenda

- Introdução às redes *wireless*
- Protocolo 802.11
- WEP
- Vulnerabilidades, ferramentas e ataques
- Segurança em redes *wireless*

Segurança WEP

- *Wired Equivalent Privacy*
- Protocolo incorporado ao 802.11b
- 40 – 104 bits
- Algoritmo de encriptação: RC4

Criptografia

- Simétrica: a mesma chave é usada tanto para criptografar quando para descriptografar.
- Assimétrica: utiliza o conceito de chave pública e chave privada.
- Desvantagens: perda de senha, sobrecarga, falsa sensação de segurança.

Cifras

- **Tipos:**
  - **Bloco**
    - **Toma um largo pedaço de dados e criptografa com a chave;**
    - **O processo é repetido até que a mensagem esteja completamente encriptada;**

```
Cipher Function (data, passphrase) = Output
```

    - **DES.**

Cifras

- **Tipos:**
  - **Faixa *(stream)***
    - **Criptografa a mensagem em uma escala menor, em nível de bits;**
    - **Utiliza uma condição de estado, além da *passphrase* e do dado;**
    - ***Cifra com auto-sincronismo***
      - ***Key stream generator***

$State_{Time+1}=StateFunction(State_{Time},Data_{Time},Password_{Time})$

      - **Função de cifragem**

$Output_{Time}=CipherFunction(State_{Time},Data_{Time},Password_{Time})$

    - **RC4.**

RC4

- **Criado pela *RSA Data Security*;**
- **Comercial, o código vazou pela *Internet* em 1994;**
- **Utilizado por várias tecnologias:**
  - ***SSL (Secure Sockets Layer);***
  - ***WEP (Wired Equivalent Privacy).***

RC4

- Utiliza XOR (Ou-Exclusivo);
- Combina a saída de um gerador de chave com o texto claro da mensagem;
- Relativamente imprevisível;
- Utiliza "estados", armazenados em um vetor que é uma matriz de valores;

RC4

- Vetor de Inicialização:
  - Composto de valores randômicos
  - Vetor de estados + propriedades da senha.
  - WEP:
    - V.I.: 24 bits (3 bytes)
  - Mesmo estado interno que criou a cifra de *streaming* deve ser gerado no lado de descriptografia

RC4

- Algoritmo gerador randômico
- KSA *(Key Scheduling Algorithm)*
  - WEP:
    - RC4 de 8 bits
    - Cria um vetor com 256 valores de 8 bit
  - Embaralha o vetor
  - Criptografa o texto claro (XOR)
  - O texto cifrado é enviado para o destinatário

Entendendo a força da chave WEP

- Na criação do *password*, os caracteres são convertidos em seu equivalente binário
- Se uma senha de 5 caracteres (40 bits) é colocada, os outros 24 bits são do V.I.
- O V.I. não é seguro, seus valores são enviados em texto plano!

CRC

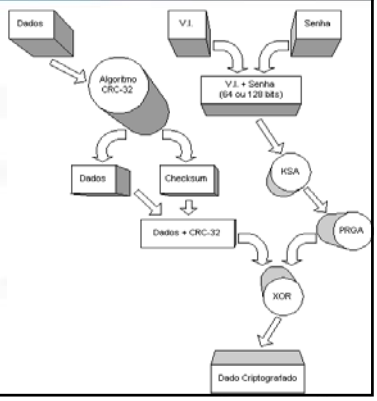
- *Cyclic Redundancy Checks*
- Verifica a integridade dos dados
- Dados são segmentados e remontados, e não devem ser corrompidos
- *Checksum* (4 bytes)

O Processo WEP

Encriptação WEP

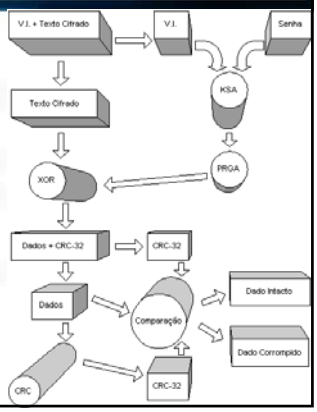
+

checksumming:



O Processo WEP

Desencriptação WEP:



GTS

Agenda

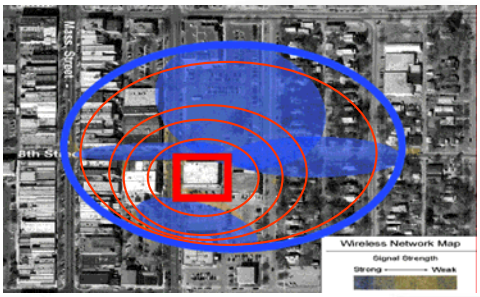
- Introdução às redes *wireless*
- Protocolo 802.11
- WEP
- Vulnerabilidades, ferramentas e ataques
- Segurança em redes *wireless*

Cenário

- Além de todos o problemas de segurança já existentes nas redes cabeadas, a tecnologia *wireless* apresenta vulnerabilidades adicionais inerentes à transmissão por rádio frequência (RF);
- Algumas empresas cometem o erro de não se preocupar com a segurança *wireless* se elas não têm sistemas críticos com informações restritas passando por estas redes;
- Entretanto poucas redes trabalham como LANs isoladas;

Cenário

- Um AP típico em uma rede *wireless*, basicamente faz um broadcast de uma conexão *ethernet*;



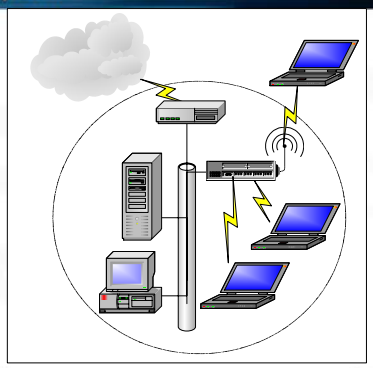
GTS 27/11/2003 94

Cenário

- O nível de segurança de uma instituição que apresenta uma política de segurança bem concisa para redes cabeadas, deixando em aberto a questão da sua rede *wireless*, pode ser comparada à construção de uma casa com uma porta de ferro bem reforçada, mas com paredes de vidro;
- Dessa forma um intruso terá facilidade em explorar as vulnerabilidades da rede *wireless* (parede de vidro) para lançar seu ataque sem precisar "driblar" um bom firewall (porta de ferro) por exemplo;

GTS 27/11/2003 95

Cenário



GTS 27/11/2003 96

Riscos de segurança das WLANs

- **Vulnerabilidades Internas.**
  - São vulnerabilidades que ocorrem devido a **má configuração** de equipamentos. Não dependem de um potencial atacante externo.
  - Fazem parte destas vulnerabilidades:
    - **WLANs Grampeáveis / *Rouge* WLANs;**
    - **Configuração inseguras de rede;**
    - **Associação acidental.**
- **Riscos Externos.**
  - São aqueles em que um atacante externo explora vulnerabilidades bem conhecidas de redes *wireless.*
  - Fazem parte destas vulnerabilidades:
    - ***Eavesdropping & Espionage*;**
    - **Roubo de identidade;**
    - **Ataques emergentes.**

Vulnerabilidades Internas (1/3)

- **WLANs Grampeáveis/ *Rogue WLANs***
  - São redes *wireless* onde ocorrem **acesso não autorizado.**
    - ***Access points* conectados em redes corporativas são utilizados como ponto de acesso externo sem o aval da empresa.**
    - **Estações de trabalho configuradas para trabalhar em modo *Ad Hoc.* Ou seja, estas estações estão abertas a ataques externos.**
  - ***Rogue Acess Points* podem ser escondidos bastando duplicar o MAC de uma máquina legítima.**
  - **Em 2001 estimava-se que 20% das redes corporativas dos EUA possuíam *rogue WLANs.***

Vulnerabilidades Internas (2/3)

- **Configuração de rede Insegura.**
  - Muitas empresas fazem a segurança de suas redes *wireless* com a utilização de **VPNs** e cometem o erro de achar que suas redes são a prova de bala.
  - Este tipo de abordagem faz com que **as demais configurações permanecam padrões.**
    - **Isto faz com que passwords fiquem padrões;**
    - ***Broadcasts* de SSIDs;**
    - **Criptografia fraca ou ausente.**
  - Técnicas mais sofisticadas conseguem atacar VPNs, mas a opção mais simples seria atacar o próprio *access point.*

Vulnerabilidades Internas (3/3)

- **Associação Acidental**
  - Ocorre quando um *access point* "a" emite um forte sinal RF que faz com que o sinal pareça melhor do que a de uma rede *wireless* vizinha "b".
  - O que ocorre então é que estações de "b" se associam a "a"
  - O Windows XP se associa automaticamente a estas redes sem o consentimento do usuário ou da rede vizinha.
  - Um outro problema grave pode ocorrer se os dois *access points* de associarem gerando uma ESS. Ou seja, fazendo com que duas redes distintas aparentassem ser uma única rede.

Vulnerabilidades Externas (1/3)

- ***Eavesdropping & Espionage.***
  - É a escuta das ondas de rádio com a finalidade de se obter informações valiosas sobre a rede.
  - Mensagens encriptadas com WEP podem ser facilmente decriptadas com um pouco de tempo e a utilização de ferramentas hackers.
  - É importante ressaltar que é um trabalho difícil identificar atacantes que se utilizam dessas técnicas.

Vulnerabilidades Externas (2/3)

- **Roubo de identidade**
  - O atacante descobre o *access point* através de *scans* e a partir de então captura o tráfego da rede.
  - A identidade é roubada através da descoberta dos SSIDs e da descoberta de um MAC válido, de um cliente que seja válido.
  - O atacante seta seus SSIDs e seu MAC como sendo de um usuário válido na rede.

Vulnerabilidades Externas (3/3)

- *Evolving Attacks.*
  - São ataques mais sofisticados, como *Denial-of-Service* e *Man-in-the-Middle*.
  - Ataques como *Denial-of-Service* fazem com que serviços de redes fiquem desabilitados.
  - Ataques como *Man-in-the-Middle* consequem comprometer redes privadas virtuais (VPNs).
  - Estes dois tipos de ataques são mais difíceis de serem efetuados, mas quando bem efetuados podem deixar a rede inteira comprometida.

Ferramentas para redes wireless

- Ethereal;
- Netstumbler;
- Kismet;
- AirSnort;
- WEPCrack;
- Windows XP;
- Wellenreiter;

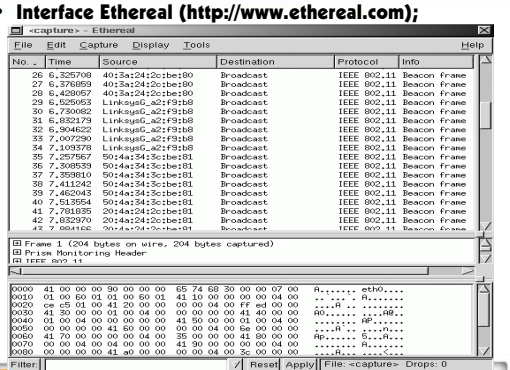
- Ferramentas para handhelds.

Ferramentas: Ethereal

- Ethereal (http://www.ethereal.com);
- Utilizada para capturar tráfego em redes cabeadas ou *wireless*;
- É um *sniffer* que se utiliza da biblioteca de captura libpcap para realizar a sondagem passiva;
- Utilizado em plataformas Linux e Windows, entretanto o funcionamento em Windows é pouco eficiente;

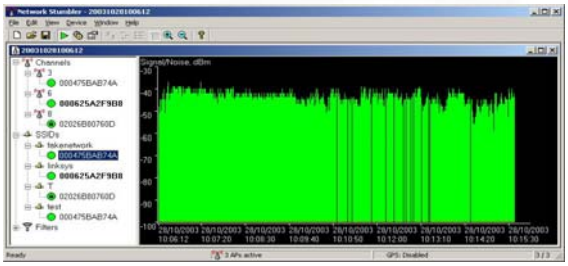
Ferramentas: Ethereal

- **Interface Ethereal (http://www.ethereal.com);**



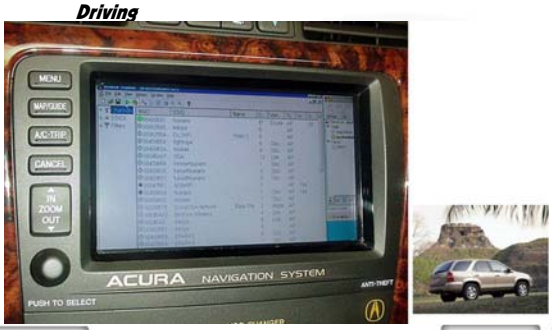
Ferramentas: Netstumbler

- **NetStumbler (www.netstumbler.com) é uma ferramenta para Windows que, por sondagem ativa faz, *probes* para tentar encontrar APs e levantar informações a seu respeito;**



Ferramentas: Netstumbler

- **Interface do NetStumbler no painel de um carro: *War Driving***



Ferramentas: Kismet

- Kismet (http://www.kismetwireless.net);
- Através de sondagem passiva, faz um levantamento sobre *access points* e estações encontradas na rede;
- É uma ferramenta de código aberto, eficiente, que fornece diversas informações tais como:
  - Número de WLANs detectadas;
  - Número total de pacotes capturados por WLAN;
  - Ausência ou não de criptografia WEP;
  - Número de pacotes com o I.V. fraco;
  - Número de pacotes irreconhecíveis;

Ferramentas: Kismet

- Informações fornecidas pelo Kismet (continuação):
  - Número de pacotes descartados;
  - Tempo decorrido desde a execução do programa;
  - SSID, BSSID (relaciona-se ao endereço MAC do *access point*);
  - Taxa máxima suportada pela rede;
  - Identifica se o dispositivo monitorado é um *access point*, ou um dispositivo convencional, qual o canal que a WLAN esta configurada e se suporta WEP;
  - IP e endereço MAC de estações conectadas aos *access points*.

Ferramentas: Kismet

- Interface do Kismet

Ferramentas: AirSnort

- AirSnort (http://airsnort.shmoo.com)
- É um programa para quebra de chaves WEP;
- Difere do WEPCrack pois consegue quebrar qualquer chave WEP após de se obter de três milhões a cinco milhões de pacotes trocados.

Ferramentas: WEPCrack

- WEPCrack (http://sourceforge.net/projects/wepcrack/)
- Trabalha utilizando-se da vulnerabilidade encontrada no início do ano 2001 no WEP. É um script *perl* que supostamente funcionaria em qualquer sistema com suporte a este tipo de script. No entanto, somente se torna inteiramente funcional em sistemas Unix.

Ferramentas: Windows XP

- Windows XP (http://www.microsoft.com/windowsxp/default.asp)
- Sistema operacional muito suscetível ao ataque de associação maliciosa
- *Notebooks* com interfaces *wireless* embutidas apresentam-se como uma vulnerabilidade para usuários leigos

Ferramentas: Wellenreiter

- Wellenreiter (http://www.wellenreiter.net)
- Aplicação Perl/Gtk+ para sistemas Linux que utiliza a técnica de sondagem passiva
- Apresenta um recurso adicional para realizar força bruta de ESSID e com geração de endereços MAC aleatórios. Para efetuar esses procedimentos a ferramenta utiliza sondagem ativa

Dispositivos Handheld

- PDAs (Personal Data Assistants)
- Dispositivos portáteis que provêem mobilidade;
- Palm (PalmOS);
- Pocket PC (Windows CE);
- Compaq iPAQ.

Compaq iPAQ

- iPAQ 3650
- Características:
  - Sistema Operacional Microsoft Pocket PC;
  - Processador RISC 32-bits Intel StrongArm 206Mhz;
  - 32 ou 64 MB RAM;
  - Capacidade de adição de pacotes de expansão.
- Com a "jaqueta" específica para PCMCIA, pode-se transformá-lo em uma estação *wireless*.

Ferramentas para Handhelds (1/3)

- **MiniStumbler:**
  - Versão em miniatura do NetStumbler
  - *Scanner* de redes *wireless*
  - Faz sondagem ativa para encontrar os APs
  - Coleta diversas informações importantes para auditoria

Ferramentas para Handhelds (2/3)

- **CENiffer:**
  - *Sniffer* capaz de executar com pouca quantidade de memória e recursos
  - Funciona em *cards ethernet wireless* e *wired*
  - Lista informações capturadas em camadas MAC, IP e TCP
  - Gera dumps em formato *Ethereal* e *tcpdump* para futuras análises

Ferramentas para Handhelds (3/3)

- **Net Force e vxUtil:**
  - Conjunto de ferramentas de rede equivalentes àquelas que fazem parte dos sistemas operacionais de PCs comuns:
    - Echo
    - WHOIS
    - Finger
    - Ping
    - Port scanner
    - DNS Lookup
    - Tracert

Pocket PC (6/6)

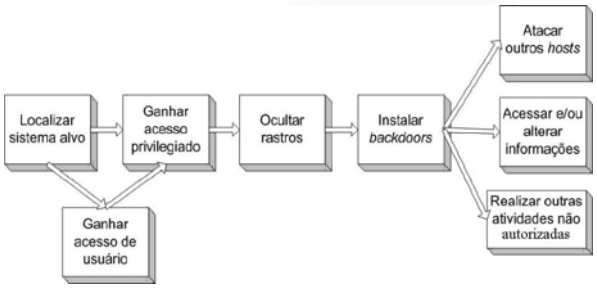
- IBM *wireless security auditor (WSA)*
  - Protótipo de um auditor de WLANs 802.11
  - Executa Linux em um PDA iPAQ
  - Auxilia administradores a eliminar vulnerabilidades
  - Verifica automaticamente configurações de segurança em redes

O ataque

- Componentes de um ataque:
  - Intrusos;
    - objetivos, *exploit scripts*;
  - Vítmas;
    - vulnerabilidades
- Bem sucedido (intrusão) X Mal sucedido;
- Diferentes tipos:
  - DoS;
  - *eavesdropping & espionage*;
  - *man-in-the-middle*;
  - dentre outros.

O ataque

- Um ataque típico:



Comprometimento do Sistema

- É caracterizado por um acesso não autorizado ao sistema;
- O comprometimento pode ser a nível de *root* dependendo do serviço acessado;
- Um sistema comprometido habilita o atacante a:
  - obter informações confidenciais;
  - alterar informações;
  - "grampear" recursos;
  - realizar atividades ilegais;
  - lançar ataques contra outros sites;

Técnicas de *hacking*

- Um ataque *hacker* é um procedimento que envolve vários passos;
- Diversas técnicas são combinadas para transpassar o computador/rede da vítima;
- Engenharia social:
  - Sondagem virtual;
  - Senha perdida;
  - Técnicos de *chat.*

Técnicas de *hacking*

- Espionagem social:
  - O atacante coleta informações críticas como senhas de sistemas, de bancos, etc. por meio da observação do ambiente e descuido da vítima.
- Coleta de lixo:
  - *Dumpster diving*
  - Provê ao *hacker* informações cruciais para a tomada de uma determinada rede
  - Senhas, memorandos, relatórios, disquetes, ...

Ataques específicos de redes wireless

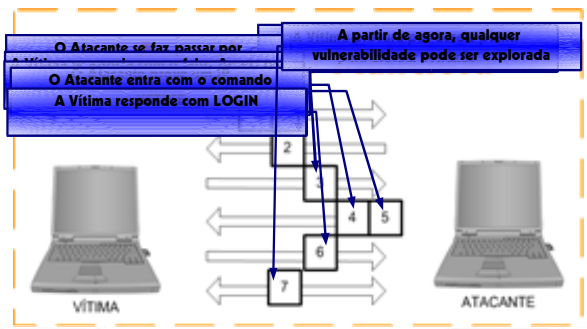
- *Eavesdropping & Espionage* (Prospecções)
  - Sondagem ativa vs. sondagem passiva.
- Associação maliciosa
- *Rogue access points*
- *War driving*
- *Warchalking*
- *Jamming* (embaralhamento de sinal)
- WEP *cracking*
- ARP *poisoning*
- MAC *spoofing*

Ataques específicos de redes wireless

- **Prospecções** em redes *wireless* são realizadas através de duas técnicas:
  - Sondagem Ativa;
  - Sondagem Passiva;
- Sondagem ativa: ocorre troca de informações entre o intruso e os dispostivos conectados à rede. Uma ferramenta muito conhecida para tal finalidade é o netstumbler (www.netstumbler.com)
- Sondagem passiva (RFMON): o intruso não envia informações para a rede. A ferramenta Kismet (http://www.kismetwireless.net) é muito ultilizada.

Ataques específicos de redes wireless

- **Associação maliciosa**



Ataques específicos de redes wireless

- ***Rogue access points:***
  - São aqueles conectados a uma rede sem permissão
  - Estende uma conexão *ethernet* para indivíduos dentro e fora da instituição vitimada
  - Ocorrem devido a falta de medidas básicas de segurança:
    - Criptografia;
    - SSID personalizado;
    - Filtragem de endereço MAC;

GTS 27/11/2003 130

Ataques específicos de redes wireless

- ***War driving***: termo surgiu da tática conhecida como *war dialing;*
- Criminosos dirigem pela cidade tentando localizar a presença física de uma rede *wireless*;
- Encontrando alguma rede, eles picham símbolos (warchalking) para demarcar que ali existe uma rede *wireless* ativa;
- Existem até sites com mapas de redes *wireless*, tais como:
  - http://www.wigle.net/gpsopen/gps/GPSDB/ (Chicago);
  - http://www.wifinder.com/

GTS 27/11/2003 131

Ataques específicos de redes wireless

- ***War driving***:
- ***Wireless Geographic Logging Engine***

http://www.wigle.net/gpsopen/gpsGPSDB (Chicago);

- Piada no dia 1° de abril: Fechado pelo Departamento de Justiça (01/04/2003);

GTS 27/11/2003 132

Ataques específicos de redes wireless

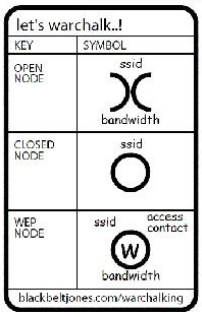
- ***Warchalking***: **ao encontrar as redes *wireless* através de war driving os atacantes picham símbolos para identificá-las;**

Símbolo pichado no chão, indicando a presença de uma WLAN grampeável: "Até uma criança consegue se conectar".

Warchalking: rede aberta sem mecanismo de autenticação, 2 Mbps, 802.11b SSID: tsunami

Ataques específicos de redes wireless

- ***Warchalking***: **Símbolos mais utilizados:**



Ataques específicos de redes wireless

- ***Jamming***: **Ataque de negativa de serviço (DoS)**
- **Ataques por negativa de serviço em redes *wireless* podem literalmente vir de qualquer direção;**
- **Simplesmente enviando grande quantidade de ruído na rede, um atacante pode efetuar esse tipo de ataque com sucesso;**
- **Entretanto, os criminosos eletrônicos tendem a se sofisticar cada vez mais.**

Ataques específicos de redes wireless

- **Como exemplo de DoS temos o seguinte tipo de ataque:**
  - **Com uma estação configurada como AP, ou seja, usando um SoftAP, o criminoso faz uma inundação de comandos persistentes de "desassociação";**
  - **Assim todas STAs são forçada a se desconectar da rede *wireless*;**
  - **Ou então o SoftAP pode ficar enviando os comandos a cada período de 10 segundos por exemplo, assim as STAs ficarão se conectando e desconectando da rede continuamente;**

Ataques específicos de redes wireless

- **WEP *cracking:***
  - **Quanto mais dados forem capturados, mais provável é o recebimento de um *frame* com um *byte* de chave.**
  - **5% a 13% de chance do acontecimento**
  - **Em média 5.000.000 de *frames***
  - **utiliza:**
    - ***Wireless sniffer***
      - ***AirSnort***
    - ***Wep Crack software***
      - ***WEPCrack***

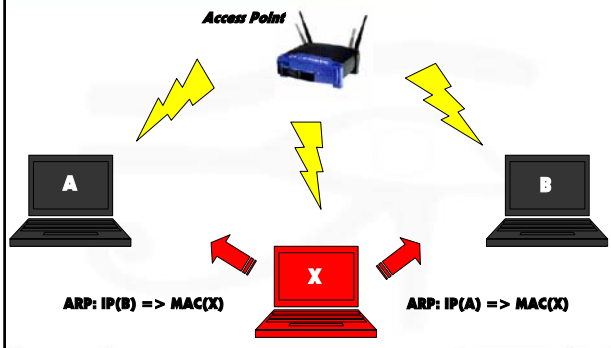
WEP Cracking na prática

1. **Capturar o sinal encriptado com WEP**
2. **Executar o *script* sobre o arquivo capturado**
3. **Ao encontrar um V.I. fraco, é criado um arquivo**
4. **É então executado outro *script* que tentará advinhar a chave WEP**
5. **É gerada uma saída decimal, a qual deve ser convertida para hexadecimal**
6. **Entre com a versão hexadecimal da chave no *Client Manager***

Ataques específicos de redes wireless

- **ARP *poisoning:***
  - Forja de pacotes ARP
  - O atacante precisa estar conectado ao mesmo dominio de *broadcast* das máquinas-alvo
  - Limitado a redes conectadas por *switches, hubs* e *bridges*
  - Aplicável a todos os *hosts* em um domínio de *broadcast*
  - A maioria dos *access points* "padrão" trabalham como um bridge transparente na camada MAC, permitindo que pacotes ARP sejam trocados entre a rede wilress e cabeada, e propagando o ataque para a rede guiada.

ARP Poisoning: Man-in-the-middle



Ataques específicos de redes wireless

- **MAC *Spoofing:***

Agenda

- Introdução às redes *wireless*
- Protocolo 802.11
- WEP
- Vulnerabilidades, ferramentas e ataques
- Segurança em redes *wireless*

Identificando Ataques

- Sondagem ativa: Esse tipo de atividade é identificada através das informações enviadas pelas ferramentas:
  - Wellenreiter: ESSID = "this_is_used_for_wellenreiter "
  - Netstumbler: string "All your 802.11b are belong to us"
  - Windows XP: string em hexadecimal:

```
0x14 0x09 0x03 0x11 0x04 0x11 0x09 0x0e
0x0d 0x0a 0x0e 0x19 0x02 0x17 0x19 0x02
0x14 0x1f 0x07 0x04 0x05 0x13 0x12 0x16
0x16 0x0a 0x01 0x0a 0x0e 0x1f 0x1c 0x12
```


Identificando Ataques

- MAC Spoofing
  - Endereço MAC fora do OUI (*Organizationally Unique Identifiers* - fornecido pelo IEEE);
  - Quebra do número de sequência;
- ARP Poisoning:
  - Tabela ARP com mais de um endereço IP apontando para um único endereço MAC;
  - Ferramenta Arpwatch (http://www-nrg.ee.lbl.gov).
- Man-in-the-middle (homem-no-meio)
  - Ataques de homem-no-meio geralmente utilizam as técnicas de MAC *spoofing* e ARP *poisoning* para serem efetuados. Identificando essas duas técnicas é possível evitar o ataque de homem-no-meio.

Identificando Ataques

- **DoS - Jamming**
  - ***Access point*** **faz enfileiramento (*queue*) dos pedidos de desautenticação / desassociação. Somente após um certo período de espera, a desautenticação ou desassociação é realizada.**
  - **Se durante o período de espera o *access point* receber algum pacote da estação que requisitou a desautenticação ou desassociação, estará identificado o ataque;**
  - **Também deve-se levar em consideração a quebra do número de sequência.**

Segurança em redes wireless

- **Identificação de *rogue access points* e vulnerabilidades;**
- **Configurando *access points;***
- **Política de segurança levando em consideração a rede *wireless;***
- **Medidas de proteções adicionais.**

Segurança em redes wireless

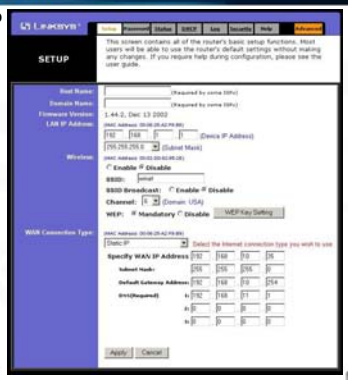
- **Descobrindo *access points* grampeáveis e vulnerabilidades**
  - **A descoberta de *access points* ilegais dentro da rede pode ser feita de duas maneiras:**
    - **Fisicamente, caminhando pela área que contém a rede com prospectores de redes *wireless*;**
    - **Monitorando a rede com sensores remotos desenvolvidos especifiamente para este tipo de serviço. Eles monitoram toda RF das WLANs.**

Segurança em redes wireless

- **Identificados os *access points* vulneráveis, deve-se:**
  - **Modificar os SSIDs padrões;**
  - **Configurar o *access point* para não fazer *broadcasts* constantes do SSID;**
  - **Fazer Filtragem por MAC no *access point*;**
  - **Utilizar criptografia WEP;**
  - **Não permitir conexões em baixa velocidade (opcional).**

Segurança em redes wireless: AP config

- **SETUP**

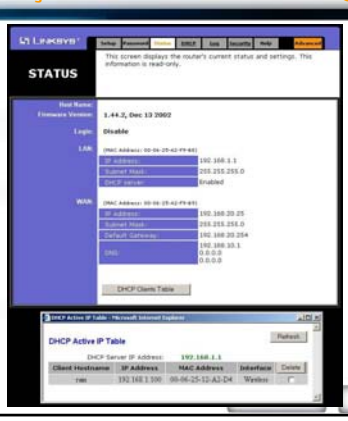


Segurança em redes wireless: AP config

- **PASSWORD**

Segurança em redes wireless: AP config

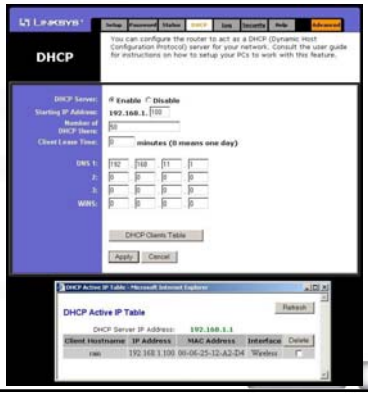
- **STATUS**



GTS 151

Segurança em redes wireless: AP config

- **DHCP**



GTS 152

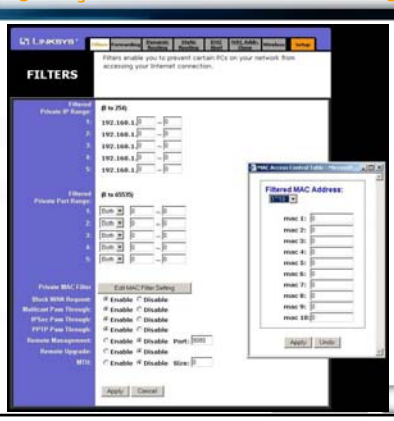
Segurança em redes wireless: AP config

- **LOG**

153

Segurança em redes wireless: AP config

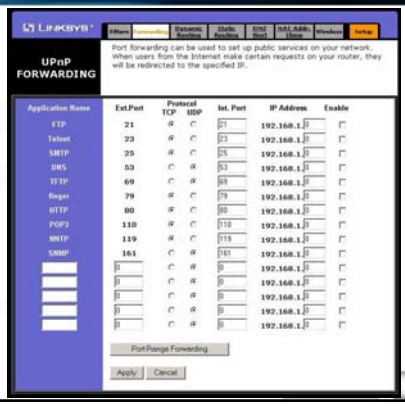
- **Advanced: FILTERS**



GTS 154

Segurança em redes wireless: AP config

- **Advanced: FOWARDING**



GTS 155

Segurança em redes wireless: AP config

- **Advanced: DYNAMIC ROUTING**

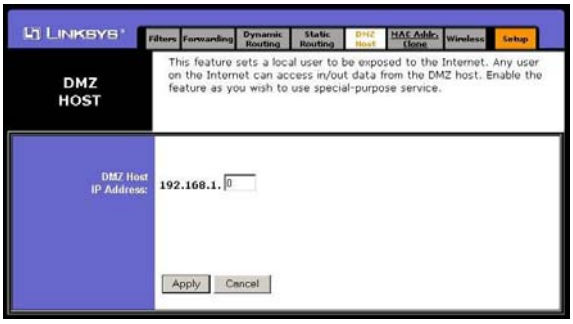
GTS 156

Segurança em redes wireless: AP config

- **Advanced: STATIC ROUTING**

Segurança em redes wireless: AP config

- **Advanced: DMZ HOST**



Segurança em redes wireless: AP config

- **Advanced: MAC Address CLONE**

Segurança em redes wireless: AP config

- **Advanced: WIRELESS**

Segurança em redes wireless

- **Além da configuração correta dos *access points* é recomendável a utilização de:**
- **Criptografia e autenticação – VPN**
  - **A criptografia do padrão 802.11b, WEP, é fraca. Softwares como WEPCrack podem facilmente quebrar essa criptografia.**
  - **Portanto, a utilização de VPN e extremamente recomendável.**
  - **O uso de servidores RADIUS para autenticação também é recomendável.**

Segurança em redes wireless

- **Fazer e reforçar as políticas levando em consideração a rede *wireless*:**
  - **Não permitir uso não autorizado de *access points*;**
  - **Não permitir a má configuração de componentes *wireless* como *Ad Hoc*;**
  - **Não permitir accesso em baixas velocidades.**
  - **Etc...**

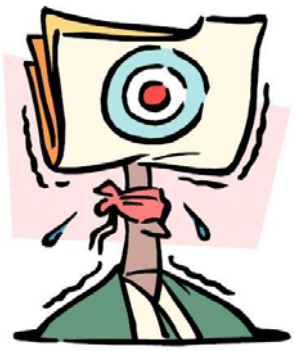
Segurança em redes wireless

- **Intrusion Detection & Proteção**
  - Implementação de mecanismos que conseguem detectar tentativas de conexões não autorizadas em redes *wireless*;
  - As formas mais conhecidas de ataque a redes *wireless* começam com pacotes de probe e escuta das RF para descoberta de SSIDs;
  - Desta maneira, identificar e combater estas ferramentas de escaneamento faz com que o número de potenciais ataques caia significadamente;
  - Detecção de intrusão também na rede cabeada. O comportamento anômalo identificado pelo IDS pode ser proveniente de uma ataque à rede *wireless*.

Conclusão

- A nova tecnologia de rede sem fio, por ser ainda muito recente, contém ainda muitas vulnerabilidades e riscos na sua implementação.
- Apesar disso, uma implementação segura já é viável.
- Poucas ferramentas são capazes de analisar o tráfego da camada 2 do 802.11.
- Apesar de ser possível detectar os scanners de redes wireless, prover detectores de intrusão para esta rede ainda é uma difícil tarefa.

Perguntas?



Thanks!

andre@acmesecurity.org
(Key id: 0x00940DC6)
www.acmesecurity.org/~andre

lod@acmesecurity.org
(Key id: 0x4CF4CB68)
www.acmesecurity.org/~lod

sacchet@acmesecurity.org
(Key id: 0x3264E801)
www.acmesecurity.org/~sacchet

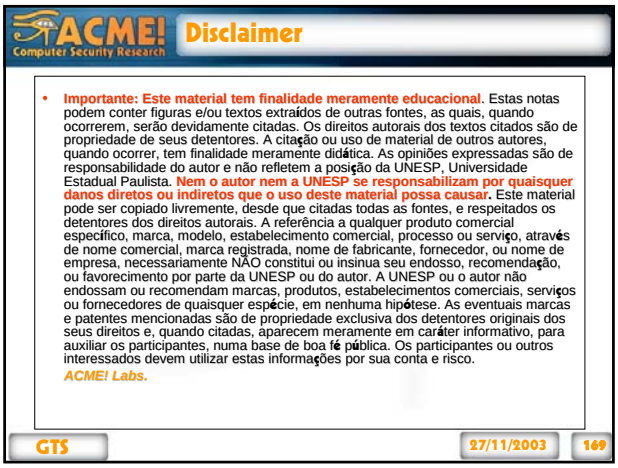
Referências

- http://www.acmesecurity.org
- https://forum.acmesecurity.org

- http://www.pluton.com.br
- http://home.jwu.edu/jwright/papers.htm
- http://www.cs.umd.edu/~waa
- http://www.airdefense.net
- http://www.kismetwireless.net
- http://www.ethereal.com
- http://www.netstumbler.com
- http://www.airsnort.shmoo.com
- http://hostap.epitest.fi

Refêrencias

- http://www.elva-1.spb.ru/pdf/d/22.pdf
- http://www.wardriving.com/
- http://www.warchalking.org/index.html
- http://www.oreillynet.com/cs/weblog/view/wlg/448
- http://verma.sfsu.edu/users/wireless/pringles.php
- http://www.netscum.com/~clapp/wireless.html


ACME!
Computer Security Research
Disclaimer
• Importante: Este material tem finalidade meramente educacional. Estas notas podem conter figuras e/ou textos extraídos de outras fontes, as quais, quando ocorrerem, serão devidamente citadas. Os direitos autorais dos textos citados são de propriedade de seus detentores. A citação ou uso de material de outros autores, quando ocorrer, tem finalidade meramente didática. As opiniões expressadas são de responsabilidade do autor e não refletem a posição da UNESP, Universidade Estadual Paulista. Nem o autor nem a UNESP se responsabilizam por quaisquer danos diretos ou indiretos que o uso deste material possa causar. Este material pode ser copiado livremente, desde que citadas todas as fontes, e respeitados os detentores dos direitos autorais. A referência a qualquer produto comercial específico, marca, modelo, estabelecimento comercial, processo ou serviço, através de nome comercial, marca registrada, nome de fabricante, fornecedor, ou nome de empresa, necessariamente NÃO constitui ou insinua seu endosso, recomendação, ou favorecimento por parte da UNESP ou do autor. A UNESP ou o autor não endossam ou recomendam marcas, produtos, estabelecimentos comerciais, serviços ou fornecedores de quaisquer espécie, em nenhuma hipótese. As eventuais marcas e patentes mencionadas são de propriedade exclusiva dos detentores originais dos seus direitos e, quando citadas, aparecem meramente em caráter informativo, para auxiliar os participantes, numa base de boa fé pública. Os participantes ou outros interessados devem utilizar estas informações por sua conta e risco.
ACME! Labs.
GTS
27/11/2003
169