Uma Visão sobre a (in) Segurança das Redes Sem Fio na Cidade de São Paulo

Adriano Mauro Cansian, André Ricardo Abed Grégio, Carina Tebar Palhares
{adriano,andre, carina}@acmesecurity.org
UNESP - Universidade Estadual Paulista

Aleck Zander Tomé de Souza
aleck@lac.inpe.br
Instituto Nacional de Pesquisas Espaciais – INPE/ MCT
Antônio Montes Filho
antonio.montes@cenpra.gov.br
Centro de Pesquisas Renato Archer – CenPRA/ MCT

GTS 02.04 Outubro 2004

Roteiro

- Introdução
- Recursos utilizados
- Procedimentos
- Dados obtidos
- Conclusões

Introdução

- Desenvolvimento da tecnologia *wireless* -> uso crescente de dispositivos sem fio.
- Meio físico -> alvo fácil para ataques de escuta.
- Configuração inadequada dos dispositivos de redes sem fio.
- Situação dos sistemas *wireless* em áreas estratégicas.

Recursos Utilizados - Hardware

- Notebook Toshiba P4 1.8Ghz 256Mb RAM
- PCMCIA Dell TrueMobile 1150 802.11b (Chipset Orinoco) com conector MC para antena externa
- Antena externa com base magnética
  - Altura: 22 cm
  - 1.50 m de cabo coaxial RG174, com conector MC
  - Impedância: 50 ohms
  - Freqüência nominal de operação: 2400 a 2483 MHz
  - Potência máxima: 50 Watts
  - Ganho antes da atenuação do cabo: 5.5 dBi
- GPS Garmin Etrex Vista

Recursos Utilizados - Software

- Linux Slackware 9.1 (http://www.slackware.com/)
- Orinoco Monitor Mode Patch http://airsnort.shmoo.com/orinocoinfo.html
- Kismet (http://www.kismetwireless.net/)
- GPSd (http://pygps.org/gpsd/)
- GPS TrackMaker (http://www.gpstm.com/)

Procedimentos

- Sondagem Passiva: modo monitor
  - Não há conexão entre dispositivo de monitoramento e redes sem fio analisadas.
- 4 leituras entre 25/02 e 08/03/2004
  - Período: entre 14:00 e 15:30 (GMT-03)
  - Duração média: 1h22m
  - Percurso por leitura: 30.47 Km
- Leitura apenas de informações de difusão pública.

Informações utilizadas para os Mapas

- Contagem dos BSSID únicos do arquivo Kismet.xml
  - BSSID
  - WEP
  - Latitude, longitude
  - Timestamp
- Criação do caminho trafegado a partir do arquivo Kismet.gps
  - Latitude, longitude
  - Altitude
  - Timestamp

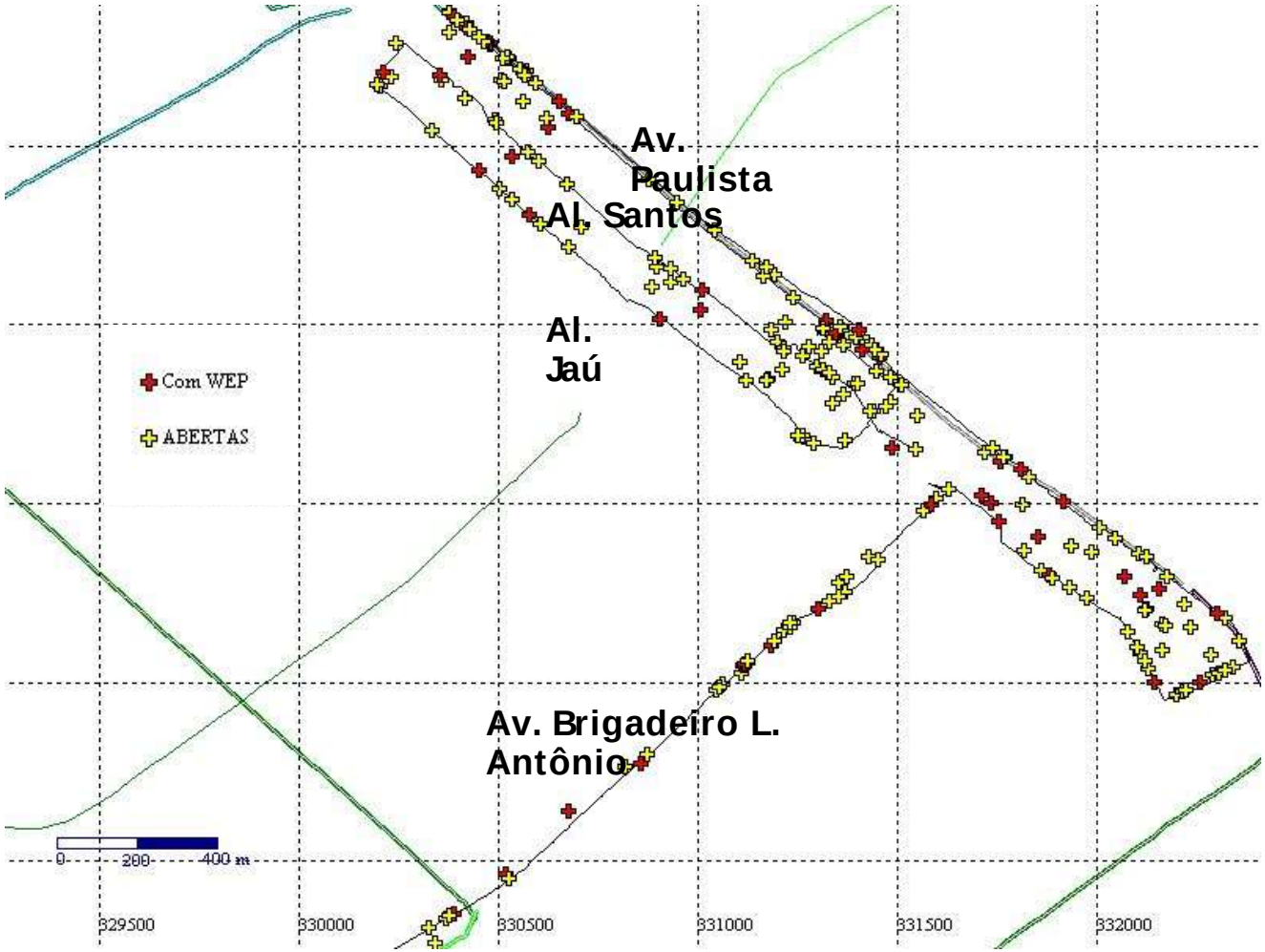
Resultados

Região	Redes com *WEP*		Redes sem *WEP*		TOTAL	
	Quant.	%	Quant.	%	Quant.	%
Av. Paulista e imediações:	26	8	89	28	115	36
Av. Berrini e imediações:	56	17	74	24	130	41
Eixo Juscelino / Brigadeiro:	22	7	49	16	71	23
TOTAL:	104	32	212	68	316	100

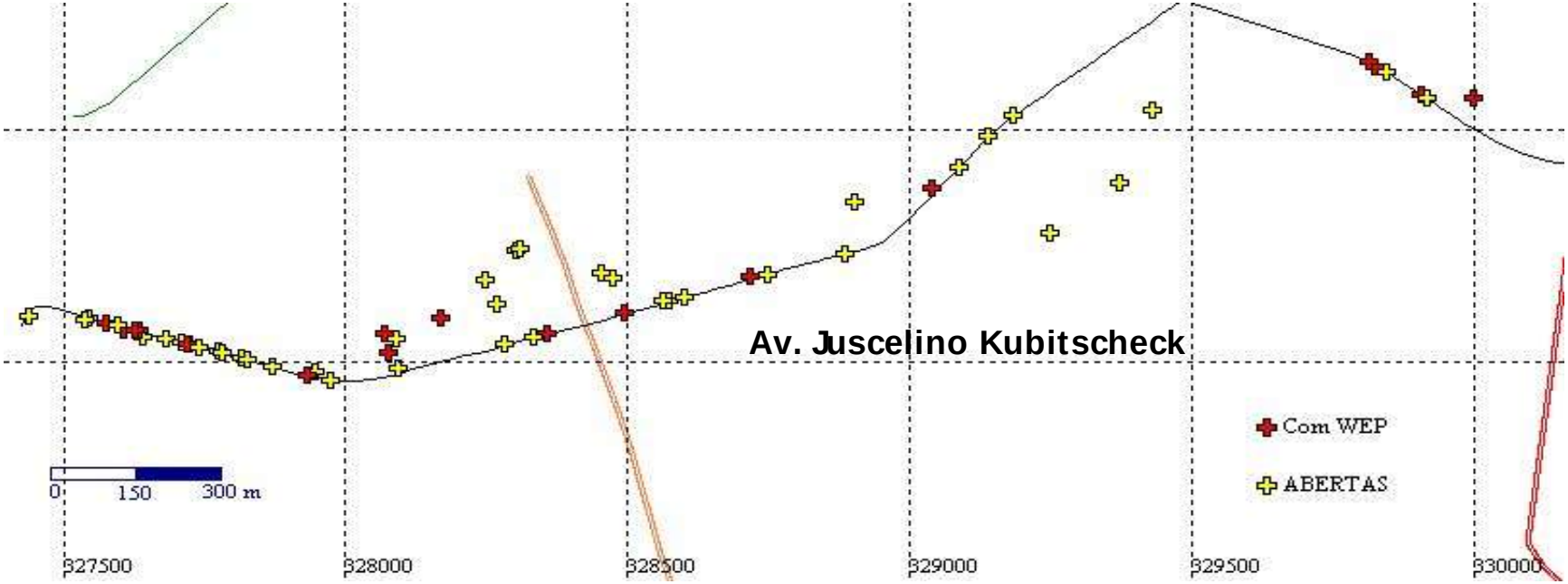
ACME! Computer Security Research

Visão geral das regiões pesquisadas

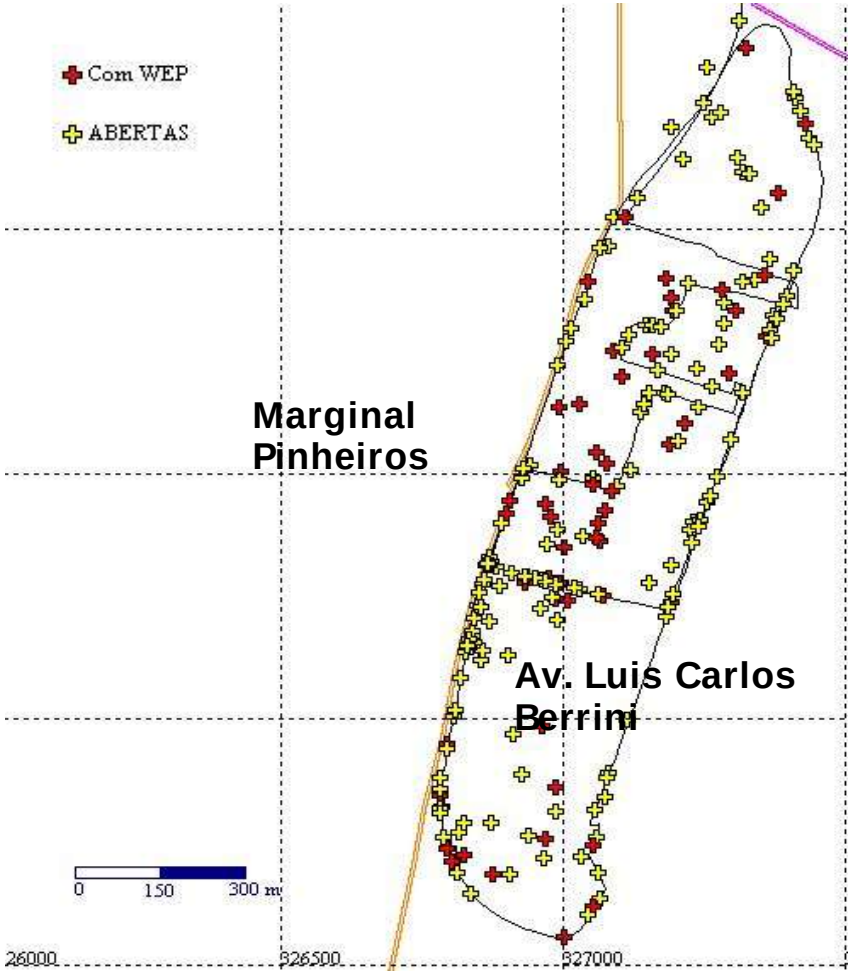
Av. Paulista


Av.
Paulista
Al. Santos
Al.
Jaú
Com WEP
ABERTAS
Av. Brigadeiro L.
Antônio
0
200
400 m
329500
330000
330500
331000
331500
332000

Av. Juscelino Kubitscheck



Av. Berrini


Com WEP
ABERTAS
Marginal
Pinheiros
Av. Luis Carlos
Berrini
0
150
300 m
26000
326500
327000

Conclusões

- 10% das redes sem fio localizadas estavam com a configuração *default* de fábrica

- Problema mais aparente: quebra de confidencialidade

Agradecimentos

- Lineu Pereira dos Santos Junior, pela paciência e suporte logístico em nossas incursões pelas alamedas e avenidas de São Paulo.

Base dos mapas utilizados

- http://www.gpstm.com/port/maps_port.htm