Wireless – Redes sem fio

Aspectos de segurança
em
redes sem fio.

Rafael Lachi

LSI – USP - 04/2003

"Study Exposes WLAN Security Risks"

"...The study found that of 328 wireless access points detected in downtown London, nearly two-thirds did not have WEP (Wired Equivalent Privacy) encryption turned on. Also, 100 of the APs were sending out signals identifying the organizations that owned them, and 208 were installed using the default configuration..."

Fonte: http://www.eweek.com/article2/0,3959,926129,0

Tópicos

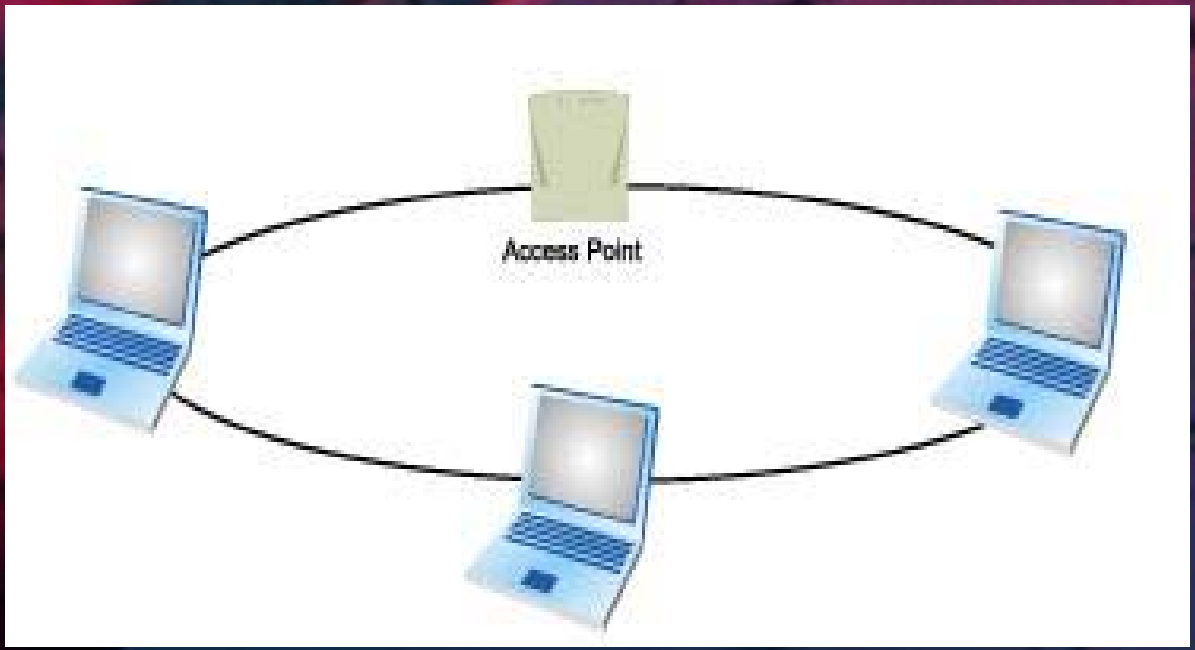
- Definições, nomenclaturas e anagramas
- Segurança
- WEP
- WarDriving & WarChallking
- WEPHacking
- EAP
- Futuro
- Conclusão

Definições

- Redes sem fio
- 802.11
- Padrões de mercado (a, b e g).
- BSS
- ESS
- IBSS – Ad-hoc

BSS

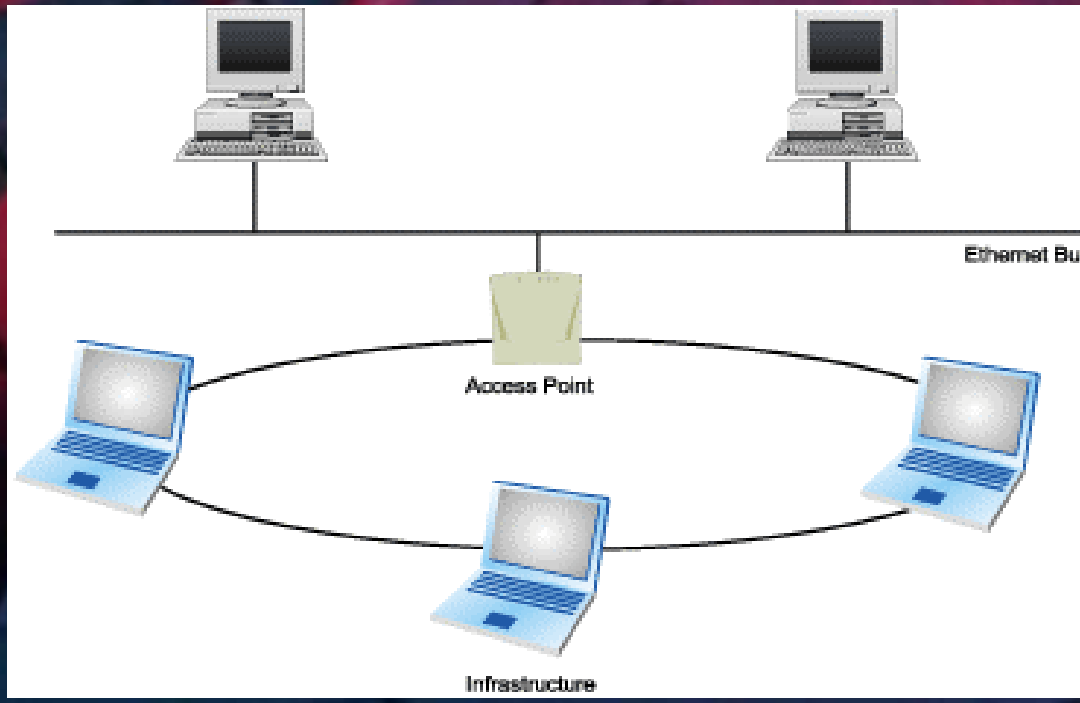
- Uma BSS é basicamente composta das estações clientes e do ponto de acesso.



Fonte: www.bromax.com.tw/faq.htm

ESS

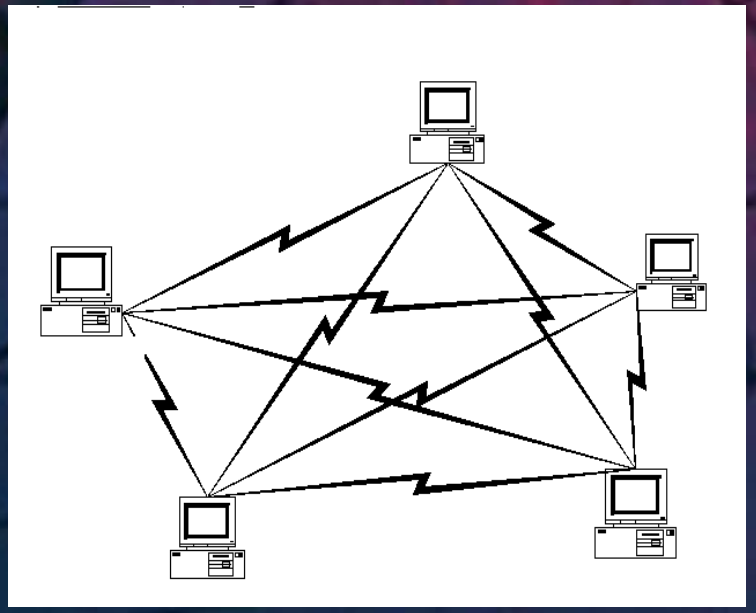
- Uma ESS possui os mesmos elementos da BSS e mais uma rede local Ethernet.



Fonte: www.bromax.com.tw/faq.htm

IBSS – Ad-hoc

- Nesta modalidade de rede não há a figura do ponto de acesso.
- As estações têm que se comunicar diretamente umas com as outras.



Fonte: www.turnpoint.net/wireless/ presentation/4.htm

Segurança

- Aspectos comuns de segurança em redes convencionais e redes sem fio.
- Meios de acesso
  - Interface aérea x Cabos de rede.

Aspectos de segurança

- Autenticação.
- Confidencialidade.
- Integridade.
- Segurança nas redes sem fio
  - WEP – Wired Equivalent Privacy

WEP

- Wired Equivalent Privacy
- Falhas
  - Confidencialidade. RC4 – 24 bits IV + 40 bits WEP Key. Chave de criptografia 64 bits.
  - Integridade. Projeto pobre compromete a integridade. Para isso faz-se uso do CRC.
  - Autenticação. Utiliza o endereço da placa de rede (MAC Address) e não o usuário para autenticação.

WEP

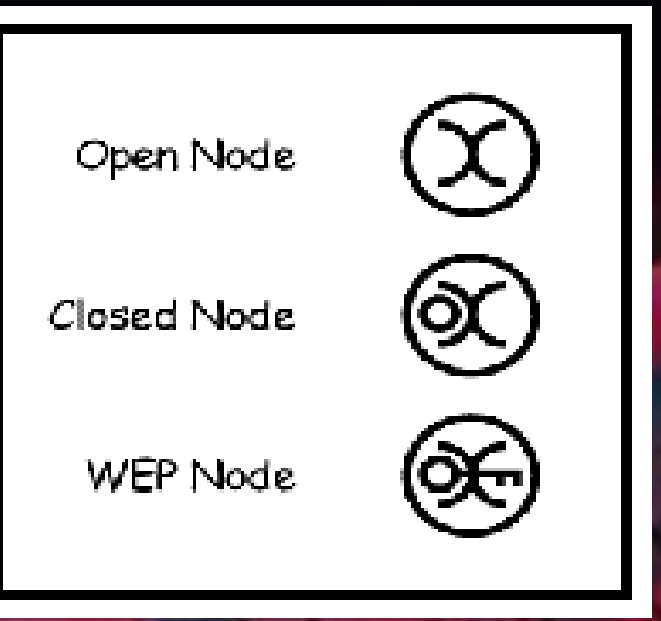
- Chave de encriptação. (WEP Key)
- Tamanhos suportados 64,128 e 256* bits.
- Vetor de inicialização (IV) 4 bytes de texto sem criptografia no cabecalho dos quadros.
- Cifra-RC4 (RC4-Cypher) IV+Wep Key.

WarDriving

- Método de busca por redes sem fio que podem ser acessadas da rua.
- Pode ser realizado com uma simples lata de “pringles”.

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

WarChalking



te: http://www.ci.ru/inform15_02/ris1a_el.gif

Fonte: http://www.ocf.berkeley.edu/~cfarivar/warchalking/rachel_warchal

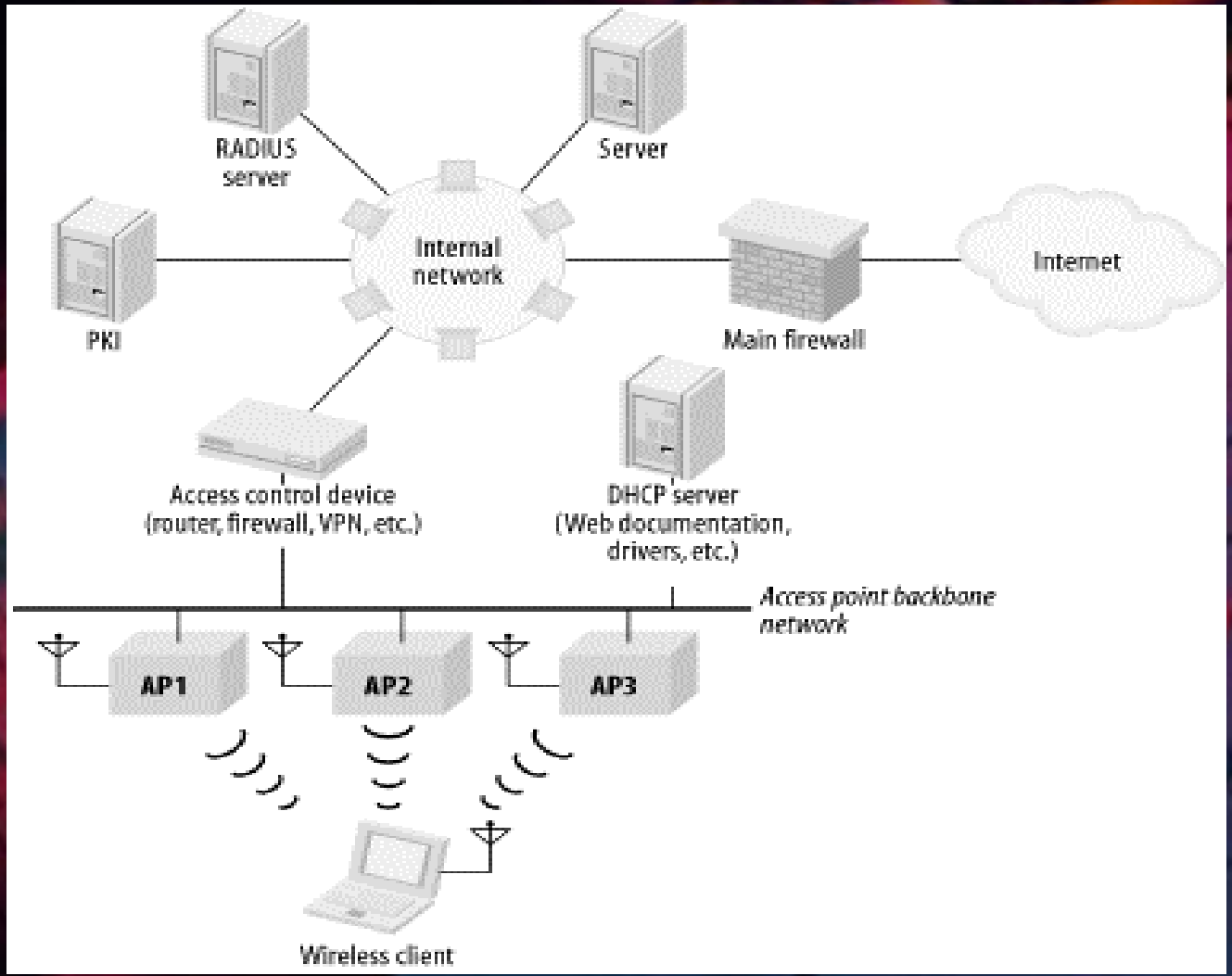
WEP-Hacking

- Relacão entre tamanho da chave e a quantidade de chaves fracas gerados pelo WEP.
  - Quanto maior o tamanho da chave, maior é a quantidade e a proporcão das chaves fracas.
- Relacão entre a taxa de utilização da rede e o tempo necessário para o Hacking do WEP ocorrer.
  - Com um taxa de 30% de utilização, o hacker leva aproximadamente 12 horas para coletar pacotes suficientes para quebrar a segurança do WEP.

EAP 802.1x

- Extensible Authentication Protocol
- EAPOL (EAP over LAN)
  - Suplicante.
  - Autenticador.
    - RADIUS (EAP over RADIUS).
  - Servidor de autenticação.

Topologia segura



Fonte: 802.11 Wireless networks – O'REILLY

Futuro da segurança nas redes sem fio

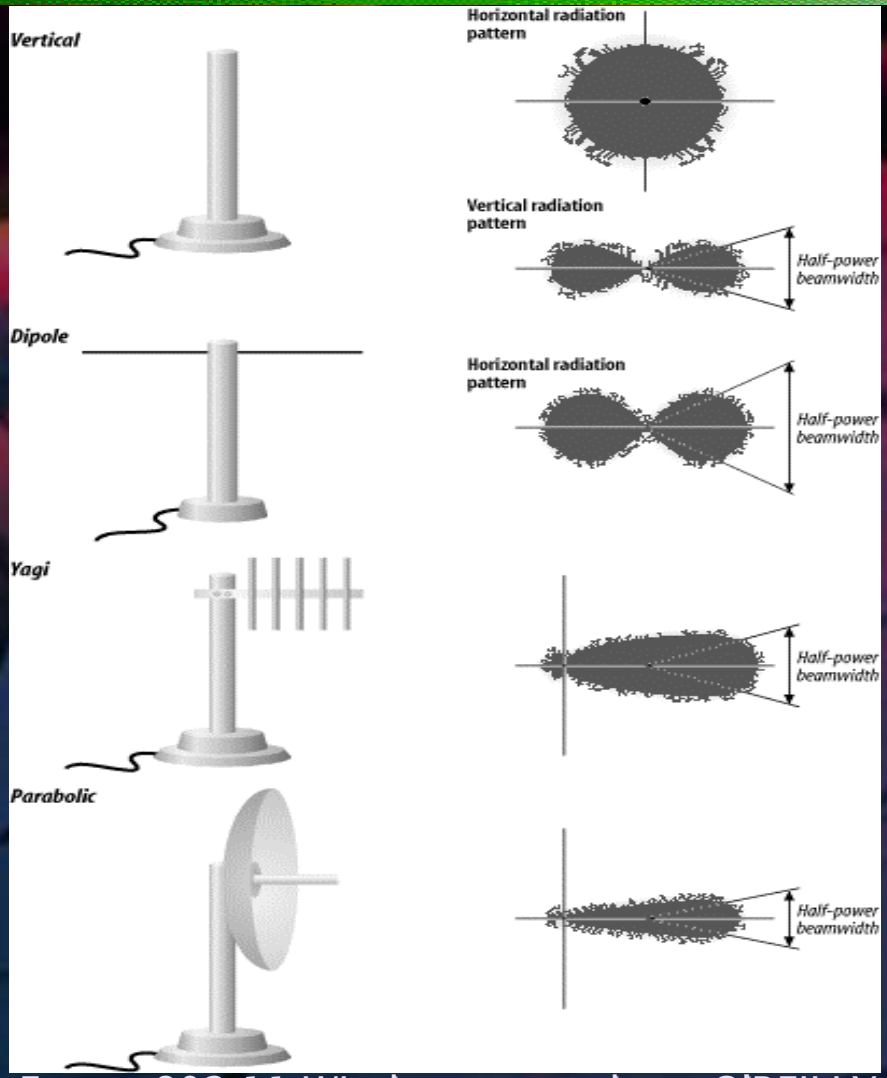
- 802.11e – Padrão de redes sem fio que tem compromisso com a segurança.
- 802.1x – Controle de acessos por porta.

Conclusão

- As redes wireless têm uma insegurança inerente que pode ser contornada através do planejamento adequado da arquitetura da rede, e drasticamente minimizada através de ferramentas de segurança já utilizadas nas redes convencionais como firewalls, Servidores RADIUS etc.

Apêndice A – Antenas

Exemplos dos tipos de polarização de ondas obtidas pelos diferentes tipos de antenas.



Fonte: 802.11 Wireless networks – O'REILLY

Obrigado

Contatos

- Rafael Lachi, rafael_lachi@hotmail.com
- Marcelo K. Zuffo, mkzuffo@lsi.usp.br
- Hilton Fernandes, hgfernan@lsi.usp.br