Wireless Network (In)Security

JIM GEOVEDI
jim.geovedi@bellua.com

Bellua Asia Pacific
www.bellua.com

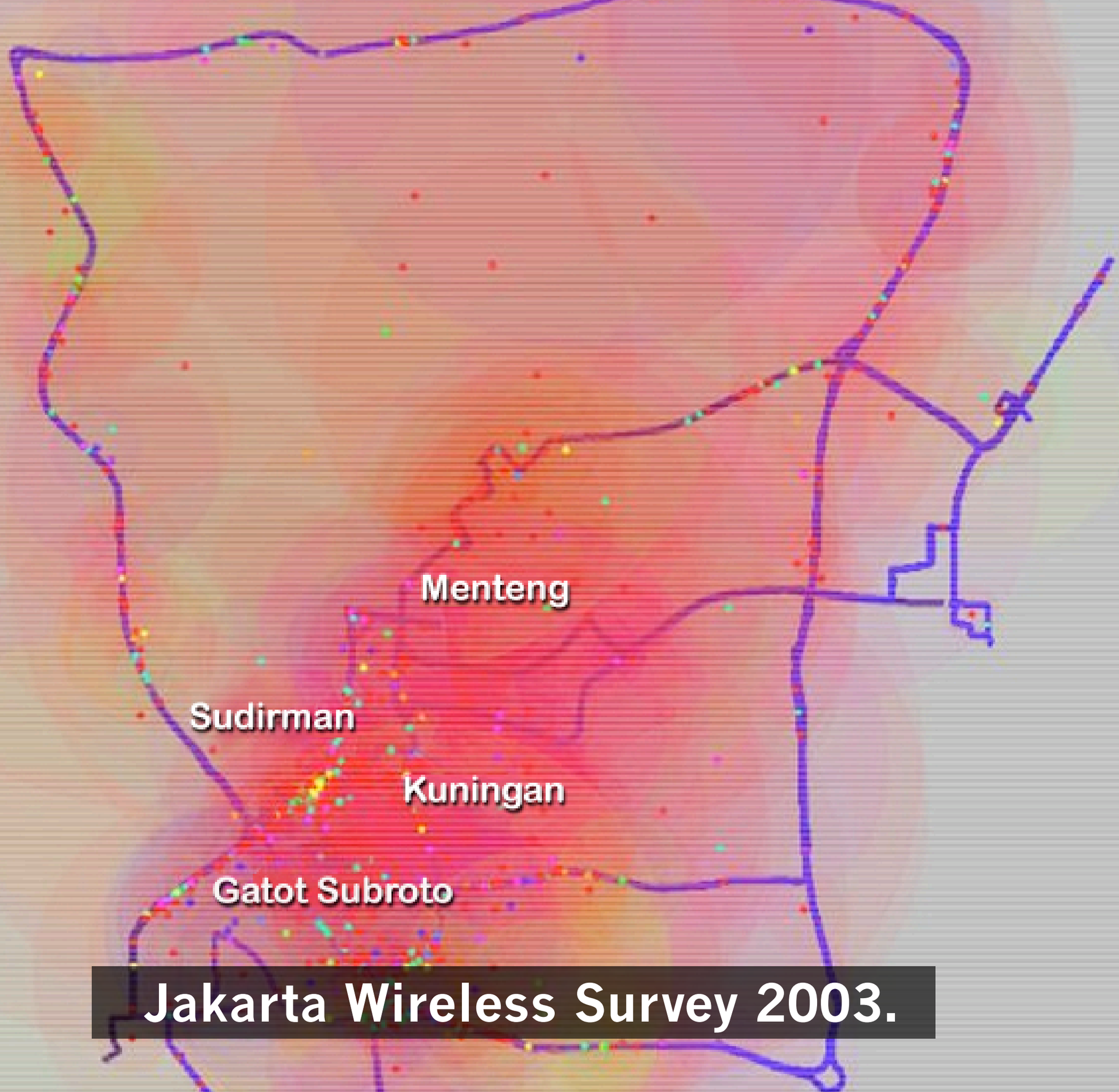
How to describe Wireless Technology?

Last mile.

Freedom.

Cheap.

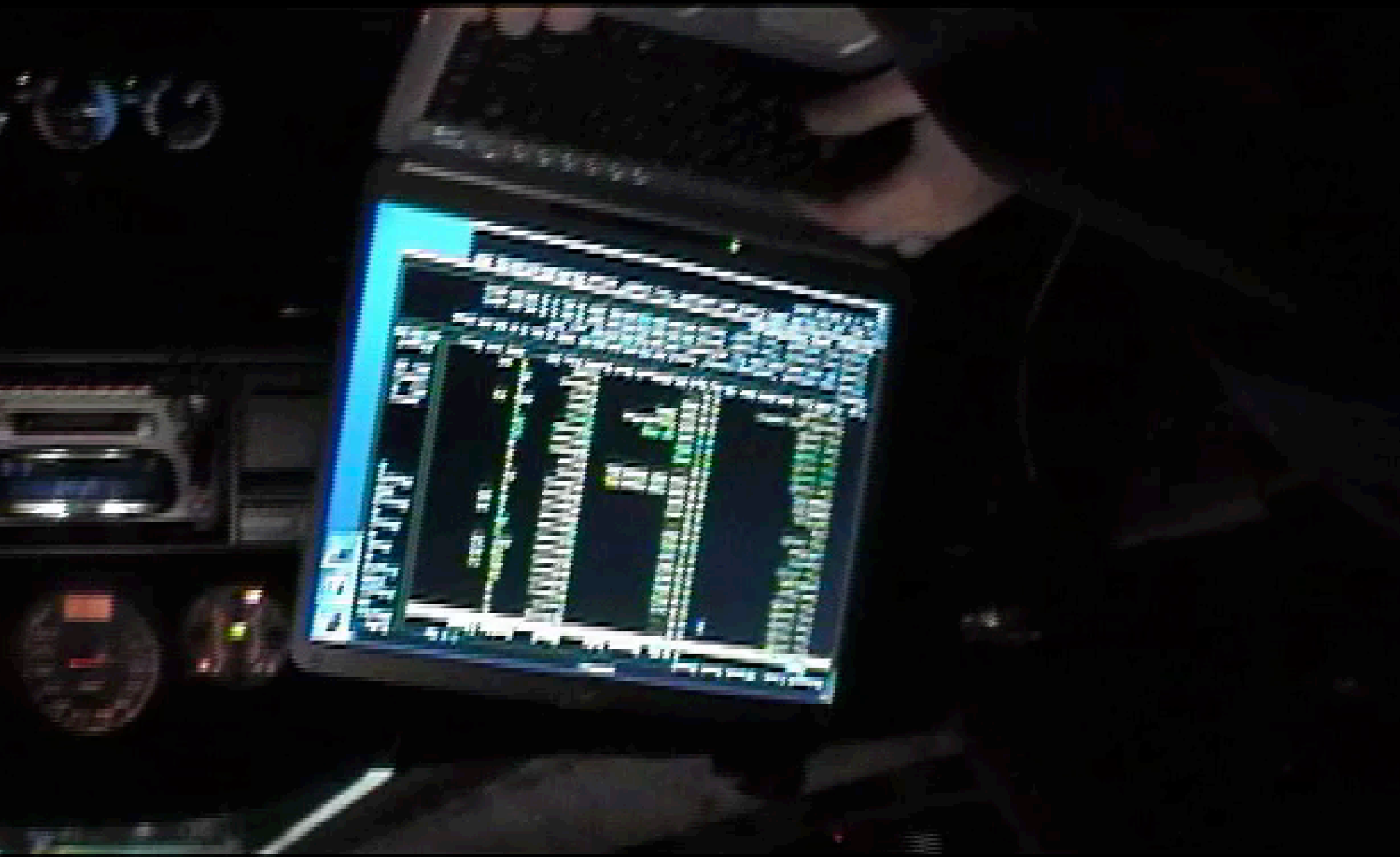

WIRELESS
ACCESS
For Espresso Royale Customers
Maintained & Serviced by
Dynamic Edge, Inc.
www.dynedge.com
Network Name (SSID): ERC-MAIN
Obtain IP Automatically (DHCP)
Simple.



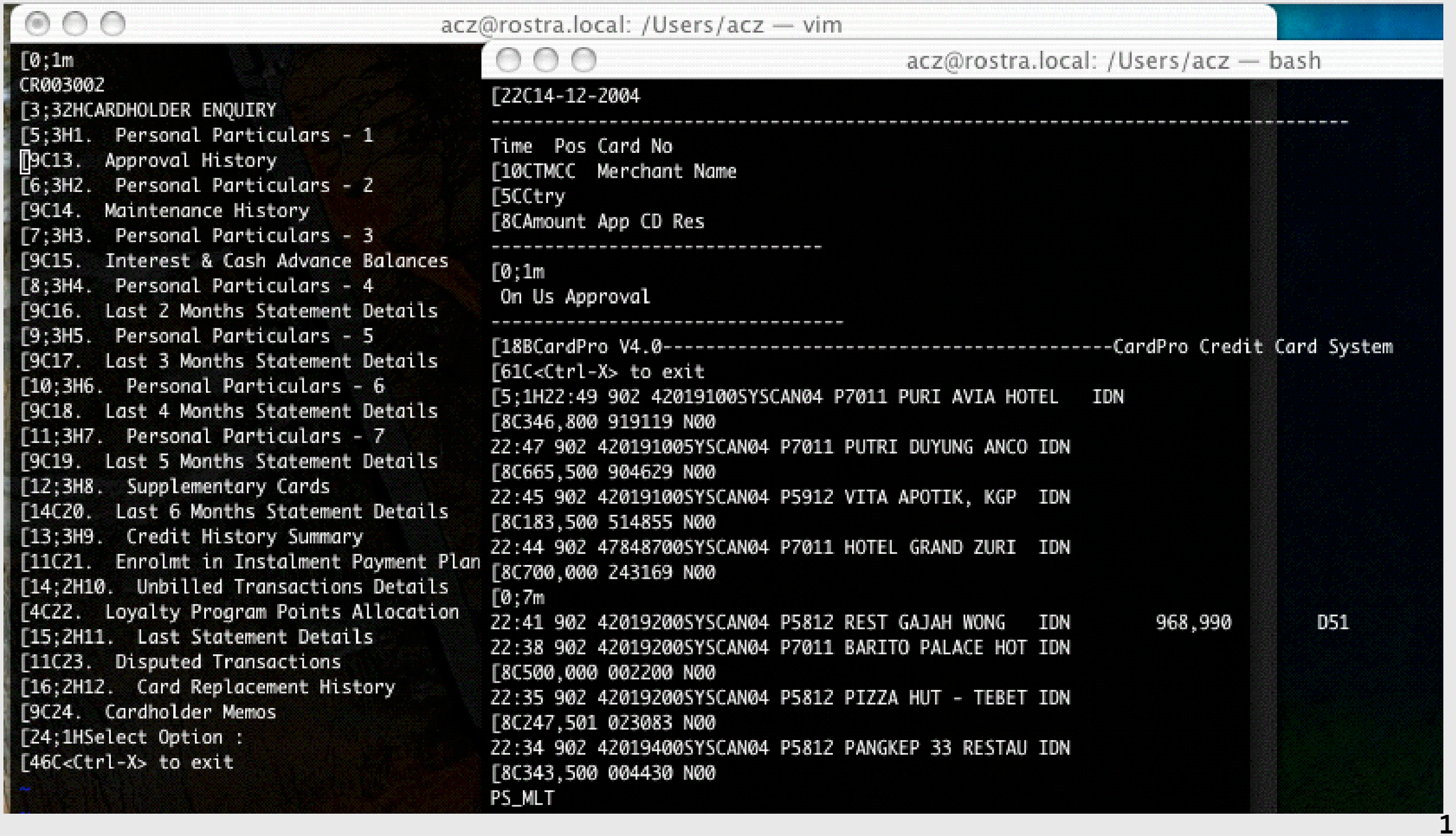
Jakarta Wireless Survey 2003.

Jakarta Wireless Survey 2005.

Wardriving
The equipment



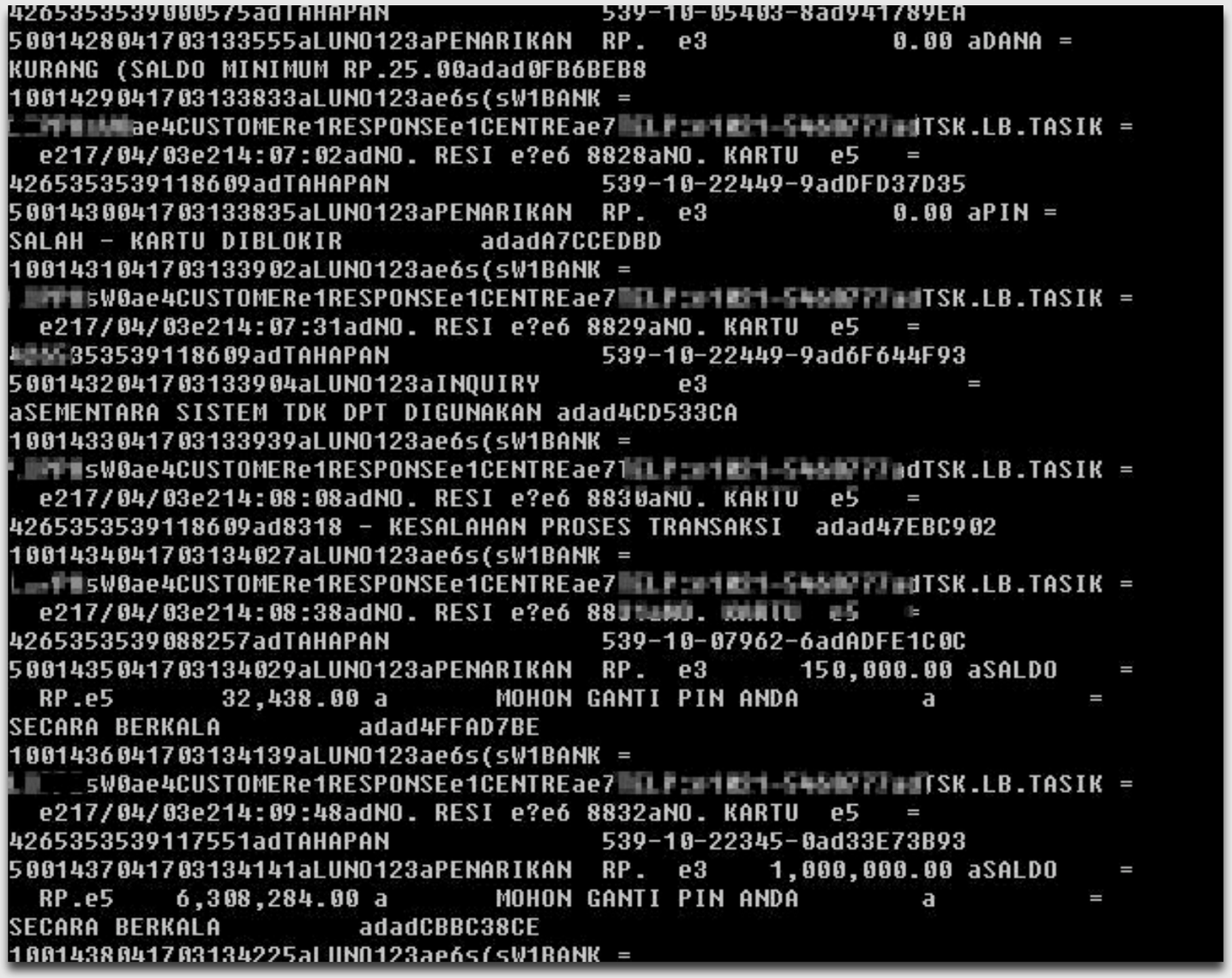
Wardriving:
Captured information



Wardriving:
Captured information

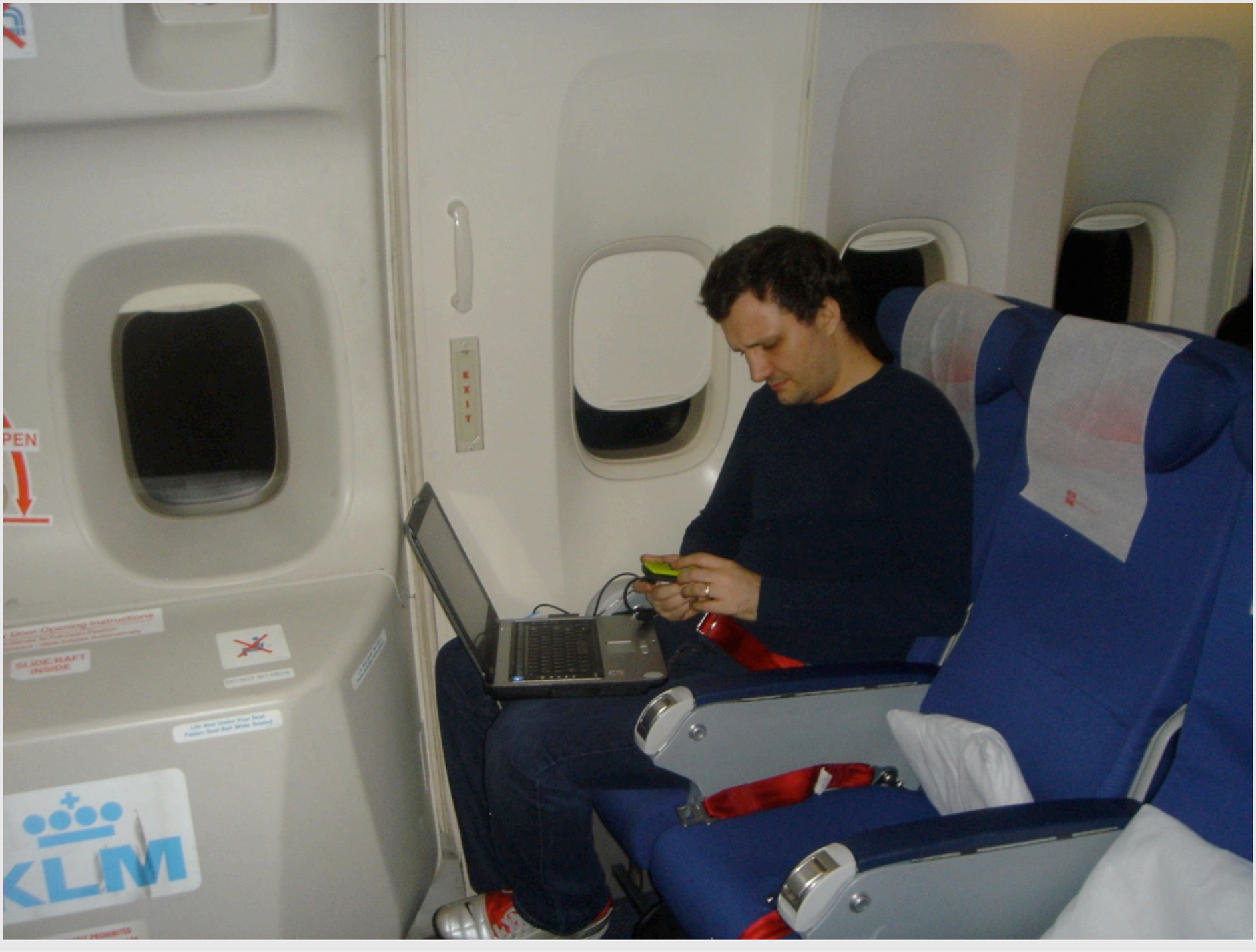
```
713662--M>8
713663--M=µ
713664-»y]@
713665-                                   PT. BANK [redacted]
713666----------------------------------------------------------------------
713667-                                CARD CENTRE INQUIRY MENU
713668- 1. Applications Enquiry
713669: 2. Cardholder Enquiry
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 Syste
713684-Select Option : ◁
713685--M>8
```

Wardriving:
Captured information

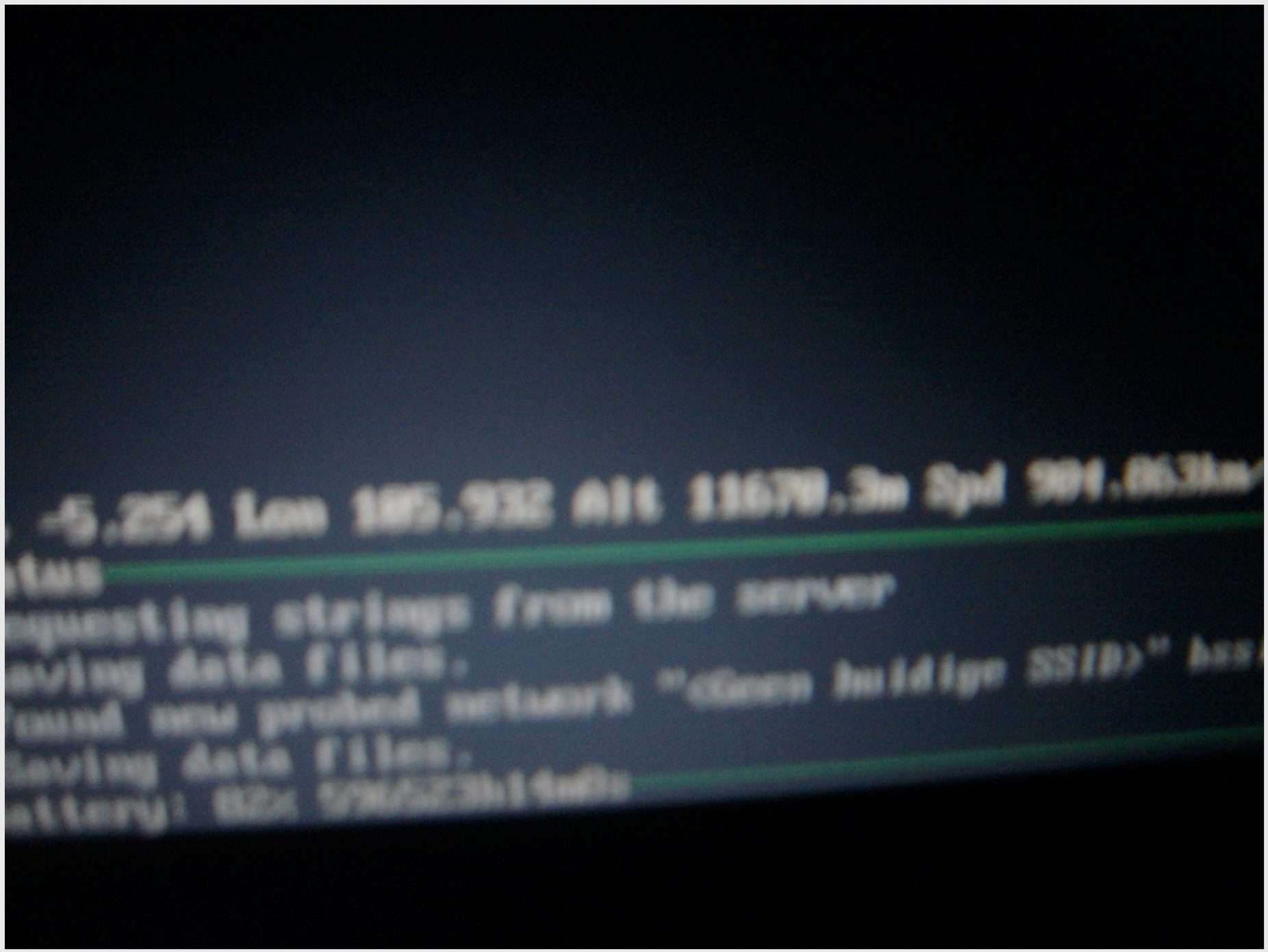


ATM transactions in cleartext

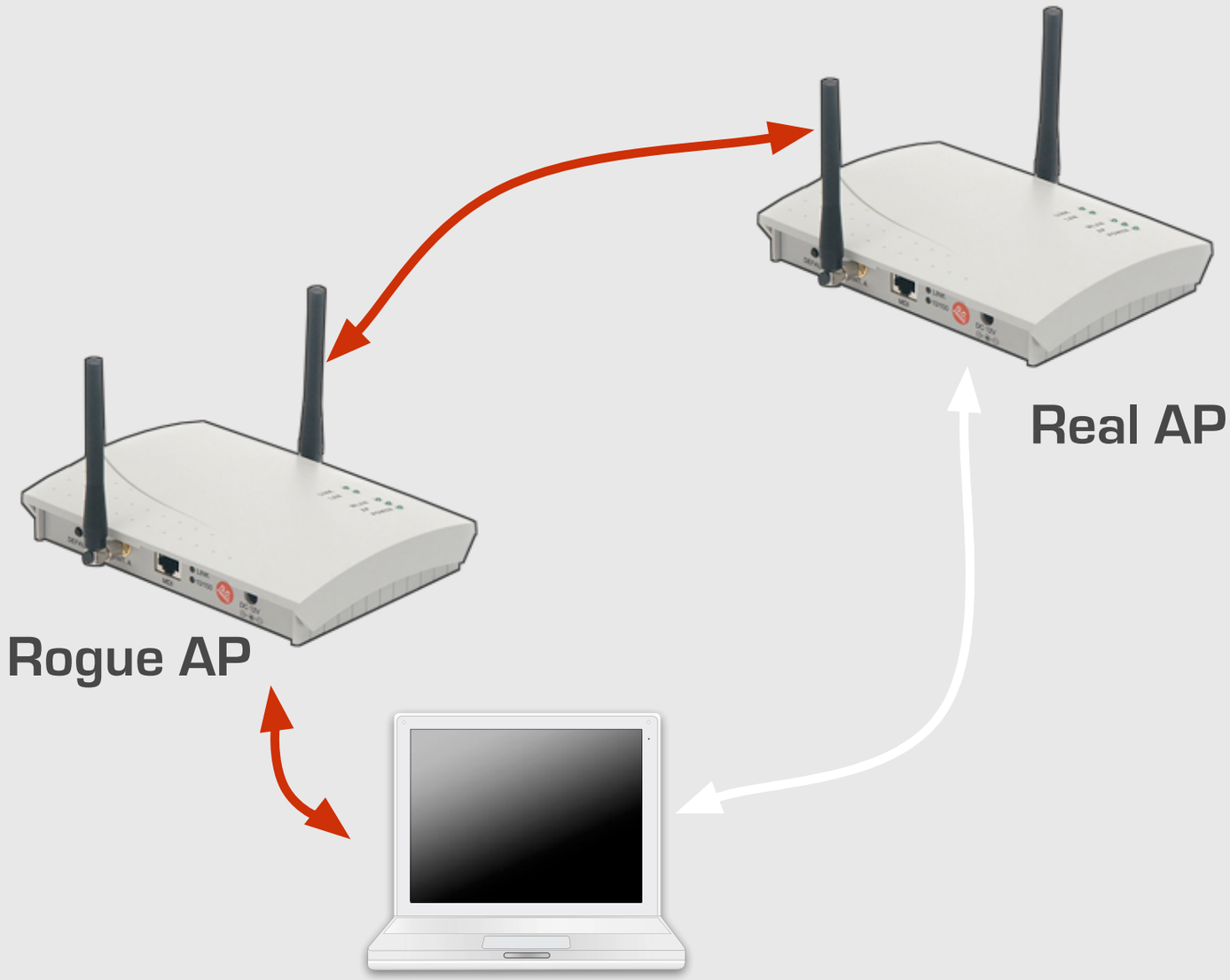
Warflying



Warflying

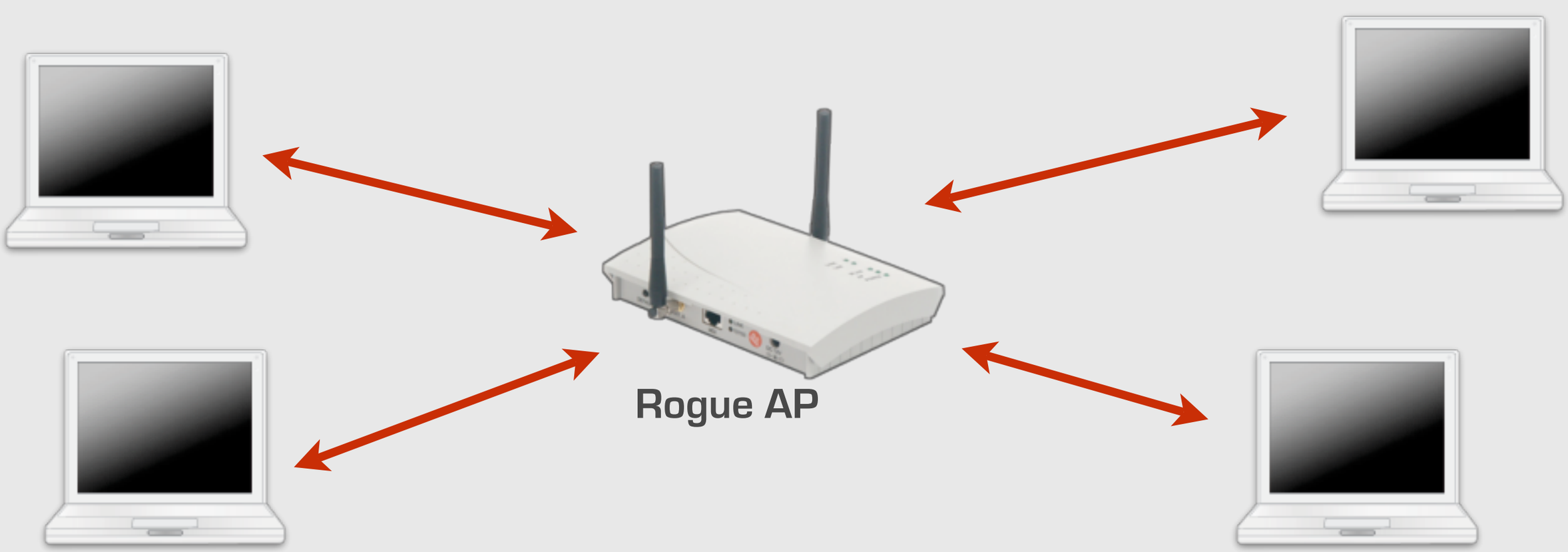

-5.254 Lon 185.932 Alt 11670.3m Spd 991.053km
requesting strings from the server
saving data files.
found new probed network "<Guest Intrigue SSID>" hex
saving data files.

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)

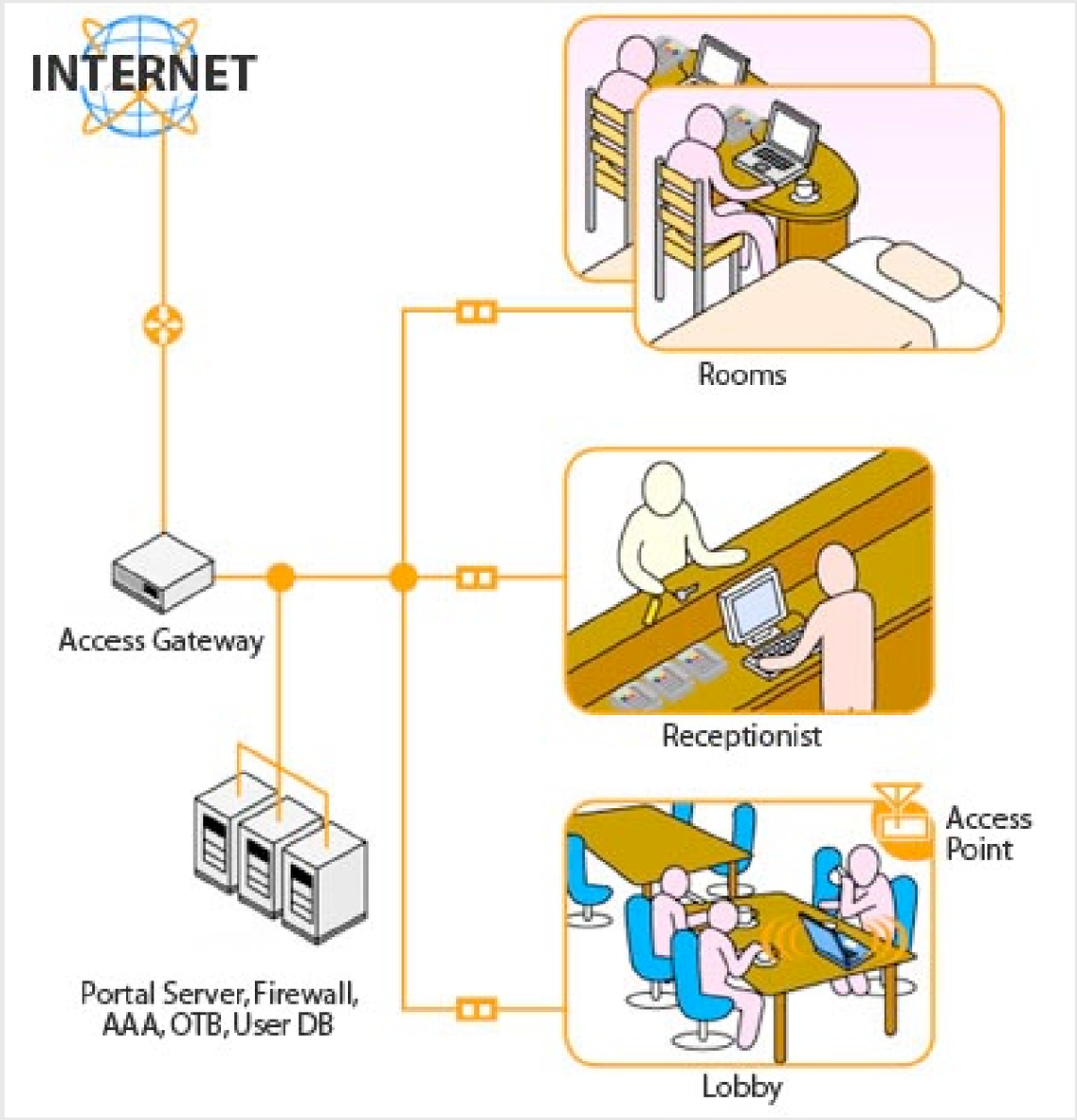
- Widely deployed protocol for authentication, authorisation, and accounting (AAA) — simple, efficient, and easy to implement
  - Issues on transport — UDP nightmare
  - Issues on cryptography — Not widely used since many embedded systems do not have the horsepower or headroom for RADIUS over IPSec

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™