Tracking Prey in the Cyberforest

Bruce Potter gdead@shmoo.com
Brian Wotring brian@shmoo.com
The Ground Rules

• Don’t believe anything I say

• Daytime - Security consultant
  – “Beltway bandit” in Linthicum MD

• Night - Founder of the Shmoo Group, Capital Area Wireless Network, periodic author

• “You have no privacy, get over it” - Scott McNeely, CEO, Sun Microsystems
  – Technology advances are only going to make this more true
• **Goal:** Understand the how you can be tracked, minus the standard FUD
  – Think like the hunter for the next hour…

• What are location services
• Physical Tracking
• Logical Tracking
• The Union of the Two
• Explanation and Summary of Bluetooth tracking Demo
The Dangers of Wireless Networking....
How to Hunt

- Cover yourself in buck scent....
- Wireless - It’s hard to hide a transmitter
  - We’re becoming a wireless society
- Biometerics - It’s hard to hide who you really are
  - Though, it may be easier to be someone else
- Logical - It’s hard to hide the fact that you’re a freak
  - You leave a slimy trail all over cyberspace
How to Flee

- Non-repudiation
  - Oft misused term
  - Legal: You signed this document
  - Crypto: This key signed this file
  - The crypto definition doesn’t account for when the key was stolen, used under duress, etc…
    - Note “key” vs “you”… handy escape at times

- Technical countermeasures
  - Jamming, spoofing, lying

- Policy/politics
  - Kobe’s accuser’s text messages
  - Various wiretap laws
Wireless Techniques

- Why are you trying to find?
  - Infrastructure determining location of client
  - Client determining location
- What are you trying to find?
  - Can you trust the client?
  - Laptop, car, PDA, phone, person?
- Where are you?
  - Urban areas have advantages over rural areas
  - Vice Versa
- How accurate do you want to be?
Physical - Wireless Techniques

Angle of Arrival

- Angle of Arrival
- Infrastructure based
- Multiple sites determine the angle of the signal received from a radio
- "simple" trig calculates where the radio is
TDOA

• Time Difference of Arrival
• Infrastructure based
• HIGHLY sensitive clocks at each site determine when a signal is received
  – Light travels REAL fast
• Central host compares differences
  – Uses known location of sites with the difference in time of arrival to compute radio location
Physical - Wireless Techniques

GPS

- Client based
- Uses GPS constellations to determine location
- Companies such as SiRF ([www.sirf.com](http://www.sirf.com)) have created incredibly small GPS chips for integration into cell phones and cars
  - In a shocking number of phones and vehicles today
Physical - Wireless Techniques

Proximity Sensors

- VERY common for access control
  - Badging into a secured area
  - Often combined with other auth factors
  - Many vendors

- Useful in other contexts
  - Bluetooth tracking - place BT radios all over a building

- May be able to leverage existing infrastructure
  - Ex: use 802.11 access points (10 - 100m resolution)
  - Not very accurate, but close enough for access control and horseshoes?
Bluetooth

- One million Bluetooth radios shipped each week
  - Many folks don’t know they have them
- In everything from printers to PDA’s to phones to keyboards
- You may suspend your laptop, or turn off your 802.11 card, but BT tends to be on all the time
- NOT necessarily short range…
  - 1/2 of radios in Columbia MD CompUSA were class 1… just as powerful as a wifi radio
Wireless Techniques

Bluetooth vs. 802.11

- FHSS
- Pattern Restarts
- DSSS
Wireless Techniques

Technology Specific Problems - Bluetooth

- FHSS harder to “find”
  - Must align with hopping pattern
  - BT uses 1/2 the normal hop time to Jump Around
  - Still averages 2.5 to 10 secs to find known device

- Devices can be Discoverable
  - Respond to inquiry requests

- Devices can also be non-discoverable
  - Must be directly probed by MAC addr

- Little to no traffic for extended periods of time (esp in low power mode)
  - Cannot easily be listened to b/c receiver cannot sync on hopping pattern

- Sophisticated RF gear can find and intercept traffic
  - Currently no one can make a standard card do this
Originally a land-line based system for determining the location of a caller
  - Used by fire and medical personnel for emergencies

Expanded to include wireless callers
  - Phase I (complete) to provide 1st responders with the location of the cell site
  - Phase II (complete by 2005) to provide location of caller

Utilizes a combination of methods including GPS

Remarkably complicated
  - Need to interface with central office and Public Safety Answer point

Development funded by NCS
  - Gov’t Emerg Telecomm System
    - Wireless Priority Service
GM’s technology for providing various in-car services

- GPS based
- Transmits VIN, account number, make, model, and color with every car
- GM petitioning to exempt “in car telematics” from Phase II of E911
  - So, the ambulance won’t know where you are, but GM will...

- Powerful commercials...
Wireless IDS

- Using the location of the wireless LAN clients to determine if associations should be allowed
  - Conference room == good
  - Parking lot == bad
- Location awareness (ie: common sense) could play a huge role in the security of future wireless networks
- Newbury Network’s WiFi Watchdog
  - Not the cheapest thing, but one of the few options out there
RFID experiments

- Don’t hurt me
  - Controversial technology
  - Y’all read slashdot, right?
- Gillette’s SmartShelves
- WalMart product tracking (just launched)
- KSW-Microtec has RFID that can be sewn into clothes
- Where’s the authentication?
- Cost dropping rapidly…
Now Lego visitors can shoot their kids with an 802.11 tracking dart

Using a phone, determine location of your child at any point
  – Where’s the authentication?

Great for parents

Also takes the guess work out of which rides are the most popular, foods kids like to eat, etc..
  – I really want to see a realtime map of kids on a rollercoaster… all Matrix-y
Physiological Biometrics

- Physiological Biometrics - Static... should be the same every time
  - Fingerprint - technology getting cheaper by the day
    - iPaq’s with fingerprint scanners built in
  - Iris
    - Very accurate, but tied up license issues
  - Retina
  - Face
  - Voice?
Physical - Biometric Techniques

Behavioral Biometrics

- Biometrics that include a temporal factor
  - Keystroke dynamics
    - Sure you know the password, but do you know how it’s typed in?
  - Signature
  - Gait
  - Voice?
Finding Criminals @ Super Bowl

- I thought it was the players who are the criminals...
- Attendees at Super Bowl XXXV in Tampa were subjected to facial scanning without their knowledge
  - Compared against facial data of known criminals
  - 19 matches total, several were false positives, no major criminals found
Sir, do you have our bonus card?

Usually, you can’t misplace your fingerprint
  – Kroger, Thriftway testing biometric loyalty programs

Facial recognition et al in Vegas casinos

It wouldn’t be hard to do signature verification with all the touch pads running around…
  – Why not just track me using my credit card?
Overcoming Biometrics

- Gummi bears
  - http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/

- Pictures of a person’s face work almost as well as the real thing
  - http://www.theregister.co.uk/2002/05/23/biometric_sensors_beaten_senseless/

- Rip the thing off the wall and short circuit it

- Don’t give up your biometric data easily
  - BM is not fool proof, but repudiation may be tough nonetheless...
Spyware

- Software that lives on a PC that “phones home” to report on the user
- Often tied to shareware programs as a way for developers to get paid
- KaZaA (full of spyware) vs KaZaA Lite
- Code executes locally… can do all kinds of nasty stuff
  - Send back very personal info, change settings, etc..
- In a corporate environment, things get interesting
  - Potential HIPPA or other regulatory violations
Fighting Spyware

- Anti-spyware tools
  - Ad-Aware http://www.lavasoft.de/software/adaware/
- Or, good hosts file (black hole evildoers to 127.0.0.1)
- OR.....

Don’t install the software in the first place....
In short, an image/script loaded from a remote website

- Can be embedded in web pages, email, Word docs, etc...
- Typically - point to organization than the source document, 1x1 gifs are common

Source of www.example.com

```html
<html><head>Welcome to Example.com</head>
<body><h1>Welcome to Example.com</h1>
<img src=http://www.tracking.com/transparent.gif>
```

- Some browsers can be configured to only load content from domain in URL
- In email, unique ID can be added to request URL allowing individual identification
  - Reason #3451 why not to load images in HTML mail
• A lot can be determined about what you want based on your referrer

xx.yy.zz.bb ---- [27/Jun/2004:18:36:10 -0600] "GET /mail/fw1/jul01/msg00034.shtml HTTP/1.1" 200 11175 "http://www.google.com/search?hl=en&ie=UTF-8&q=printing+through+the+firewall&btnG=Google+Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)"

xx.yy.zz.aa ---- [27/Jun/2004:18:38:48 -0600] "GET /mail/cypherpunks/mar00/msg00019.shtml HTTP/1.1" 200 9387 "http://web.ask.com/web?qsrc=6&q=Free+Bomb+Making+Instructions&o=0" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
An Anonymous Existence

• Don’t load images, disable cookies, provide no refererrer info, change browser data
  – But most of the Interweb stops working right…

• Anonymous web/mail service
  – Mixmaster/mixminion - Mixmaster.sourceforge.net
  – Anonymizer.com
Aggregation is Fun

• One dataset is interesting
• Cross referencing is powerful
• GAO says 52 federal agencies had 199 active or planned data mining projects
  – 122 use personal information
• Not all uses were “evil”
  – 55 - Improving service
  – 17 - Managing HR
• Data mining goes on in the private sector as well
Role of an ISP

- ISP’s contain a great deal of personal information
  - Mail logs, connection logs, web sites, address, CC…
  - And the traffic, of course
- Logs can be accessed by external parties
  - RIAA going after P2P users
    - Verizon caused RIAA to take up “John Doe” offense
  - Criminal investigations can lead to packet capture…
Best Company Ever

• If Google bought an ISP and cell provider…
  – What’s the next number bigger than a google?
• AOL, Google, Walmart
  – Deal with so much data, they are defacto aggregators
    • Seriously, do I even need a bonus card… track me by my credit card
  – Laws keep them in check… in theory
  – Why do we trust companies (motivated by money) more than the government (motivated by servicing the taxpayer)?
Bluetooth Tracking Demo

- Two day exercise at Blackhat to track users
- Devices must be in discoverable mode
- Proximity based, not triangulation
- GPS doesn’t work in Caesars, so hokey “station” concept has to be used

Are you still reading these?
Data From last 2 days

- X devices found
- Y hits against the website
- <breakdown of devices found>
- Code can be downloaded from http://bluetooth.shmoo.com
Where to go from here?

• There is no stopping the technical ability to track us
• Controlling these issues is going to be a mix of:
  – Politics
  – Industry
  – Society
  – Technology
    • Technology will NOT be the savior…
• Keep a level head