Tempest Radiation – "you are what you emit" …

Jim Binkley

bibliography

- Ross Anderson, Security Engineering, c. 15 (soft tempest paper too)
- Cryptonomicon – Neal Stephenson
- Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Wim van Eck, Computers & Security 1985, v.4
- www.eskimo.com/~joelm/tempest.html

what is it

- 3 possible names
- **Van Eck radiation**
- **tempest radiation**
- **emsec** for **emissions security**
- emsec means PREVENTING computers or networks from emitting information
- electro-magnetic info leakage is usually the main point (detect it or prevent it)
- may apply to display, computer itself, or networking (ethernet/rs232)

related problems

- closed related to questions of electronic warfare
  - passive prevention of electronic attacks (shielding)
  - active detection of electronic attacks
    - looking for bugs in the room
  - tempest radiation is not: launching a missile
- somewhat related to traffic analysis
  - Japanese aircraft carrier - akagi

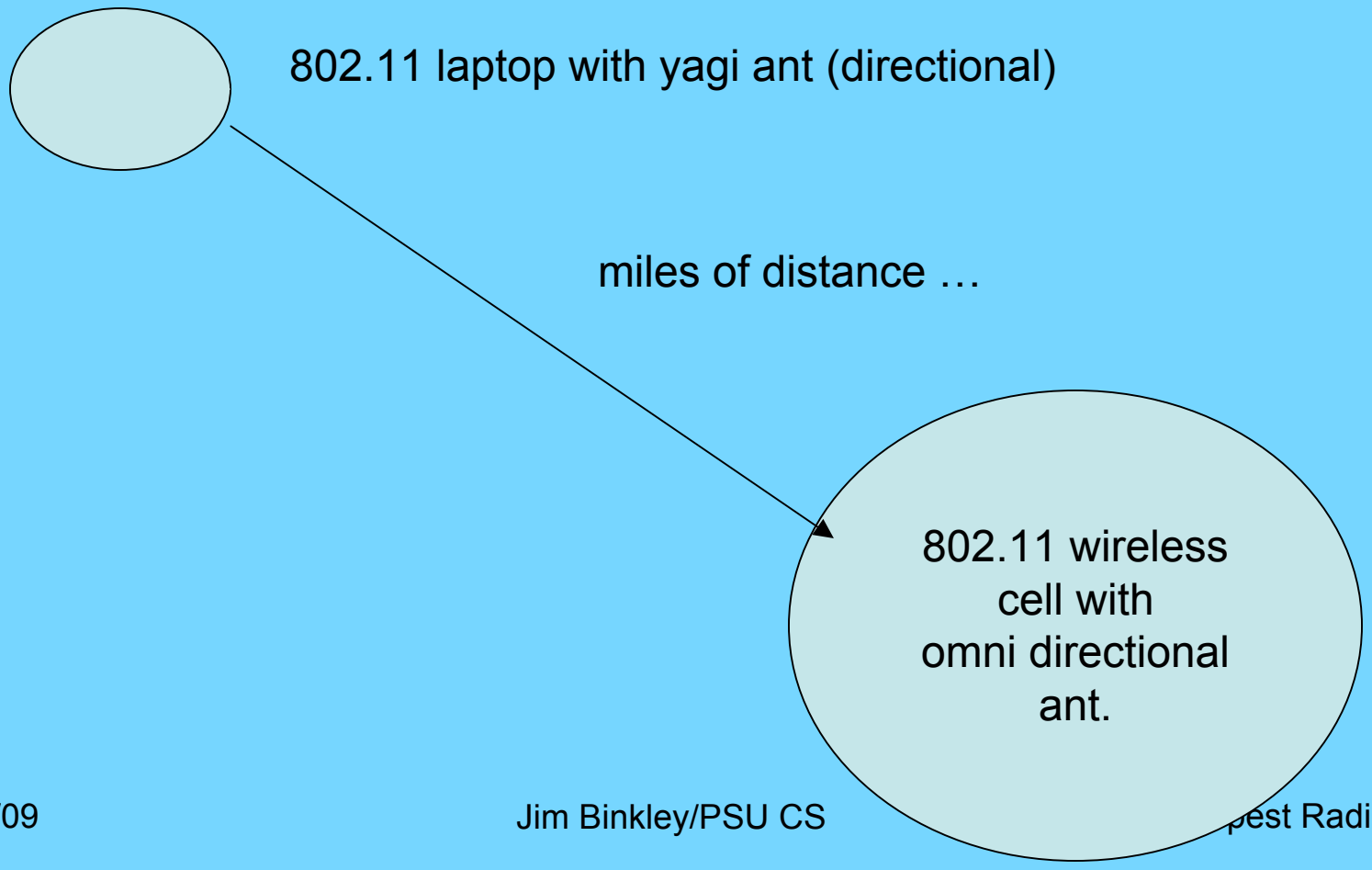
power analysis is related

- can watch power used by smartcard
- may be able to use measurement to recover a key
- oops …

is this stuff important?

- read Ross Anderson and decide
- certainly important at govt vs govt level
  - military vs military
  - spy vs spy
- what about commercially?
- what about your neighbors using your wireless ap because the radio emits there too …
- what about accidents – sorry about my cell phone making the plane crash …

consider 802.11 wireless



actually this is a soup can …

history

- crosstalk on telephone lines is old
  - line A picks up traffic from line B
  - twisted pair design mitigates against this
- in ww1, earth return in field telephone lines allowed leakage across the front
  - valve amps and piles of unused wire improved attacking capabilities
  - earth return circuits were abolished
- ww2 – direction finding equipment used to track radio signals, radar, etc.

history

- Brits used vans to track down “unlicensed” TV sets
- detector vans may be used to look for cable and satellite pirates
- in 60s, MI5 found that French encrypted emissions had faint secondary signal
  - when amplified, it was the plaintext
  - how common is this?
- Van Eck demonstrated that monitor signals could be “monitored” at a distance and fairly cheaply
  - computers are noisy …

history

- 90s – attacks on smartcards possible
  - via power measurements
  - via inserting glitches in power or clock lines
- of course lots of incidents in spy land too
  - the U.S. embassy in Moscow that had to be abandoned
  - but about black vans we actually know very little

bugs and anti-bugs

- info comes into being as speech or keystrokes
  - capture it at the source
  - recent work in decoding keystroke sounds
  - if captured as input, doesn't matter if encrypted

bugs and anti-bugs

- bugs are available in many forms
  - camera
  - mikes (battery life is constraint)
  - mike may be hooked up to power via telephone or AC
  - may look like something normal (electrical adapter)
    - but contain mike, camera, radio transmitter
  - trojan computer board with radio in it
  - variations on cellphone technology
  - laser microphone aimed at window pane
  - equipped with esoteric radios (burst transmission)

counter-measures include:

- nonlinear junction detector: finds hidden electronic equipment
  - sends radio and listens for harmonics
  - therefore hide bug IN computer
- surveillance receivers
  - sweep radio spectrum for signals
- break line of sight
  - lasers need line of sight
- shield the entire building (or just your head)

what is kitty thinking?

bet you cannot find out …

procedural controls may exist

- but may be pain to users
  - security is a pain to users?
- NSA banned furby toys
  - because they had microphone in them
- red lights go off at headquarters and follow visitor around
  - so that everyone knows to be careful with computer screens, and telephone conversations

passive attacks

- opponent uses esignals that exist and does not create them on her own
- 1. signal is conducted over wire
  - phone/power/network (or radio stupidly enuf)
- 2. radiated as radio frequency as 2nd order effect (radio again …)
- not mutually exclusive
  - computer radio signals may be amplified by power circuits within a building

power/signal cable leaks

- if it's electronic or electrical it leaks
- we can however filter and attenuate both power supplies and data wires
- red/black physical separation
  - red equipment is isolated and may contain plaintext
  - black – talks to outside world
  - cipher machine does both (harder problem)
  - military may very well have separate wires

power analysis

- problem with smart cards is there is no room to add filtering equipment
- power supply may be controlled by adversary
- lots of info available by simply monitoring the power consumption
  - called power analysis or rail noise analysis
- if attacker understands the cipher, may be able to deduce key

leakage thru RF signals

- computers have clocks and may emit radio at different harmonics of the clock
- VDUs unless designed otherwise emit a weak TV signal
  - VHF or UHF radio signal
- ethernet/rs-232 cables emit signals
- one attack at 8 meters demonstrated on ATM machine in late 90s
- military grade TEMPEST equipment has not been available in the commercial sector

active attacks

- e.g., against keyboard
  - irradiate cable with radio wave at resonant frequency
  - due to nonlinear junction effect, keypress codes can now be read at 50..100 yards
  - one must encrypt the keyboard codes
- tempest virus
  - send virus to computer and have it capture and send info as radio

nonstop

- US military – exploiting RF emanations accidentally induced by nearby radio devices
- computer near mobile phone
  - so use mobile phone's radiations
- so the question becomes:
  - cell phone plus radar – which is relaying the information that you need to hide?

commercial exploitation

- radio station, car dealer, mall operators may have radio pickup gear
- to monitor what customers are listening to
- what about RFID radio frequency identification chip/s?
  - and detection of same

how serious should we take this stuff?

- threats to embassies are certainly real
  - shielding all electronic equipment etc is necessary
- govt. regulations about crypto may play a role
  - business can't have it, therefore govt. may be spying on business
- wireless data comm. exposure is real enough

"On the Internet, nobody knows you're a dog."

business?

- smartcards and cash machines are possible targets
- may be fruitful long term
  - minimal standards in non military realms
  - more and better wireless devices
  - more digital electronics
  - assumptions about protection distances that are wrong
  - software radio too

802.11 wireless

- 3 key ideas:
- 1. confine antenna propagation
- 2. consider use of crypto at whatever layer
  - L2 WPA-2, 802.1X with bulk crypto,
  - L3 IPSEC
  - L7 SSL(TLS), secure shell, tunnels
- 3. shielding
  - yes, chicken wire, metal in the walls

802.11 antennas

- 1. may be directional
  - consider side lobes though
  - doesn't have to be outside
- 2. may be OMNI-directional
- 3. may be patch antenna
  - some compromise between OMNI and directional
- in any case, you should test the reach
  - . at layer 1 with EM signal analysis equipment
  - . at layer 2-above with a sniffer on the same channel

faraday cage application?