



Radio Reconnaissance in Penetration Testing

“All Your RF Are Belong to Us”

By: Matt Neely

Presented: February 7th 2009 at ShmooCon



Radio Spectrum





I haz ur
frekwinses
I pwns u



- I am not a lawyer
- Know the wiretap laws and do not violate them
 - Some states require that both parties consent to a phone call being recorded
- Know the scanner laws for the state you are operating in, remember to check this **before** traveling out of state
- Make sure your activities are authorized in the written rules of engagement
- In most states it is legal to monitor any radio transmission as long as its not a telephone call or pager traffic



Illegal Activity to Avoid

- I am still not a lawyer.
- Additional activities to avoid:
 - Jamming transmissions
 - Decoding pager traffic
 - Illegally transmitting



Finding Frequencies to Monitor

PROFILING A TARGET



- Before arriving on site try to determine as much information as possible such as:
 - In house or contract guard force
 - Frequencies they are licensed to use
 - Make and model of equipment they use



- Search for:
 - “Company name” scanner
 - “Company name” frequency
 - “Company name” guard frequency
 - “Company name” Mhz
 - Look for press releases from radio manufactures and reseller regarding the target
 - Look for press releases from guard outsourcing companies talking about contracts with the target company
 - Etc...



- <http://www.radioreference.com/apps/db/>
 - Free part of the site containing a wealth of information
- <http://www.nationalradiodata.com/>
 - FCC database search
 - \$29 year
- <http://www.perconcorp.com/>
 - FCC database search
 - Paid site – custom rates

Example: Off Site Profiling

Hotels Scanner Frequencies and Radio Frequency Reference - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.radioreference.com/apps/db/?aid=4080

wardman park scan

Most Visited Getting Started Latest Headlines

452.73750 457.73750 WQAF804 RM 167.9 PL Security FMI Security

Marriott Metro Center ▶

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
466.68750	WQCT918	M	123.0 PL		Engineering	FM	

Marriott Wardman Park ▶

Frequency	Input	Type	Tone	Alpha Tag	Description	Mode	Tag
464.57500	469.57500	RM	565 DPL		Security	FM	Security

Omni Shoreham ▶

Frequency	Input	License	Type	Tone	Alpha Tag	Description	Mode	Tag
464.35000	469.35000	WPCZ551	RM	606 DPL		Banquet/Convention Services?	FM	
464.52500	469.52500	WPCZ551	RM	351 DPL		Engineering (also used by Housekeeping?)	FM	
464.77500	469.77500	WPCZ551	RM	74.4 PL		Security	FM	Security

One Washington Circle ▶

Frequency	Type	Tone	Alpha Tag	Description	Mode	Tag
-----------	------	------	-----------	-------------	------	-----

Done



On-Site Profiling – Frequency Counters

- Displays the frequency of the strongest “near field” signal
- Can quickly identify the transmit frequency of a radio
- Problems:
 - Can have problems in signal rich urban areas
 - Only locks onto very strong signals
- Recommend: Optoelectronic Scout





- In the field:
 - Try to identify make and model of radios
 - Note the length and type of antenna used
 - Do all targets use the same radio or a mix?
- Use the information gathered above to determine:
 - Frequency range
 - Features of the radio such as digital, trunk and encryption support
- BatLabs (www.batlabs.com) is a great source of information on Motorola radios



On Site Profiling – Common Frequency Ranges

- Labor intensive process
- Common frequencies
 - FRS, GMRS and “Dot” frequencies
- Common ranges
 - Business
 - 150 – 174 MHz
 - 420 – 425 MHz
 - 450 – 470 MHz
 - 851 – 866 MHz
 - Cordless telephones and headsets (Make sure this is in scope and legal!)
 - 43.7– 50 MHz
 - 902 – 928 MHz
 - 2400 – 2483.5 MHz – Most are digital



HARDWARE



Selecting a Scanners

- Do not need a fancy or expensive scanner to gather valuable information
- Must have features:
 - Triple conversion
 - Receives 900 MHz
- Nice to have features:
 - Alpha numeric memory
 - PC programmable
 - Trunk tracking
 - Capable of decoding APCO P25 (Digital) traffic
 - Discriminator out
 - PC controllable
- Specialized features
 - Receives frequencies over 1.8 GHz
 - IF output



Recommended Scanners

AOR 8200
~\$620



Uniden Bearcat BCD396T
~\$500



Uniden Bearcat SC230
~\$180





If You Have Unlimited Budget

- 0.005-3335 MHz coverage
- Quadruple conversion
- Very sensitive and selective receiver
- Spectrum scope
- Build in video decoding
- FSK modulator and decoder
- ~\$14,000



Image provided by Icom of America



- Good antenna can make the difference between hearing and missing a signal
- Recommended antennas
 - Flexible “rubber duck”
 - Telescoping whip
 - Magnetic-mount mobile
 - Frequency specific antennas
 - Max Systems 800 Mhz discone





Recommended Accessories



- Scout frequency counter
- Recording equipment
- Camera
- DTMF decoder
- Video convertor



REAL WORLD EXAMPLES



- Scenario: Physical penetration test of a casino
- Off-site profiling:
 - Discovered frequency for the radio link between casino security and state police from forum postings
- Started monitoring the radio link between the casino and state police the night we arrived in town
 - Casino dispatchers often chatted with the police
 - Learned names of the 2nd and 3rd shift dispatchers



Case Study #1

- On-site profiling:
 - Visually identified handheld radios
 - Appeared to be Motorola HT Pro Series, most likely GP-338
 - Operate in 29.7-42, 35-50, 136-174 and 403-470 MHz
 - Do not support encryption or trunking
 - Short antenna suggested target radios operate in 136-174 or 403-470 MHz range
 - Carried the Scout through hotel and gaming floor

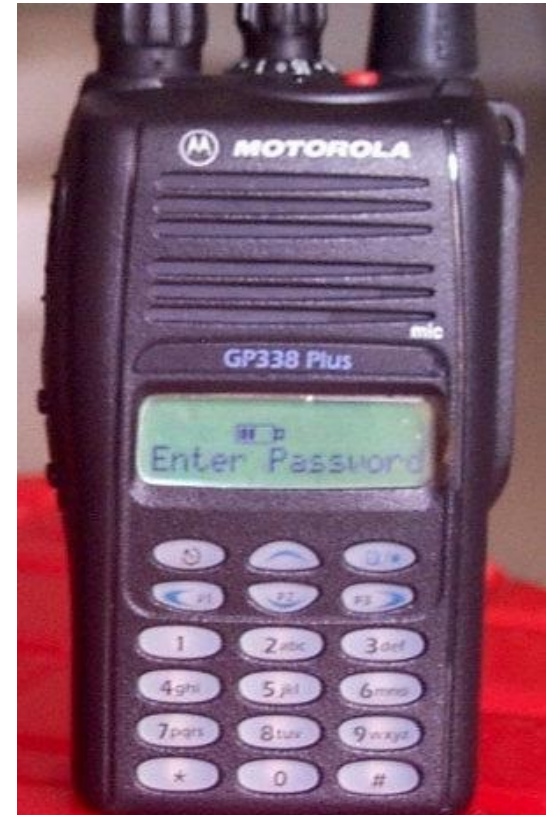


Image provided by BatLabs.com



- In the car: pulled frequencies from the Scout and noted those in the 136-174 and 403-407 MHz range
- Programmed relevant frequencies into scanner and listened
- We heard:
 - General chatter
 - Guards going on and off shift
- We learned:
 - Lingo
 - Guard names
 - When shift changes occur
 - Schedule and locations of guards doing rounds



- Scenario: Internal penetration test against insurance provider
 - While being escorted through the building noticed a number of wireless headsets
 - Requested permission to add into scope of engagement monitoring conversations over headsets
- Permission granted: started scanning ranges commonly used by headsets
 - Found several dozen headsets in use in the 902-928 MHz range
 - Used signal strength and geographic information to determine which headsets were located inside the target's building (!)
- Started monitoring traffic



Case Study #2

- We heard:
 - Many phone calls
 - Lots of helpdesk calls
 - Employees checking voicemail
 - Conversations even when the phone was hung up
- We learned:
 - Passwords from helpdesk calls
 - PII used to reset passwords
 - Voicemail passwords, recovered using a DTMF decoder





- VOIP enabled radio dispatch systems
- Software defined radios





- Test your equipment – Make sure headsets and cordless phones are secure
- Check your facility for unencrypted radio traffic
- Only use encrypted cordless phone and headset
 - DECT may not count as encrypted
- Consider switching to digital or encrypted radios
- Train guards to be aware that what is said on the radio is public



CATS : ALL YOUR RF ARE BELONG
TO US.



CAPTAIN: FOR GREAT SECURITY
JUSTICE.//



More Info:

<http://www.securestate.com>

<http://www.matthewneely.com/blog/>

CAPTAIN: WHAT YOU SAY //