

# Wireless Network (In)Security

**JIM GEOVEDI**

*jim.geovedi@bellua.com*

**Bellua Asia Pacific**  
**www.bellua.com**

# **How to describe Wireless Technology?**



**Last mile.**



**Freedom.**



Cheap.

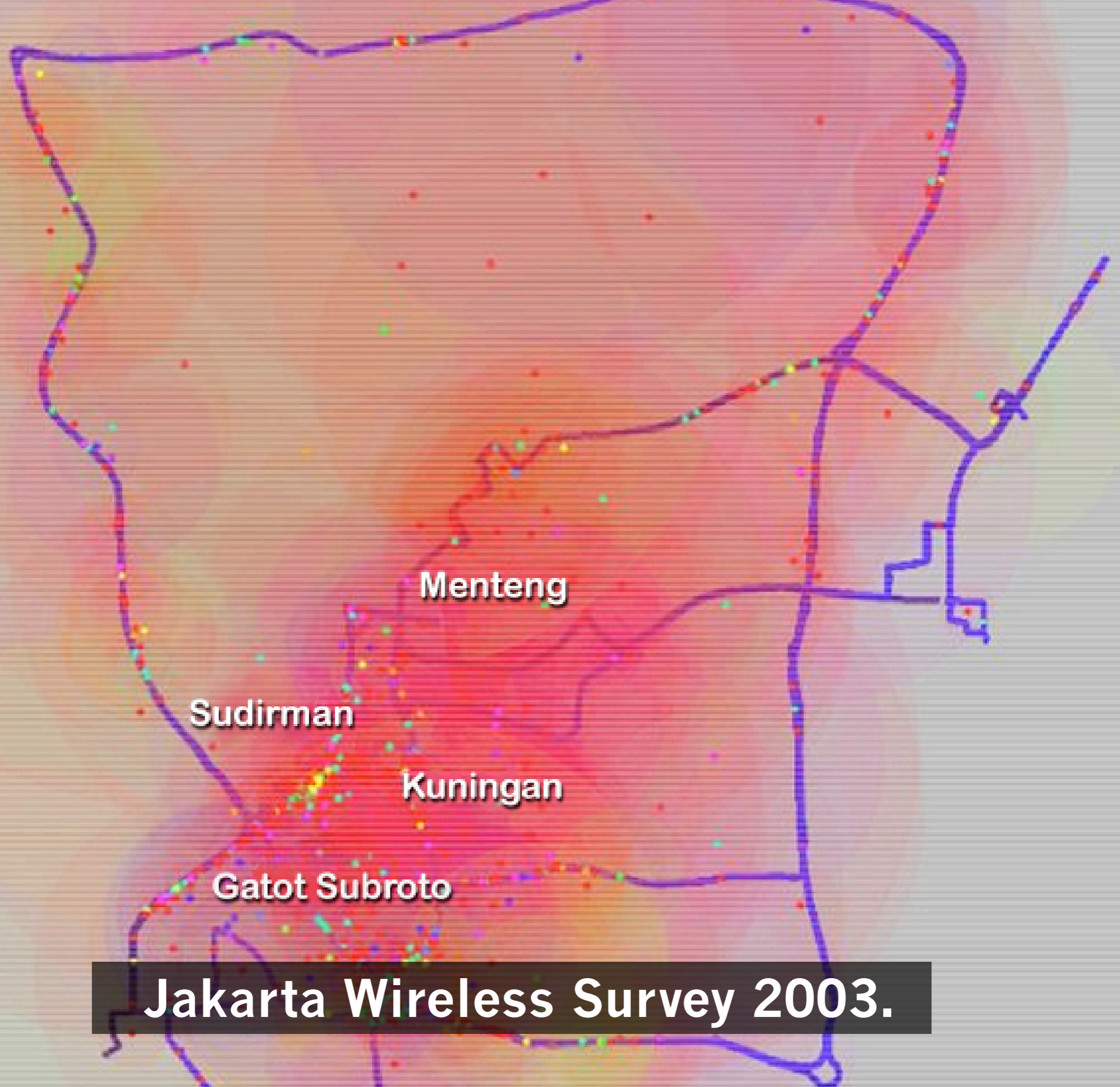
# WIRELESS ACCESS

**For Espresso Royale Customers**

Maintained & Serviced by  
Dynamic Edge, Inc.  
[www.dynedge.com](http://www.dynedge.com)

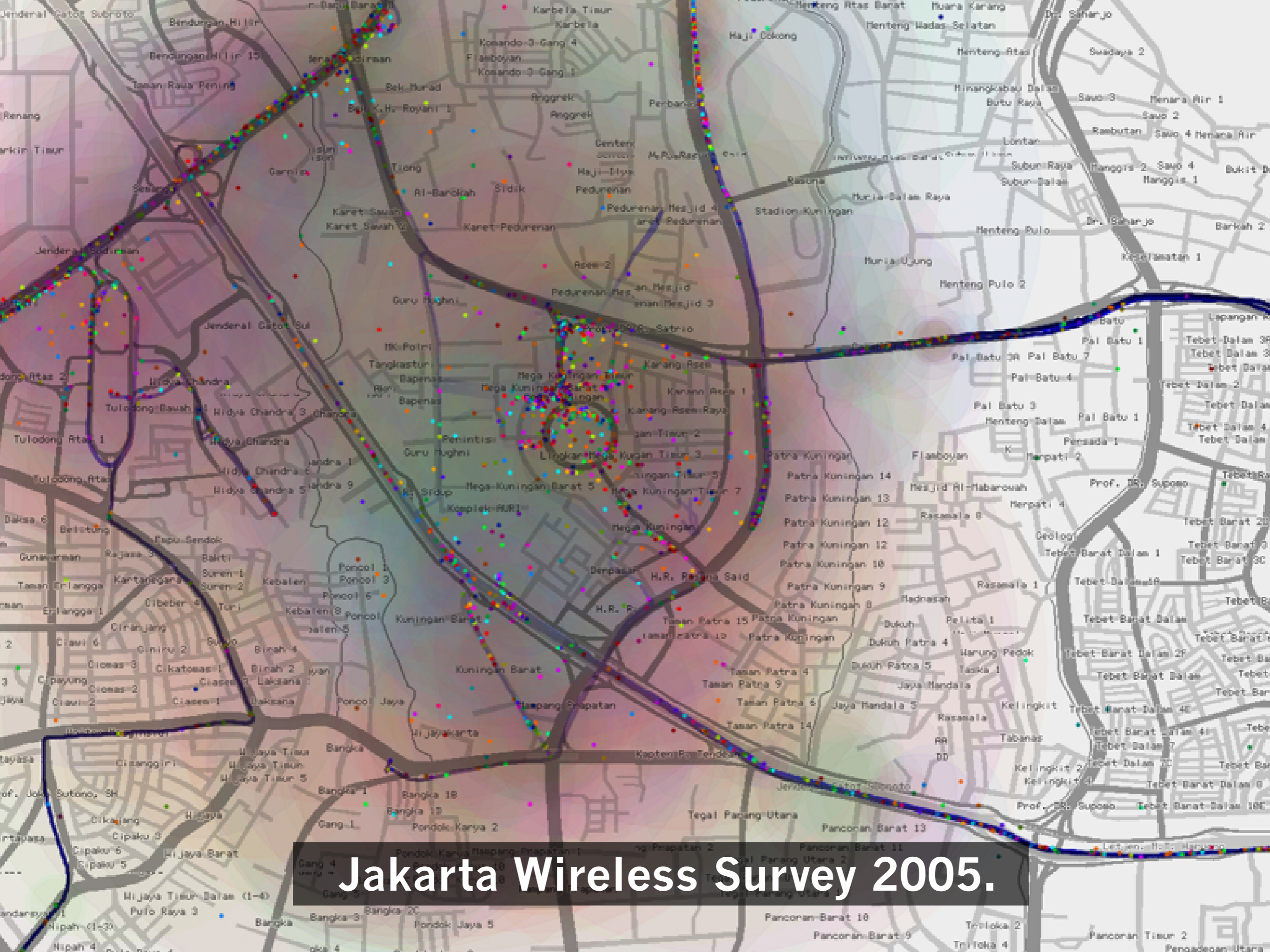
Network Name (SSID): ERC-MAIN  
Obtain IP Automatically (DHCP)

**Simple.**



**Jakarta Wireless Survey 2003.**





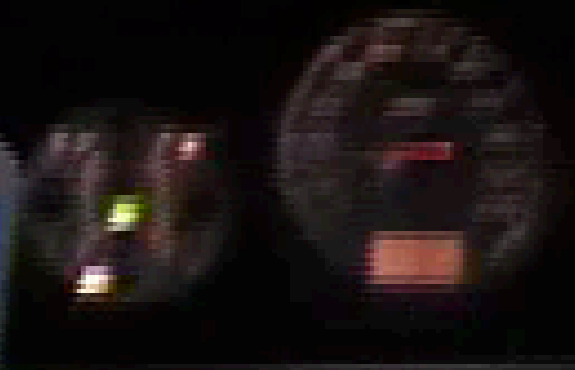
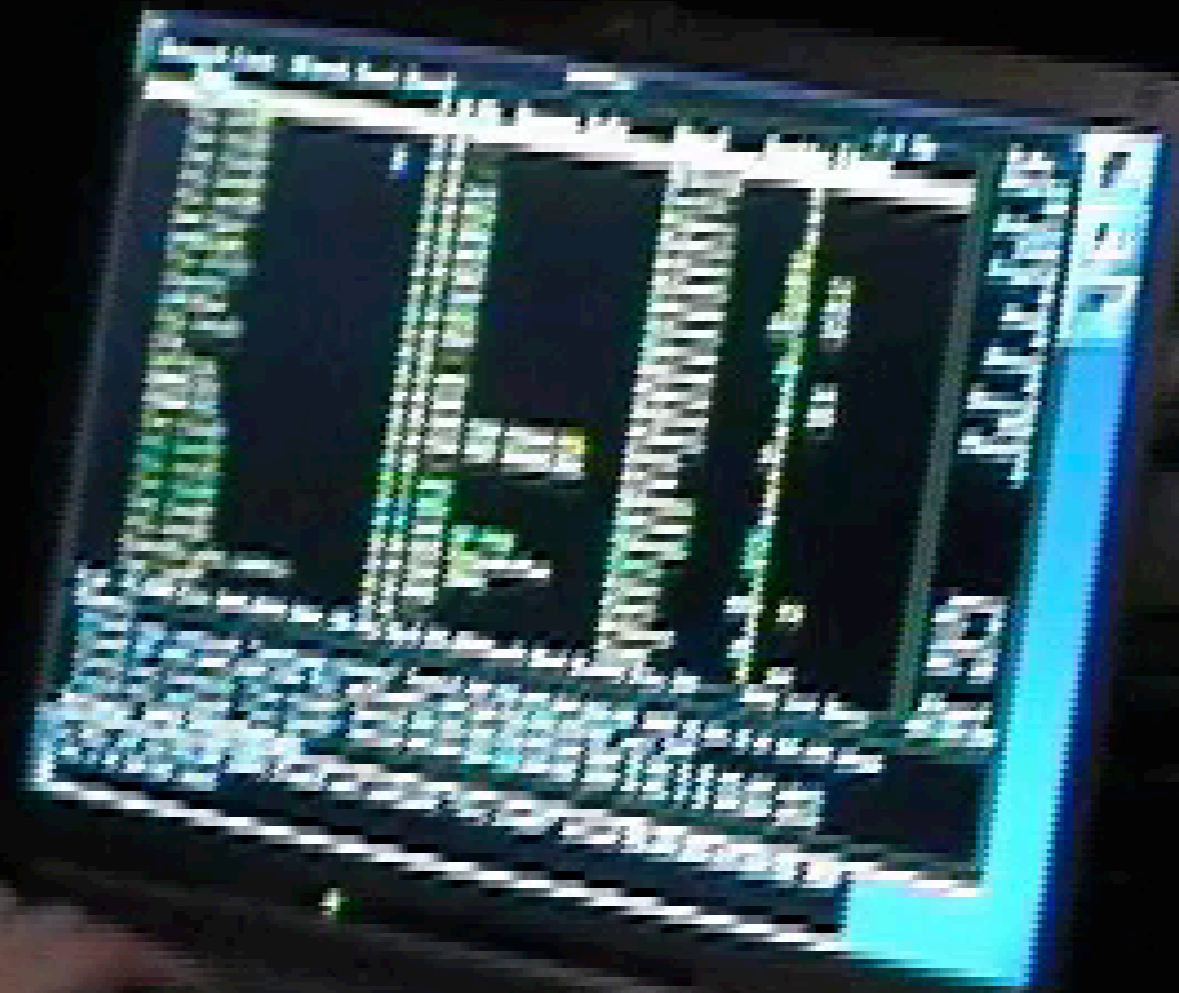
# Jakarta Wireless Survey 2005.



# Wardriving

## The equipment





# Wardriving: Captured information

```
ac@rostra.local: /Users/acz — vim
[0;1m
CR003002
[3;32HCARDHOLDER ENQUIRY
[5;3H1. Personal Particulars - 1
[9C13. Approval History
[6;3H2. Personal Particulars - 2
[9C14. Maintenance History
[7;3H3. Personal Particulars - 3
[9C15. Interest & Cash Advance Balances
[8;3H4. Personal Particulars - 4
[9C16. Last 2 Months Statement Details
[9;3H5. Personal Particulars - 5
[9C17. Last 3 Months Statement Details
[10;3H6. Personal Particulars - 6
[9C18. Last 4 Months Statement Details
[11;3H7. Personal Particulars - 7
[9C19. Last 5 Months Statement Details
[12;3H8. Supplementary Cards
[14C20. Last 6 Months Statement Details
[13;3H9. Credit History Summary
[11C21. Enrolmt in Instalment Payment Plan
[14;2H10. Unbilled Transactions Details
[4C22. Loyalty Program Points Allocation
[15;2H11. Last Statement Details
[11C23. Disputed Transactions
[16;2H12. Card Replacement History
[9C24. Cardholder Memos
[24;1HSelect Option :
[46C<Ctrl-X> to exit

ac@rostra.local: /Users/acz — bash
[22C14-12-2004
-----
Time Pos Card No
[10CTMCC Merchant Name
[5CCtry
[8CAmount App CD Res
-----
[0;1m
On Us Approval
-----
[18BCardPro V4.0-----CardPro Credit Card System
[61C<Ctrl-X> to exit
[5;1H22:49 902 42019100SYSCAN04 P7011 PURI AVIA HOTEL IDN
[8C346,800 919119 N00
22:47 902 42019100SYSCAN04 P7011 PUTRI DUYUNG ANCO IDN
[8C665,500 904629 N00
22:45 902 42019100SYSCAN04 P5912 VITA APOTIK, KGP IDN
[8C183,500 514855 N00
22:44 902 47848700SYSCAN04 P7011 HOTEL GRAND ZURI IDN
[8C700,000 243169 N00
[0;7m
22:41 902 42019200SYSCAN04 P5812 REST GAJAH WONG IDN 968,990 D51
22:38 902 42019200SYSCAN04 P7011 BARITO PALACE HOT IDN
[8C500,000 002200 N00
22:35 902 42019200SYSCAN04 P5812 PIZZA HUT - TEBET IDN
[8C247,501 023083 N00
22:34 902 42019400SYSCAN04 P5812 PANGKEP 33 RESTAU IDN
[8C343,500 004430 N00
PS_MLT
```

# Wardriving: Captured information

```
713662--M>8
713663--M=μ
713664-*y}e
713665-                               PT. BANK ████████
713666-.....
713667-                               CARD CENTRE INQUIRY MENU
713668- 1. Applications Enquiry
713669: 2. Cardholder Enquiry
713670- 3. On-us Online Monitoring
713671- 4. Not On-us Online Monitoring
713672- 5. On-us & Not On-us Online Monitoring
713673- 6. Visa Electron Online Monitoring
713674- 7. Customer Enquiry
713675-
713676-
713677-
713678-
713679-
713680-
713681-                               98. Password Maintenance
713682-                               99. Exit
713683:CardPro V4.0-.....CardPro Credit Card System
713684-Select Option : <e
713685--M>8
```

# Wardriving: Captured information

```
4265353539000575adTAHAPAN 539-10-05403-8ad941789EA
5001428041703133555aLUNO123aPENARIKAN RP. e3 0.00 aDANA =
KURANG (SALDO MINIMUM RP.25.00adad0FB6BEB8
1001429041703133833aLUNO123ae6s(sW1BANK =
[REDACTED]ae4CUSTOMERe1RESPONSEe1CENTREae7[REDACTED]adTSK.LB.TASIK =
e217/04/03e214:07:02adNO. RESI e?e6 8828aNO. KARTU e5 =
4265353539118609adTAHAPAN 539-10-22449-9adDFD37D35
5001430041703133835aLUNO123aPENARIKAN RP. e3 0.00 aPIN =
SALAH - KARTU DIBLOKIR adadA7CCEDBD
1001431041703133902aLUNO123ae6s(sW1BANK =
[REDACTED]sW0ae4CUSTOMERe1RESPONSEe1CENTREae7[REDACTED]adTSK.LB.TASIK =
e217/04/03e214:07:31adNO. RESI e?e6 8829aNO. KARTU e5 =
4265353539118609adTAHAPAN 539-10-22449-9ad6F644F93
5001432041703133904aLUNO123aINQUIRY e3 =
aSEMENTARA SISTEM TDK DPT DIGUNAKAN adad4CD533CA
1001433041703133939aLUNO123ae6s(sW1BANK =
[REDACTED]sW0ae4CUSTOMERe1RESPONSEe1CENTREae7[REDACTED]adTSK.LB.TASIK =
e217/04/03e214:08:08adNO. RESI e?e6 8830aNO. KARTU e5 =
4265353539118609ad8318 - KESALAHAN PROSES TRANSAKSI adad47EBC902
1001434041703134027aLUNO123ae6s(sW1BANK =
[REDACTED]sW0ae4CUSTOMERe1RESPONSEe1CENTREae7[REDACTED]adTSK.LB.TASIK =
e217/04/03e214:08:38adNO. RESI e?e6 8831aNO. KARTU e5 =
4265353539088257adTAHAPAN 539-10-07962-6adADFE1C0C
5001435041703134029aLUNO123aPENARIKAN RP. e3 150,000.00 aSALDO =
RP.e5 32,438.00 a MOHON GANTI PIN ANDA a =
SECARA BERKALA adad4FFAD7BE
1001436041703134139aLUNO123ae6s(sW1BANK =
[REDACTED]sW0ae4CUSTOMERe1RESPONSEe1CENTREae7[REDACTED]adTSK.LB.TASIK =
e217/04/03e214:09:48adNO. RESI e?e6 8832aNO. KARTU e5 =
4265353539117551adTAHAPAN 539-10-22345-0ad33E73B93
5001437041703134141aLUNO123aPENARIKAN RP. e3 1,000,000.00 aSALDO =
RP.e5 6,308,284.00 a MOHON GANTI PIN ANDA a =
SECARA BERKALA adadCBBC38CE
1001438041703134225aLUNO123ae6s(sW1BANK =
```

ATM transactions in cleartext



# Warflying

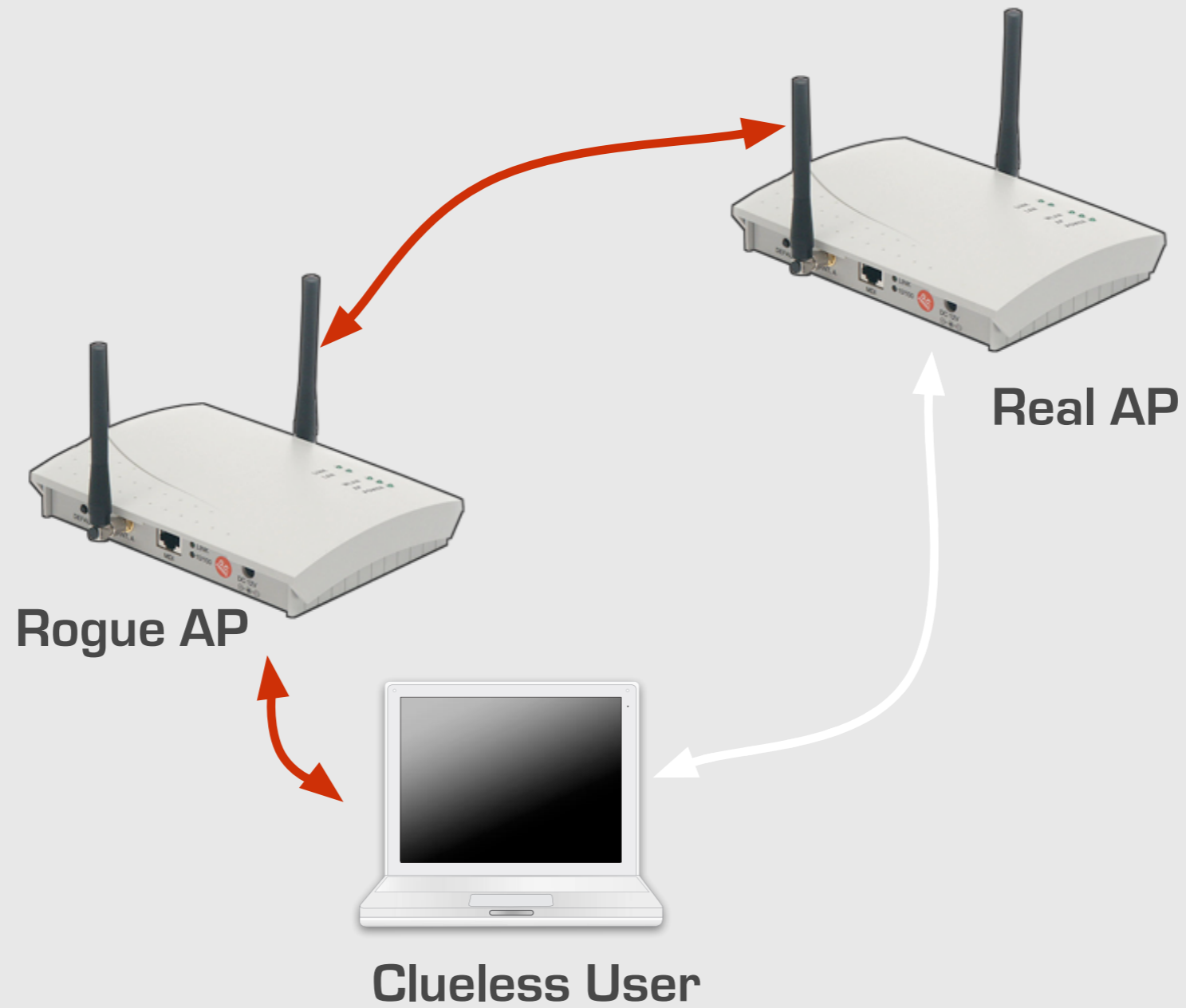




# Warflying

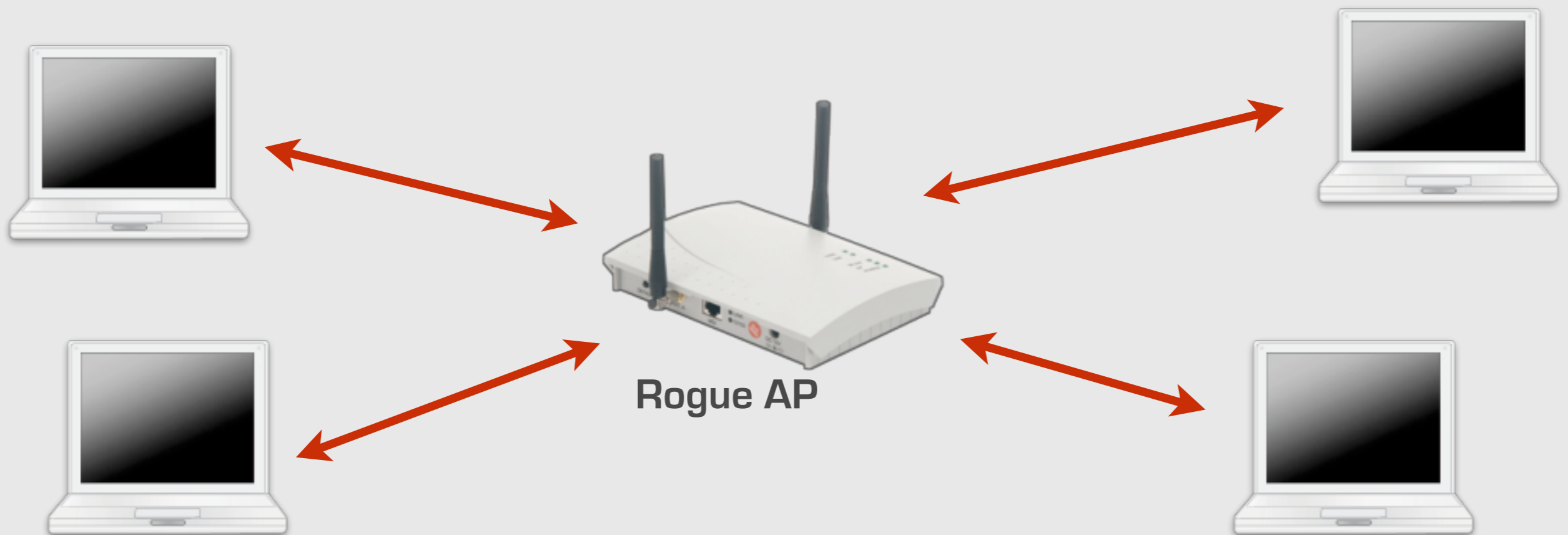
```
-5,254 Len 105,932 All 11670,3m Spd 904,063km  
*  
requesting strings from the server  
saving data files.  
found new probe network "(Green building SSID)" has  
saving data files.  
battery: 82% 526523190
```

# Rogue APs



# Gnivirdraw

- Inverse Wardriving.
- A Rogue AP looking for “Wi-Fi Suckers”.



# Rogue AP how-to

- Use a compatible wireless card to create a competing access point
- Must provide network information (IP address, gateway, DNS) — DHCP
- Resolve all or specific addresses to your address, or NAT and provides fake DNS replies
- Dynamically display fake websites for popular URLs via virtual hosting
- Pray?!

# 802.11 Phising

- What bits of information are users giving away via wireless?
  - Domains
  - Shares
  - Proxies
  - Installed software
  - Other preferred wireless network
  - More?

# FishNet

- Taking advantage of suspected client behaviour, such as zero configuration (rendezvous), auto-update services, etc.
- Fake services traps, exploiting clients, then install backdoors or propagate worms or whatever you want!
- Control the clients!



# Defence?

- Oh, there are many!
  - Authentication and authorisation
  - Cryptography
  - etc.

# MAC address filtering

- Identification factor — **MAC address**
- Provided by manufacturers
- Intended to be permanent
- Today, changing MAC address is pretty easy

# Piggy-jacking on wireless connection

- Gaining access to a restricted communication channel by using already established other user session.
- Rule of thumb: Sniff the traffic, choose the target (other user) then impersonate the target as soon as the target logged off.
- Denial of service is FAIR in the game.

# Wired Equivalent Privacy (WEP) security issues

- IV (initialisation vector) reuse
- Known plain-text attack
- Partial known attack
- Authentication forging
- Denial of service
- Dictionary attack
- Realtime decryption

# Wi-Fi Protected Access (WPA) security issues

- Attack against *Michael* — cryptanalytic
- PSK (pre-shared key) dictionary attack vulnerability
- Attack on default key
- Denial of service attacks

# IEEE 802.11i (WPA2) insecurity

- One Message Attack on the 4-way handshake
  - The attacker is capable of impersonating the authenticator, composing a “message”, and sending to the supplicant
  - One simple one-message attack will cause PTK (Pair-wise Transient Key) inconsistency



# EAP

## (Extensible Authentication Protocol)

- IETF standard for extensible authentication in network access. It is standardised for use within PPP, IEEE 802.1X, and VPNs
- Proposed methods:
  - Certificate authentication
  - Token card/smartcard authentication
  - Password authentication
  - Pre-shared keys

# Security vulnerabilities in EAP methods

- Known security vulnerabilities of implemented or proposed EAP methods
  - Kerberos vulnerability
  - Cisco's LEAP vulnerability — vulnerable to dictionary attacks
  - EAP/SIM vulnerability — GSM/GPRS
  - PAP vulnerability — cleartext authentication using RADIUS (even with protected tunnel)
  - MITM attacks on Tunneled Authentication Protocols

# RADIUS

## (Remote Access Dial-in User Service)

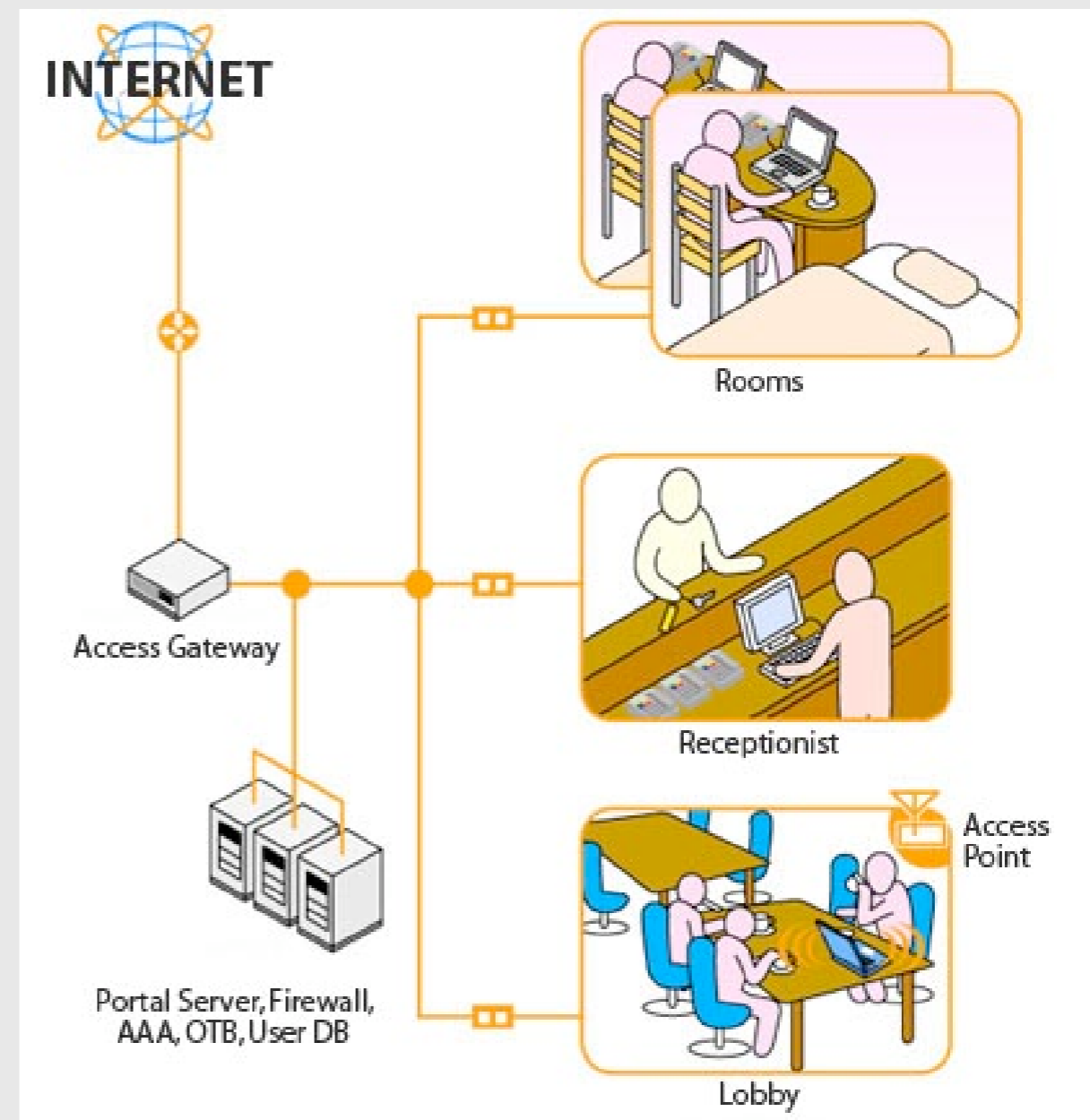
- Widely deployed protocol for authentication, authorisation, and accounting (AAA) — simple, efficient, and easy to implement
- Issues on transport — UDP nightmare
- Issues on cryptography — Not widely used since many embedded systems do not have the horsepower or headroom for RADIUS over IPSec

# Security issues on Ad-hoc networks

- 802.11 enables Ad-hoc networking to communicate stations without an AP
- Recent IETF work in progress enables hosts to automatically assign IPv4 addresses without a DHCP server, and resolve names without a DNS server (IPv4 or IPv6)
- Stations can act as bridges (layer 2 approach) or routers (layer 3 approach, MANET)

# Wireless Implementation Hotspot

- Hotels
- Airports
- Coffee shops
- etc.



# How to use paid Hotspot

- Getting access
- Visit hotspot with wireless device
- Associate and get network configuration
- Open web browser and get redirected to login page
- Authenticate
- ... welcome to the Internet

# Getting access to paid Hotspot

- Buy pre-paid card
- Registration with credit card
- Pay later — charged in room hotel, need room number
- Send text message (SMS) via mobile phone
- Social engineering
- Hacking! :-)

# Wireless Hotspot critical points

- Network configuration
- Authentication and authorisation methods
- 3rd party interfaces
- Misunderstanding the trust



# Upcoming...

- Bluetooth
- RFID
- IrDA

# Bluetooth

- Wire replacement technology
- Low power
- Short range: 10m — 100m
- 2.4 GHz
- 1 Mbps data rate

# Bluetooth Hacking: Bluejacking

- Early adopters abuse '**Name**' field to send message
- Now more commonly send '**Business Card**' with message via OBEX
- 'Toothing' — casual sexual liasons

# Bluetooth Hacking: Bluesnarfing

- ‘Snarf’ — networking slang for ‘unauthorised copy’
- Target:
  - Data theft
  - Calendar: Appointments, Images
  - Phone Book: Names, Addresses, Numbers, PINs and other codes, Images

# Bluetooth Hacking: Bluebugging

- Create unauthorised connection to serial profile
- High level of control to AT command set
  - Call control — turning phone into a bug
  - Sending/Reading/Deleting SMS
  - Reading/Writing phonebook entries
  - Setting Forwards
  - Causing costs on vulnerable phones

# Bluetooth Hacking

Demo



# RFID

- The card information is obscured by a cycling code
- To defeat RFID is not by cracking the encryption, but by using repeater-transmitter to “extend” the range of RFID
- It is a whole lot easier to re-broadcast than crack and recreate the code

# IrDA

- Infra red unlikely to be replaced — fit for use, simple, and **cheap**
- The ultimate in ‘security by obscurity’: invisible rays, simple code with total control, inverted security model (end-users filters content)
- Vulnerable to simple replay attack. — record codes and retransmit
  - One-line command can open your garage door!
  - `for i in `perl -e 'for (0..255){printf("%02x\n", $_)}'`; do irsend SEND_ONCE garage $i; done`

# IrDA

## Garage door opener



Before



After

# IrDA

## Hotel TV

- Inverted security model
  - Back-end may broadcast all content
  - TV filters content
  - TV controlled by end-user
- No authentication required
- No encryption — closed system, eh?

# IrDA Hotel TV



# Defending Wireless networks

- Multiple issues afoot. Need a solid grasp of network engineering, security, and user needs
  - Architecture and Configuration
  - Protecting the enterprise and the client
  - Secure and Security Operations

# Wireless Architecture

- Many options... perhaps too many
- First, must understand how network and system architecture impacts wireless security
- Layered defences are a good way to start
  - Securing layer-2 only
  - Securing layer-3 only
  - Securing both layers

# Other Defences

- Wireless usage policy
- Regular check for Rogue APs and latest vulnerability information
- Wireless honeypot



# Conclusion

- Fundamental problems in wireless security are no longer about technology; they are about how to use the technology
- Wireless is a complicated series of interconnections — security must permeate the system: its components and connections
- Like other modern systems have so many components designers, implementers, or users — that insecurities always remain

**No system is perfect; no technology is The Answer™**