Security and Privacy Issues of Wireless Technologies

Collin Mulliner
<mulliner[AT]cs.ucsb.edu>
http://www.cs.ucsb.edu/~mulliner/

Agenda

- Introduction
- Issues
- Technology specific issues
  - Wi-Fi
  - Bluetooth
  - RFID
  - Misc.
- Conclusions

Introduction

- Wireless technologies are part of our daily lives
- They already influence our social interaction
  - and will even more in the future
- We trust that they just work
  - and maybe you already have a bad day if they don't
- Are we aware that we use them all day long?
  - maybe most of the non-techy people aren't

The Wireless Medium

- The wireless medium is a shared resource
  - anyone, with the right equipment, can access it
    - walls, doors, security guards don't stop the radio waves
- You can see when other people are access it
  - other people see you
- Data send over wireless is public
  - anyone can see what you are doing
    - (we save encryption for later)

Where Wireless is used

- Home and Office
  - wireless access points for laptops or handhelds
- Commercial applications
  - infrastructure, hotspots, cash registers, etc...
- Personal usage
  - cell or smart phones, PDAs, cars, etc...

Personal Data

- What is personal
  - CC, SSN, phonebook, calendar, password, etc...
  - your daily routine
    - where do you go, what do you do, who do you know
- Where do you keep your personal data
  - PC, laptop, PDA, cellphone
- What data is somebody else keeping about you
  - where do they keep it?

Now Combine

- Your valuable data is wirelessly access able
- *Anyone* can access it, this means:
  - data theft / financial harm
  - privacy invasion
    - reading your email or Amazon orders
  - identity theft, your...
    - social security number
    - internet connection
    - phone number

Relax

Its not that bad!

Issues

- Wireless technology is
  - design for EaseOfUse
  - changing fast and continuously evolving
  - hard getting it right
- The average user just doesn't know
  - how and why

Safety

- Would you drive a car that is known for harming it's passengers?
  - its really easy to use, you don't have to walk
  - no need to adjust to the bus schedule
- Would you use a technology that is known for...
  - its really easy to use, you don't need to plug-in
  - no need to buy 100 cables and adapters
- You do both, just need to watch out for yourself

Technology Specifics

- Theory is done ... lets checkout the specifics
- Also the different technologies are somehow similar, they all have their own special problems
- The next slides cover
  - Wi-Fi
  - Bluetooth
  - RFID
  - and very briefly mobile com. systems and Clickers

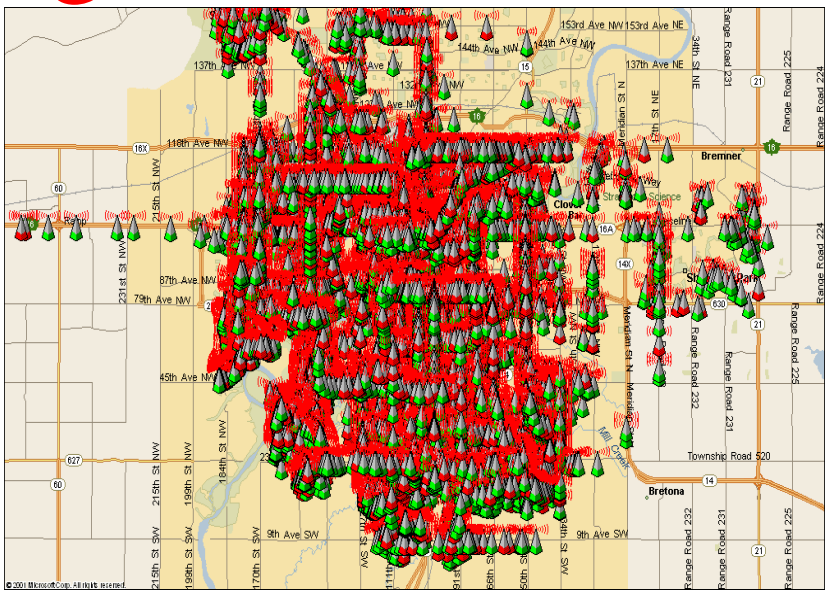
Wireless Lan/Wi-Fi (802.11)

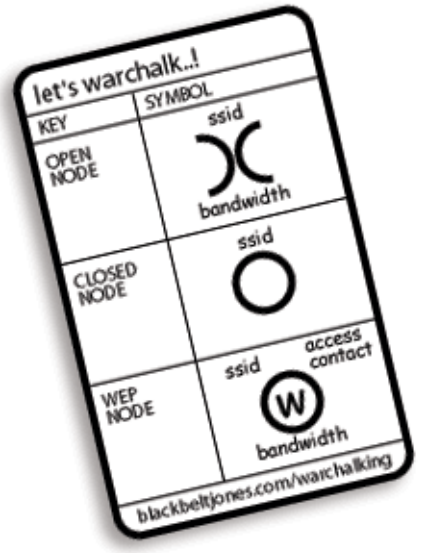
- Most popular wireless technology
  - not counting mobile phone technologies like GSM!
- Its been around for quite some time now
  - basically replaces wired networks
  - widely adopted for all kinds of things
- EaseOfUse principal
  - access points announce them self's to help the user
  - plug 'n play auto-configuration, it just works

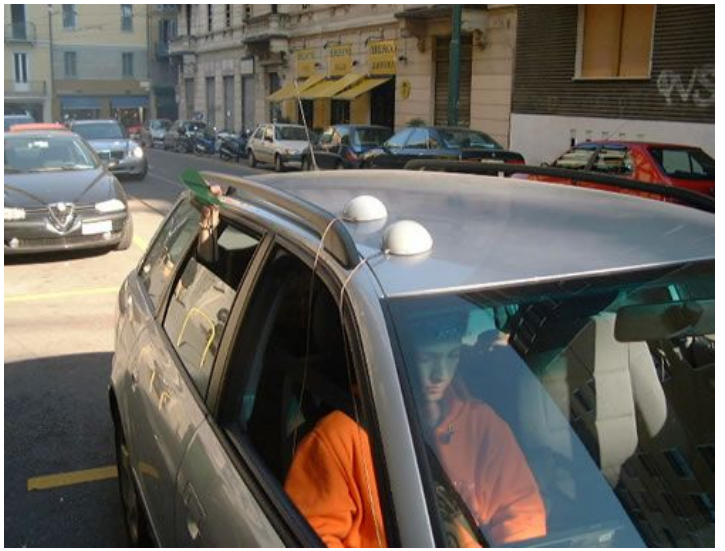
Wi-Fi cont.

- You're not the only one to see the access point announcing itself
  - everybody in range can use it (sometimes by accident)
- The whole EaseOfUse thing created a new sport or hobby called **WarDriving**
  - basically you drive around with a car packed with a laptop and a pile of wireless equipment to find and catalog access points

WarDriving


153rd Ave NW
153rd Ave NE
144th Ave NW
144th Ave NW
137th
137th Ave NE
118th Ave NW
215th St NW
87th Ave NW
79th Ave NW
45th Ave NW
184th St NW
199th St NW
215th St SW
199th St SW
179th St SW
9th Ave SW
Bremner
Bretona
Township Road 520
Range Road 232
Range Road 231
Range Road 225
Range Road 224
34th St NE


let's warchalk..!
KEY
SYMBOL
OPEN NODE
ssid
bandwidth
CLOSED NODE
ssid
WEP NODE
ssid
access contact
W
bandwidth
blackbeltjones.com/warchalking



WarDriving cont.

- Most wardrivers are friendly, they just want to
  - explore their neighborhood
  - have non-destructive/harmful fun
  - read *their* email
- Wardriving mostly not necessary anymore
  - way to many people run access points these days
  - just switch on wireless and you're connected

Wi-Fi Abuse

- *Open* access points can cause all sorts of problems and easily get you in to trouble
  - data theft
    - CC, SSN, other valuable data on your network
  - identity theft (committing crimes in your name)
    - fraud (eBay, etc...)
    - SPAM
  - privacy invasion
    - read your email or instant messages

Wi-Fi Abuse cont.

- Public hotspots are equally dangerous
  - profiling individuals using their hardware
  - directed attacks, you and your laptop are visible
    - executive lounge at airports, hotel lobbies, $tarBucks...
  - security is up to the user since lowlevel security mechanisms mostly don't work here
    - (more on the next slide)

Secure Wi-Fi

- Many protection mechanisms (thru encryption)
  - the *secure* versions of POP/SMTP/HTTP/...
  - for closed networks
    - WEP - Wired Equivalent Privacy (broken)
    - WPA - Wi-Fi Protected Access
  - for public networks
    - VPN - Virtual Privat Network (a cooperate thing)
- All in all its not that bad, but...
  - you're still track-able

Bluetooth

- Short range wireless technology
  - replaces cables and infrared
- Mostly used by *small* mobile devices
  - cell and smart phones, PDAs and laptops, etc...
- Typical applications are
  - dial-up networking using a cellphone
  - business card exchange using a cellphone or PDA
  - wireless headsets

Bluetooth cont.

- Point-to-point semantic other then Wi-Fi which is basically broadcasting
  - therefore sniffing Bluetooth is much harder and in fact can't be done with consumer equipment
- More secure by design, some features are:
  - can be set to a non visible mode
  - only respond to known devices
  - traffic encryption

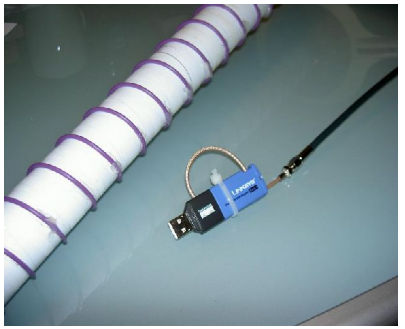
Bluetooth Bugs

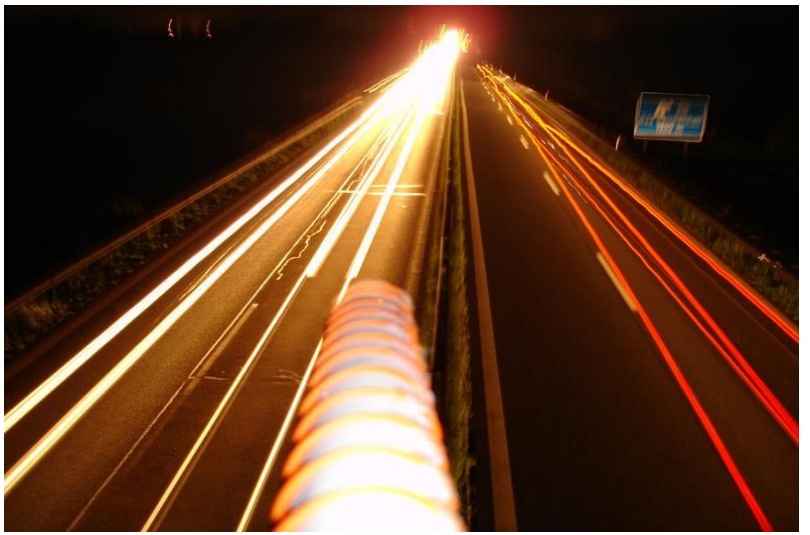
- Many implementation bugs in various devices
- Especially cellphones are affected
  - some bugs allow:
    - copying phonebook and calendar entries
    - initiating calls and sending text-messages
    - Denial of Service (DoS) attacks (phone becomes unusable)
    - special kind of wiretapping
      - using a phone or a hands-free car kit as a bug

Bluetooth WarDriving

- Apply what you have learned from WarDriving
  - not drive but walk or have a coffee and wait
- Supposed to be short range (10-100m)
  - same frequency as Wi-Fi, reuse Wi-Fi antennas
- A new hobby...

Bluetooth WarWaiting





Bluetooth Examples

- Copy phonebook at interesting events
  - Capitol Hill press conference
    - done in germany, got secret service internal phone numbers
- Social engineering
  - use names from copied phonebook to gain trust
- Tap wireless headsets of cars driving >80mph
  - you can also talk to the driver

Bluetooth Abuse

- Most Bluetooth devices are very personal
  - cellphone or PDA
- Can be abused to track and profile individuals
  - tracking done to proof feasibility (where is person X)
  - companies sell products to do this
- BlueSpam, spam via Bluetooth to your phone
  - again, companies sell products to do this

RFID

- RadioFrequencyIDentification
  - small tags/transponders which can be read wirelessly
    - by small we actually mean very small (post stamp or rice)
  - many different types
    - powerless/self powered
    - non/authenticated (encrypted) data transfer
    - readonly/writeonce-readmany/read-write
- Works just like anti-theft system stores have
  - electromagnetic field powers tag, tag responds

RFID cont.

- RFID is meant to be very short range (cm)
  - magnetic field strength, security, etc...
- Data stored on tags
  - GUID – Globally Unique Identifier (128bit number)
    - most common for very small passive tags
  - Anything else possible
    - cost, size and power consumption are the main constraints

RFID Usage

- Access Control / Authentication
  - security badge
  - passport / ID
- Item identification
  - customer cards
  - goods in warehouses (GUID)
    - not only pallets, every single item!
  - basically everything you can possibly think of

RFID Abuse Risks

- Tracking and spying
  - open system, readers are cheap and public available
  - tags are mostly not visible and unmarked
  - reading range can be extended using antennas
- Identity theft – tag duplication
  - low security applications (customer cards)

RFID / Proximity Card Cloner

Mobile Communication Systems

- Systems like: GSM, PCS, CDMA, UMTS, etc...
  - mostly secure against *cheap attacks*
  - a while ago some issues with GPRS, got fixed
- Maybe reliability and availability...
  - too many users in a certain area
    - I.V. during Halloween or New Years Eve
  - no total coverage
    - trip to the mountains or desert...

Classroom Clickers
(what I found on the net)

- Infrared based
  - tool found that claims to:
    - easily sniff and display *clicks*
    - spoof feedback (right/wrong)
- RF based
  - some interfere with Wi-Fi/Bluetooth (2.4Ghz band?)
    - maybe easy to DoS the classroom

Conclusions

- All the different technologies haven common security and privacy problems
  - each having it's special impact for the users
- New technologies are by nature more vulnerable
  - like wine, they need to age to become good
- In general its worse then you think it is
  - at the same time its not as bad as it sounds

End

Questions?