Segurança em redes sem fio

Nelson Murilo
<nelson@pangeia.com.br>

Segurança em redes sem fio

- Perfil
- Conceitos iniciais
- Tipos
  - Freqüências
  - Características
  - Padrões atuais
- Problemas
- Defesa

pangeia

Segurança em redes sem fio

Perfil

- **Atuação na área de segurança desde 1992**
- **Testes de intrusão** (Bancos, órgãos militares, governo, instituições financeiras, comp. aéreas, etc.)
- **Administrador do Centro de Resposta à Incidentes do Departamento de Polícia Federal**
- **Investigação forence computacional**
- **Projetos e implantação de políticas de segurança, em órgãos do governo, de inteligência e militares**
- **Monitoramento de *sites* em tempo real**
- **Desenvolvimento de ferramentas de segurança**
- **Colaborador do Grupo de Segurança do Comitê Gestor/BR**
- **Autor do livro "Segurança Nacional –** Técnicas e ferramentas de ataque e defesa de rede de computadores"

pangeia

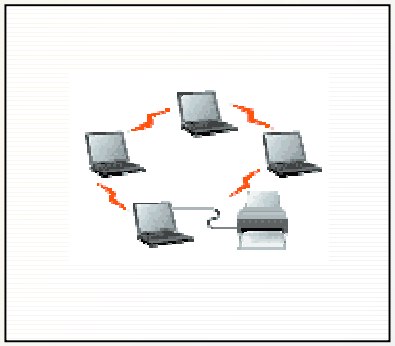
Segurança em redes sem fio

Conceitos

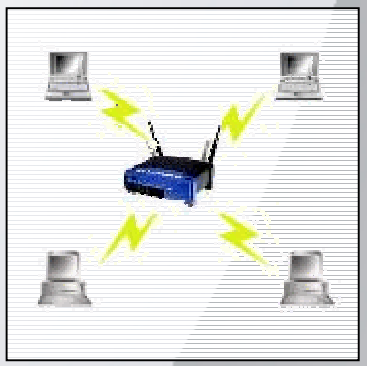
- Uso de freqüências ISM [1] (900mhz/2.4Ghz/5Ghz)
  - Freqüências também usadas por celulares, telefones sem fio, bluetooth, etc.

- Dois modos de operação

GRUPOS



INFRAESTRUTURA



[1] Industrial Scientific and Medical

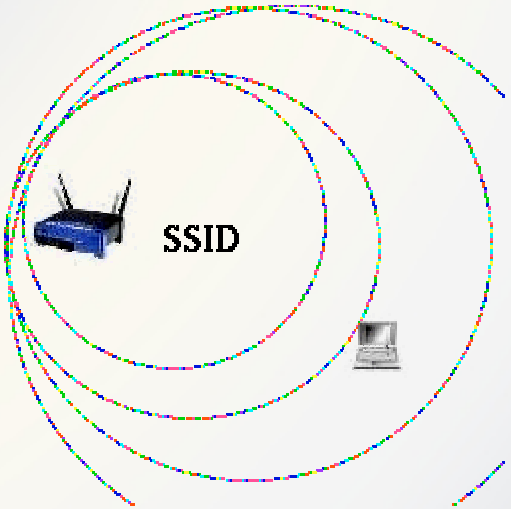
pangeia

Segurança em redes sem fio

Conceitos

- Métodos de busca

PASSIVA



ATIVA

pangeia

Segurança em redes sem fio

Tipos

- **IEEE 802.11**
  - Freqüências de 900, 2.4 e 5Ghz
- **802.11b** (padrão atual)
  - 2.4Ghz
  - Máximo de 22Mbs
  - Freqüência compatilhada
- **802.11g**
  - 2.4Ghz
  - Máximo de 54Mbs (72 em modo turbo)
  - Freqüência compartilhada
- **801.11.a**
  - 5Ghz
  - Máximo de 54mbs (108 em modo turbo)
  - Limitações de uso em alguns países
  - Menor área de abrangência

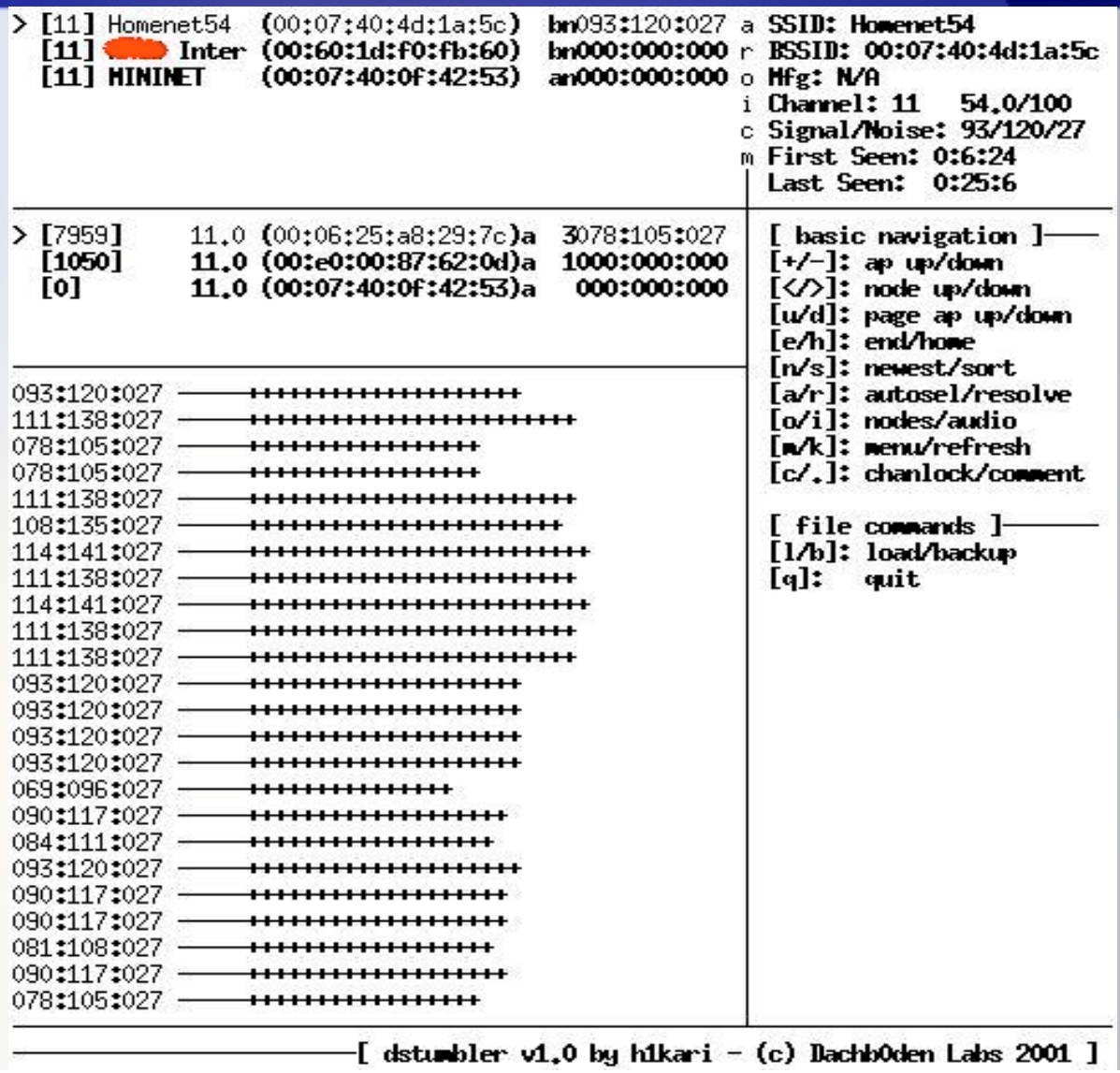
Segurança em redes sem fio

Ameaças

- Negação de serviço e jamming
- Análise do ambiente
- Captura de tráfego
- Monkey in  the middle
- Acesso não autorizado

Segurança em redes sem fio

Análise do ambiente



Segurança em redes sem fio

Análise do ambiente

- SNMP (.iso.member-body.us.ieee802dot11)
  - dot11StatiotionID
  - dot11WEPDefaultKeyValue (somente leitura(?))
  - dot11ManufacturerID
  - ...

Segurança em redes sem fio

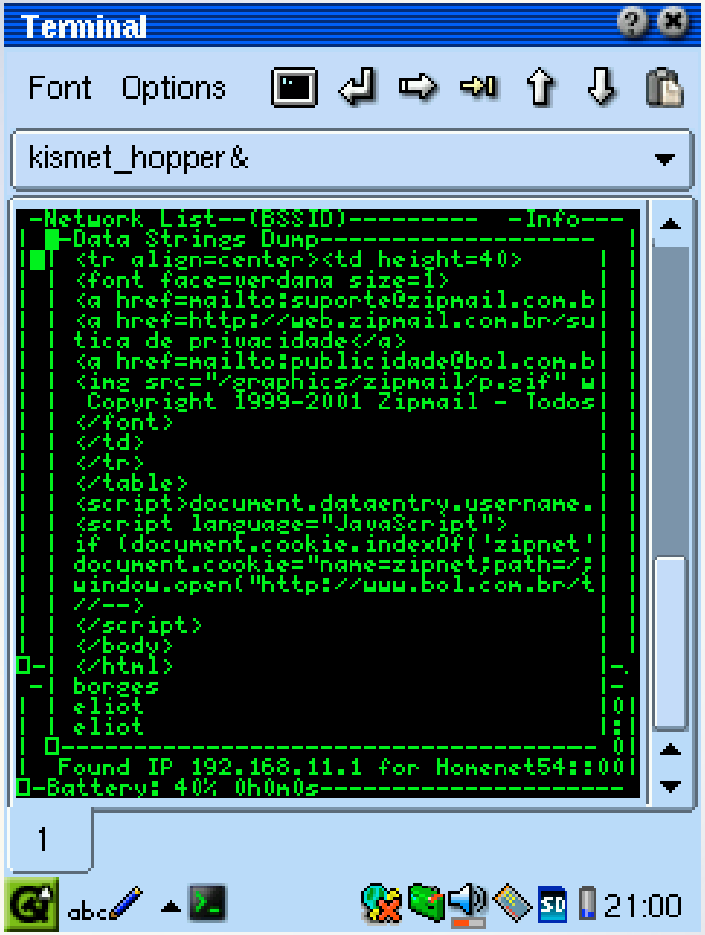
Negação de serviço

- 2.4Ghz é usado também por celular, telefones sem fio, bluetooth, cameras de vigilância e até por babás eletrônicas e forno de micro ondas.
- Não existem (ainda) outros aparelhos de baixo custo usando 5Ghz, mas os próprios equipamentos (antenas, placas, etc) podem ser modificados para gerar ruído.

Segurança em redes sem fio

Captura de tráfego

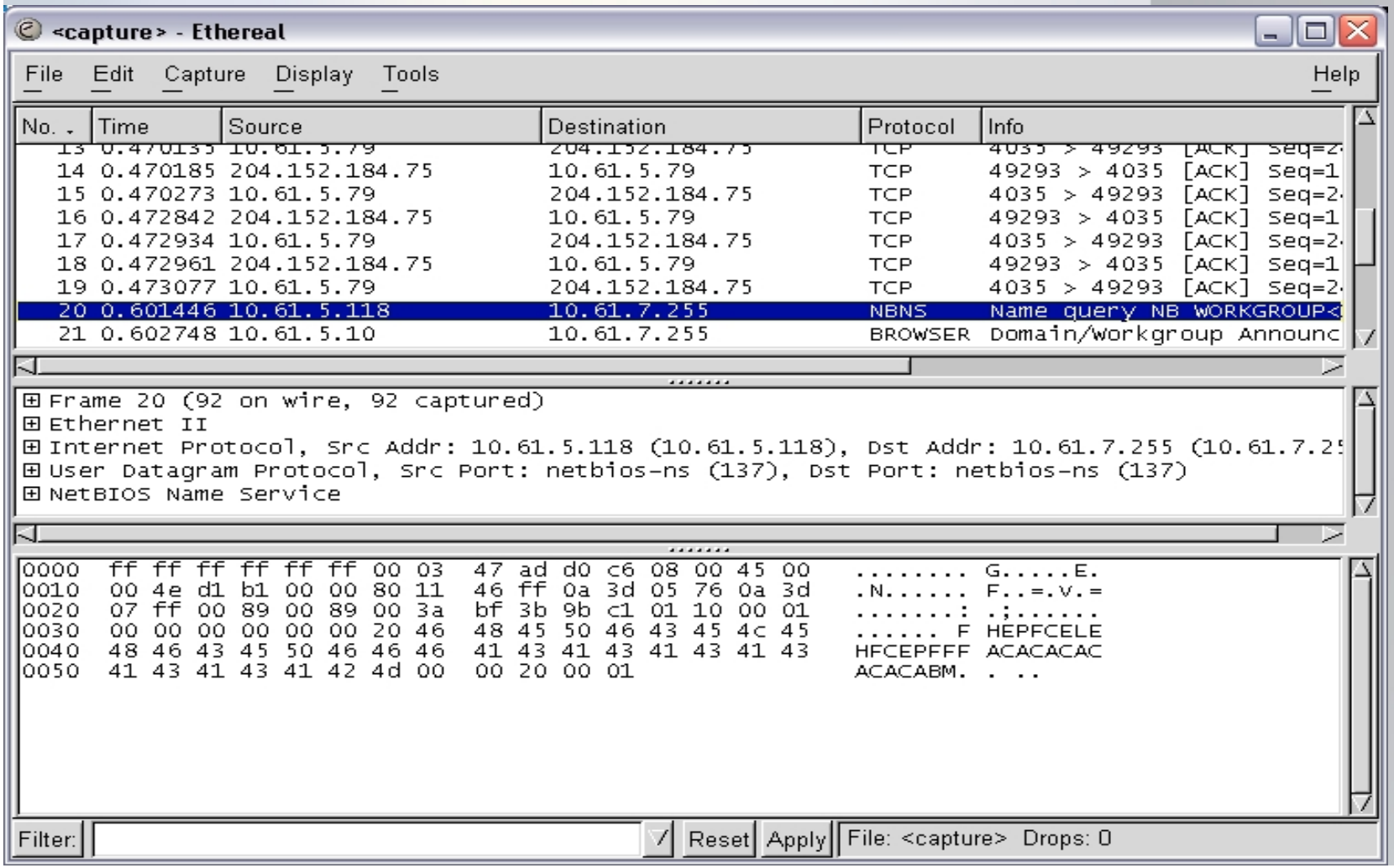
É possível a captura de tráfego mesmo não fazendo parte da rede



Segurança em redes sem fio

Captura de tráfego

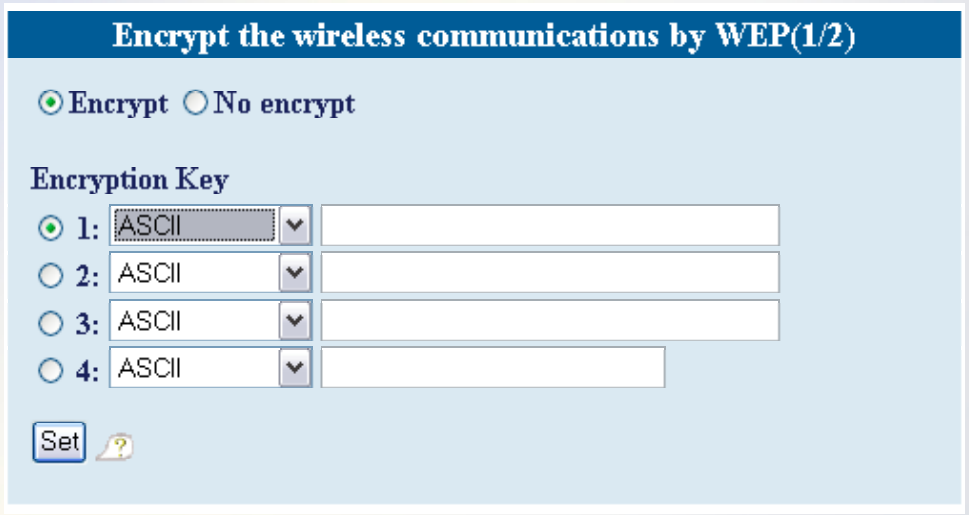
Dentro da rede a captura pode ser feita com ferramentas tradicionais



Segurança em redes sem fio

Captura de tráfego

O uso de chaves pré-configuradas facilita a quebra do tráfego criptografado



pangeia

Segurança em redes sem fio

Monkey in the middle

- Redes sem fio são mais suceptíveis a este tipo de ataque
- Muitas soluções de segurança confiam nas camadas mais baixas
- Muitas soluções de VPN são inadequadas para redes sem fio

pangeia

Segurança em redes sem fio

Monkey in the middle – cenário comum

1) Vítima procura por um concentrador qualquer

2) Vítima se associa ao falso concentrador do atacante
   - Falso concentrador pode ou não usar um canal diferente do real
   - Falso concentrador duplica o endereço MAC e ESSID do real

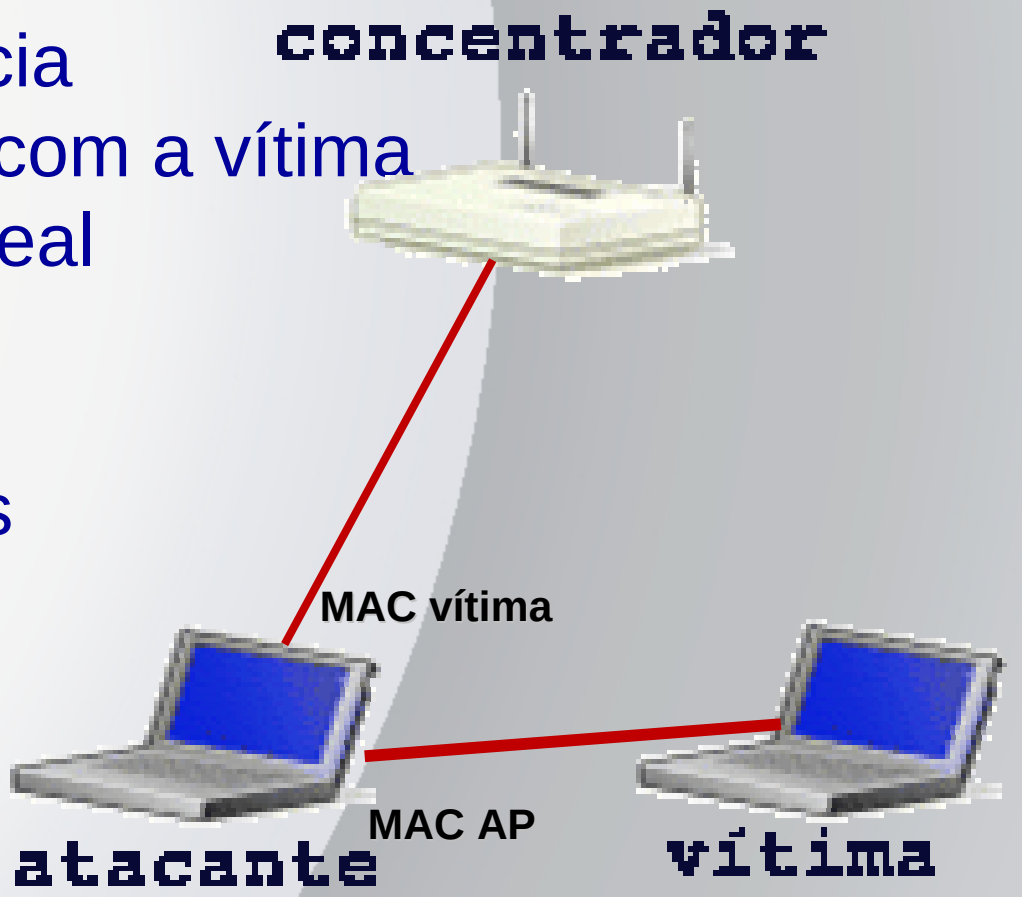
pangeia

Segurança em redes sem fio

Monkey in the middle – cenário IPSec

1) Falso concentrador inicia negociação de chaves com a vítima e com o concentrador real

2) Dois túneis são criados



pangeia

Segurança em redes sem fio

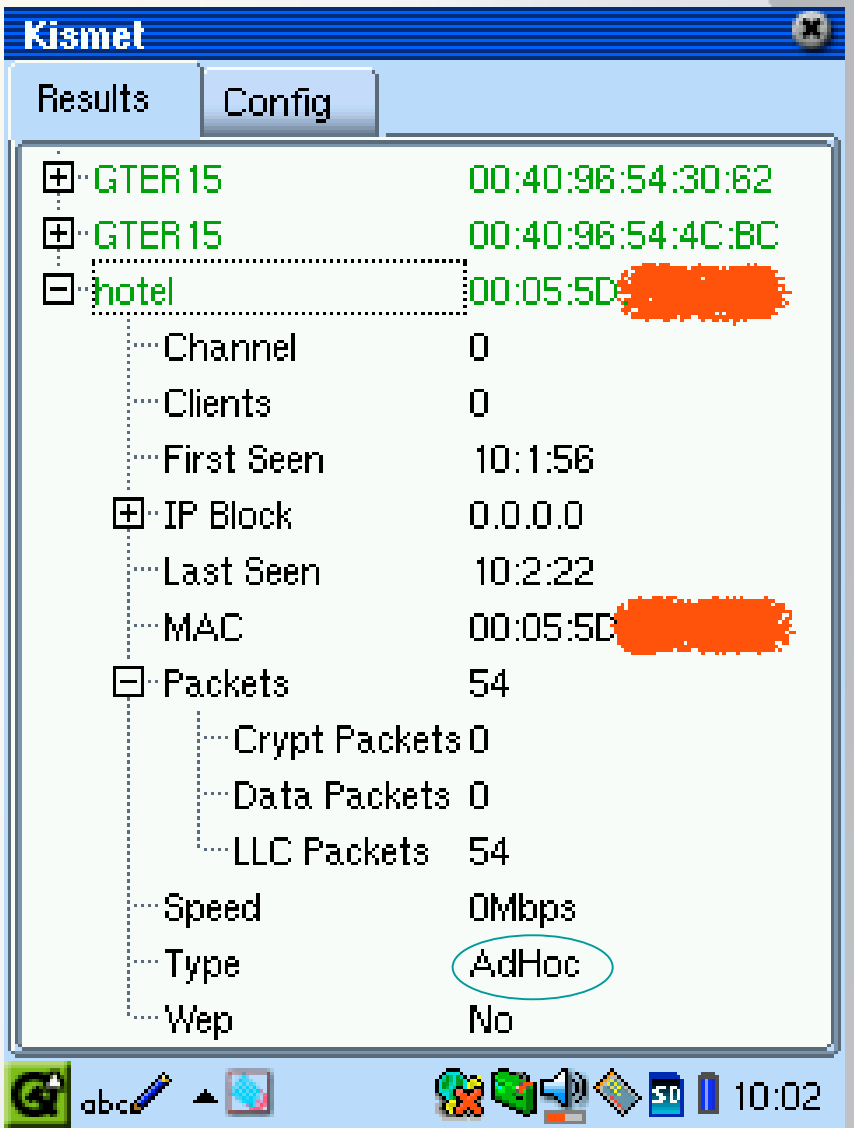
Acesso não autorizado

- **Servidores**
- **Clientes**
- **Roteadores**
- **Concentradores**

Segurança em redes sem fio

Acesso não autorizado

Clientes



pangeia

Segurança em redes sem fio

Acesso não autorizado

Acesso ao concentrador

- Configuração padrão (incluindo senhas)
- Gerenciamento sem uso de criptografia
  - HTTP
  - Telnet
  - SNMP

Segurança em redes sem fio

Defesa

Acesso ao concentrador

- Mudança das configurações padrão
  - Senhas, chaves wep, SSID e canal
- Gerenciamento com criptografia
  - SSH (Primeira troca de chaves segura)
- Gerenciamento sem criptografia via LAN
- Configurar concentrador como ponte

pangeia

Segurança em redes sem fio

Defesa

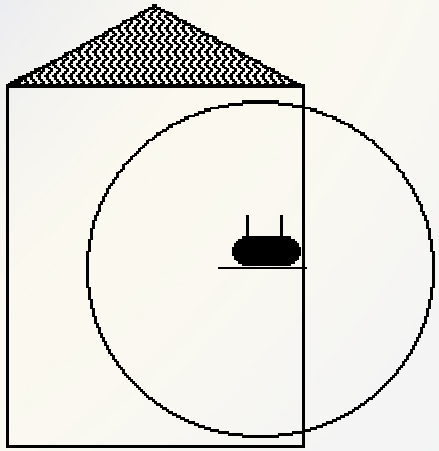
- Concentrador (AP)
  - Desabilitar propagação da identificação da rede
  - Não usar nomes que identifiquem a empresa
  - Não usar padrões de fábrica (ID, WEP, etc)
  - Usar WEP
  - Restringir MAC quando possível
  - Segurança física (posição e potência do concentrador)
  - VPN com autenticação mútua quando possível (PKI)
- Cliente
  - Desabilitar modo AD HOC
  - Desligar o retirar a placa após o uso

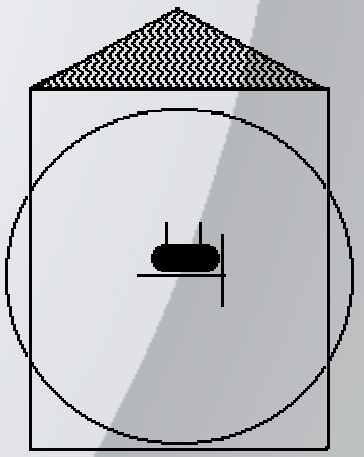
pangeia

Segurança em redes sem fio

Segurança física

Posição do concentrador influencia no desempenho e na segurança





Segurança em redes sem fio

Segurança física

Propagação em ambiente aberto

802.11a	~240mt
802.11b	~320Mt
80211g	~500mt

Segurança em redes sem fio

Freqüências

Canal	Freq
1	**2.412**
2	**2.417**
3	**2.422**
4	**2.427**
5	**2.432**
6	**2.437**
7	**2.442**
8	**2.447**
9	**2.452**
10	**2.457**
11	**2.462**
12	**2.467**
13	**2.472**
14	**2.484**

Segurança em redes sem fio

Considerações finais

E possível ter redes sem fio seguras utilizando camadas de segurança, e principalmente, utilizando VPN com autenticação mútua.

Grande expectativa pelo fechamento do 802.11i (enfase em autenticação e extensão de mobilidade)

Segurança em redes sem fio

Nelson Murilo
<nelson@pangeia.com.br>