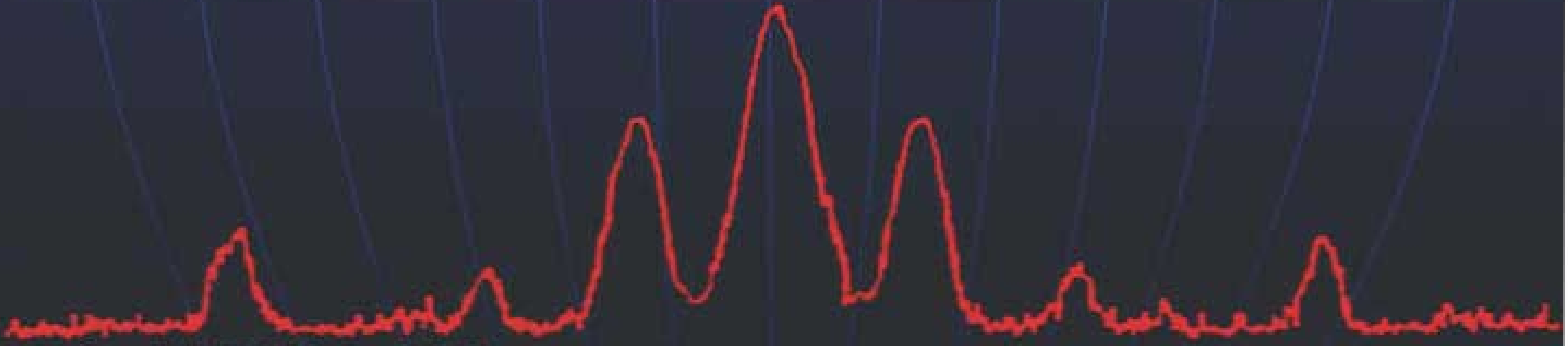
Cordless Phones
Security Threat Profile

2009



Cordless Telephones

Telephone Eavesdropping Risk

James M. Atkinson

Granite Island Group

www.tscm.com

Speaker Contact

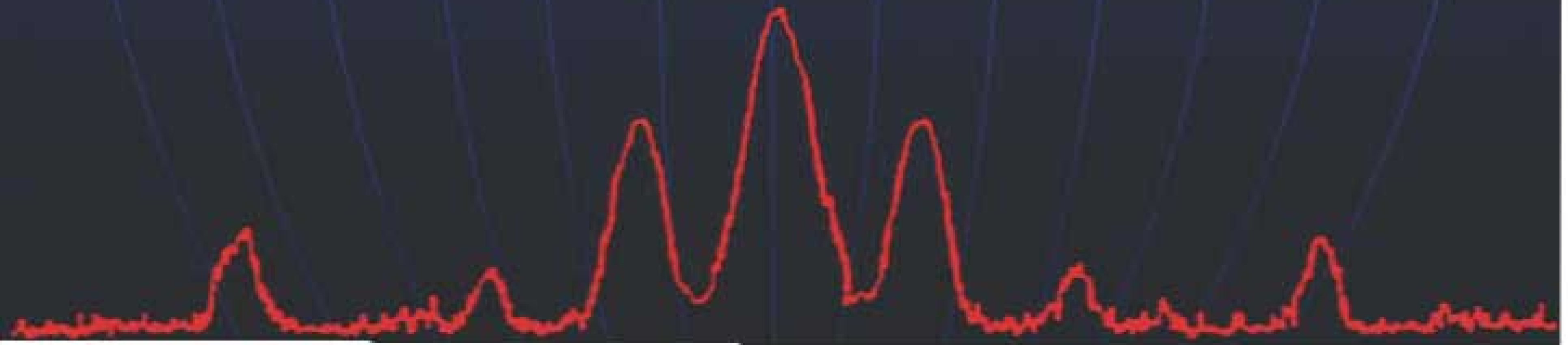
James M. Atkinson
www.tscm.com

jmatk@tscm.com
(978) 546-3803

http://groups.google.com/group/TSCM-L2006

www.linkedin.com/in/jamesmatkinson

www.tscm.com



Kill Your Cordless Phone

It’s Not Worth the Risk

Jim’s Cardinal Rule

If it has an Antenna,
it is Not Secure™

This is about the **Risk** of Cordless Phone Eavesdropping

Not a lesson on how to Eavesdrop on Cordless Phones

The Elegant Instrument

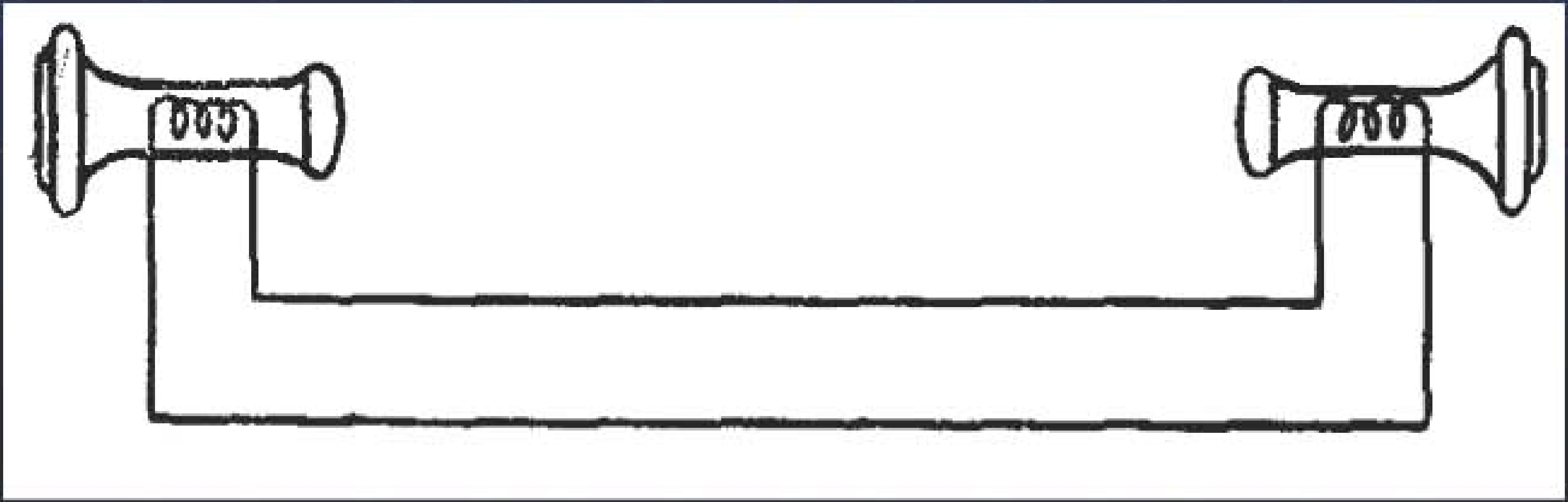
The telephone instrument is one of the most elegant, and carefully designed of all electronic devices on Earth.

They are also one of the Easiest and <u>Most Common Things</u> To Turn Into Bugs or Eavesdropping Devices

Telephone Vulnerability Points

Overly Simplified Telephone Circuit

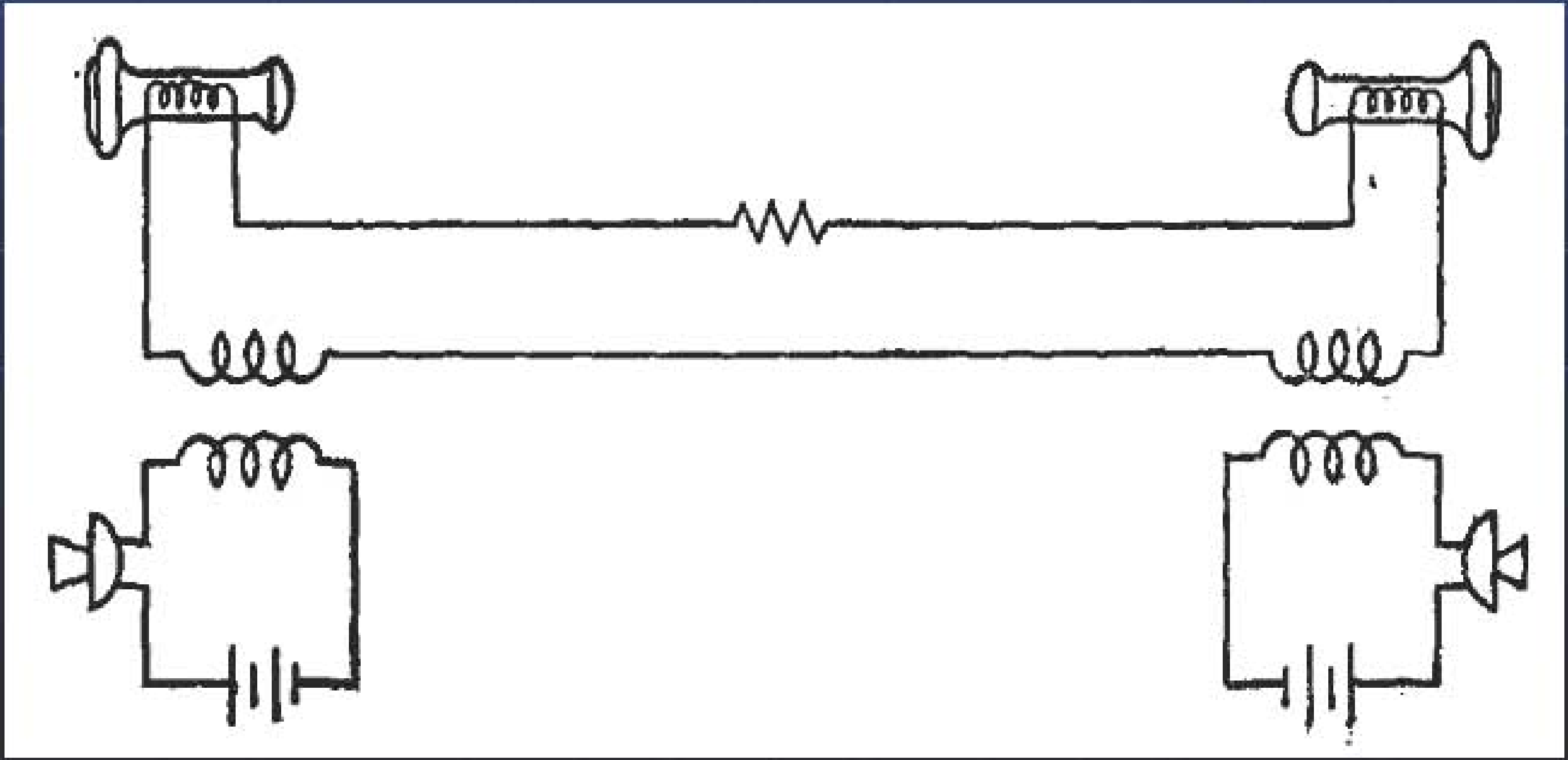
(No Battery Circuit – 2 transducers/inductors)



Telephone Vulnerability Points

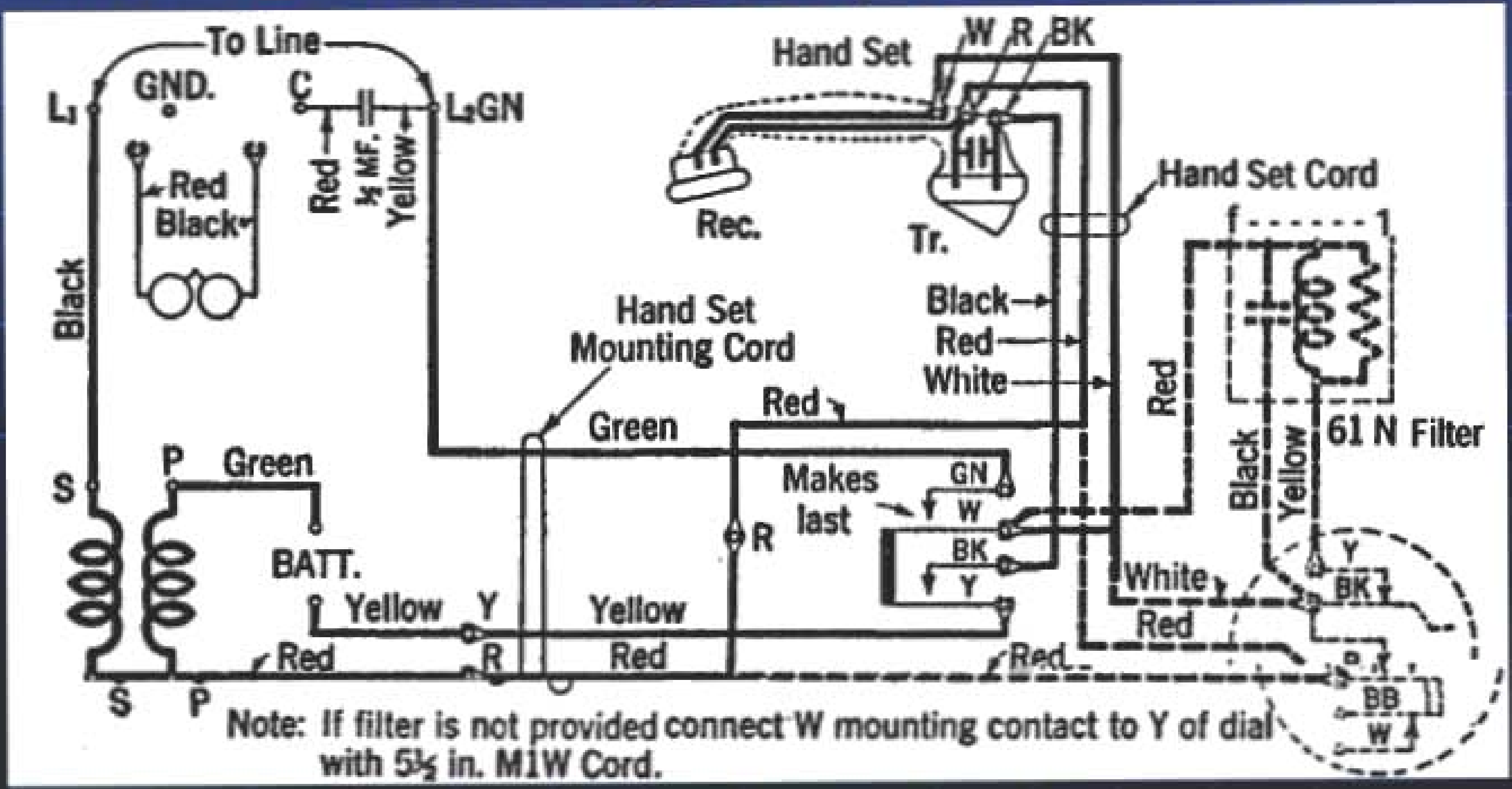
Less Simplified Telephone Circuit

(Local Battery Circuit – 4 transducers, 6 inductors)



Telephone Vulnerability Points

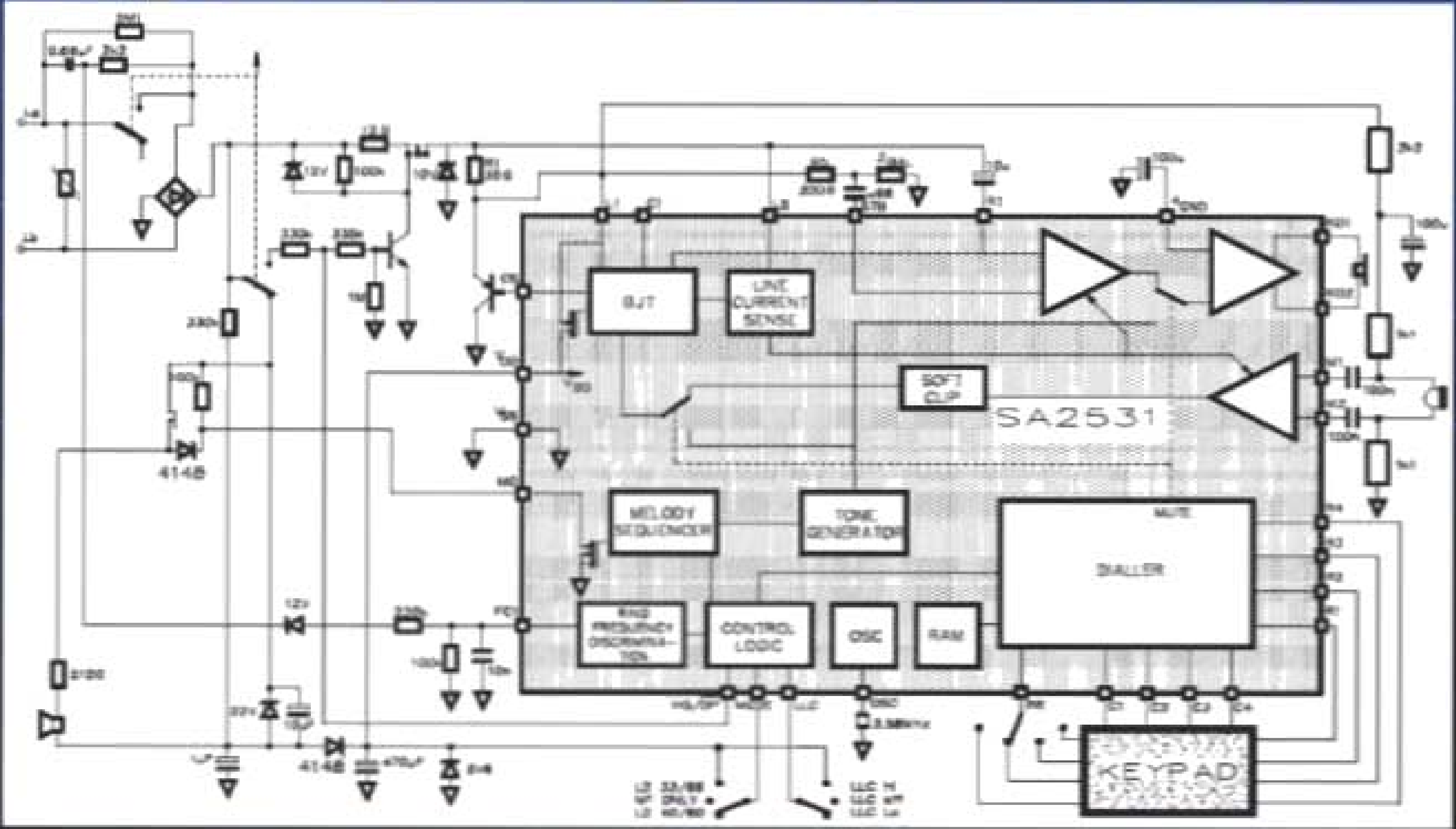
Old WECO Analog Telephone Circuit



Note: If filter is not provided connect W mounting contact to Y of dial with 5½ in. M1W Cord.

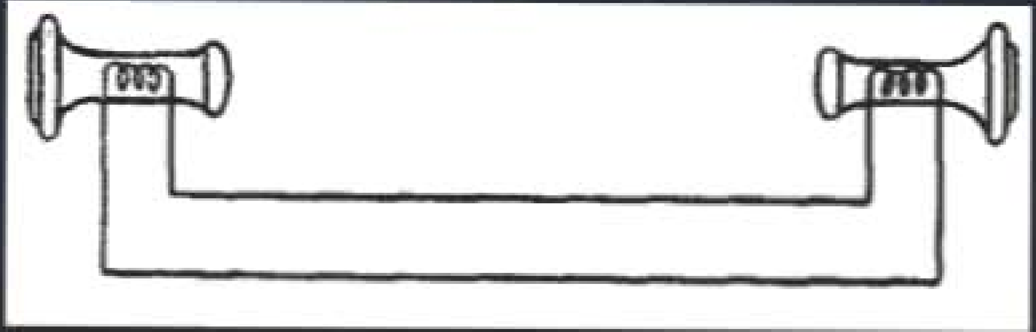
Telephone Vulnerability Points

Single Chip Analog Telephone Circuit



Telephone Vulnerability Points

1. Instrument ← Topic of this Presentation
2. Local Distribution/In-House Wiring
3. Local Switch/PBX
4. Demarcation/Network Interface
5. Transmission
6. Switching Systems



Telephone Vulnerability Points

1. Cordless Phones Provide More Attack Surface then a Hardwired Phone

2. Many People are Totally Clueless About the Risk of Cordless Phones

3. How Many Cordless Phones Do You Have In Your Life?

Brief History of Cordless Phones

- Invented by George Sweigert
  - World War II Radio Operator
    - Injured During War
  - Radio Controlled Telephone Coupler
  - Submitted Patent: May 2, 1966, US 3,449,750
  - Invented Full Duplex Radio Operation
  - Full Remote Control of Phone
    - Used a Relay To Activate and Release Phone
    - Parts From A Washing Machine
  - Acoustic Coupling, Not Direct Connection
    - Direct Coupling Into Line Came Later

Brief History of Cordless Phones

1969 Initial Cordless Phones Sold

1972 WECO Markets Cordless Phone

1980 Sony Cordless Phone Chip Sets

1984 AT&T/WECO Break Up

1984+ Cordless Phones Gain Popularity

Average Business Instrument

A Spies Best Friend

Average Cordless Phone

Also, a Spies Best Friend

FCC Definition

- **47 CFR § 15.3 Definitions**
  (j) *Cordless telephone system*

  - A system consisting of two transceivers, one a base station that connects to the public switched telephone network and the other a mobile handset unit that communicates directly with the base station.

  - Transmissions from the mobile unit are received by the base station and then placed on the public switched telephone network. Information received from the switched telephone network is transmitted by the base station to the mobile unit.

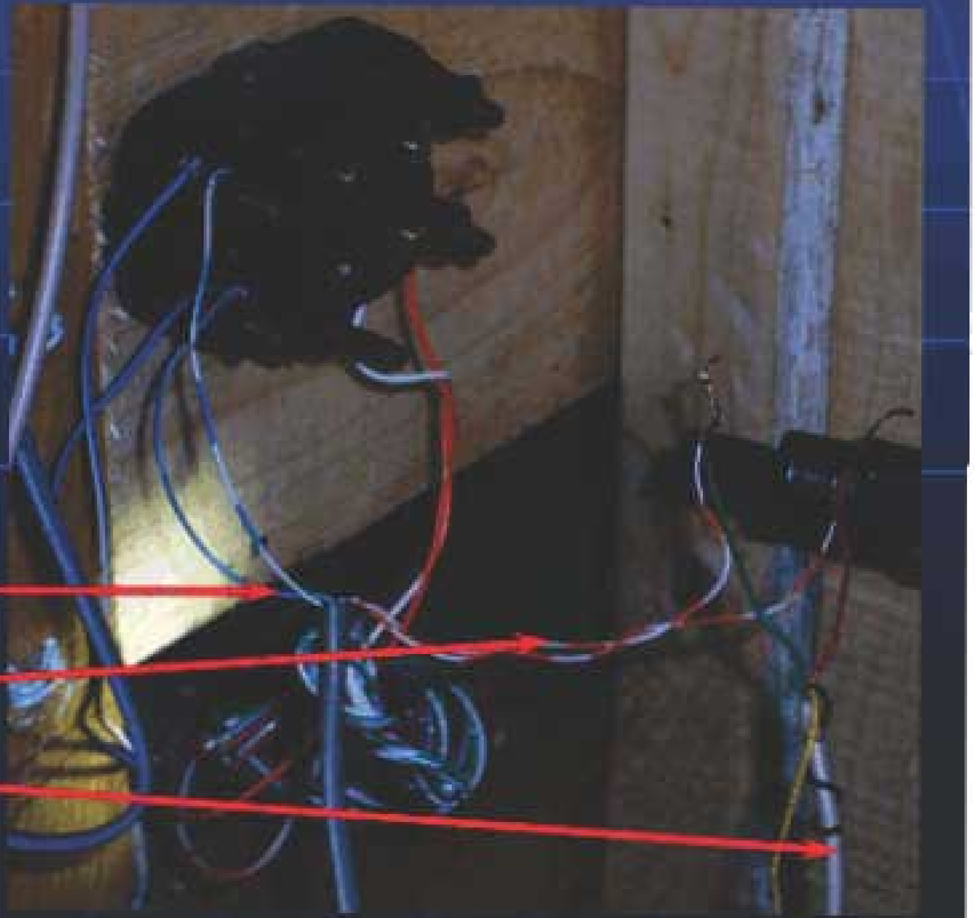
Hardwired vs. Cordless Phone Tap

Hardwired	**Cordless**
• Wires Usually Lead to Eavesdropper	• No Wires to Eavesdropper
• Requires Some Level of Physical Access	• No Physical Access Required
• Huge Evidence Trail	• Minimal Evidence Trail
• Time Consuming, but not Expensive to Detect Eavesdropping	• Time Consuming, and Expensive to Detect Eavesdropping

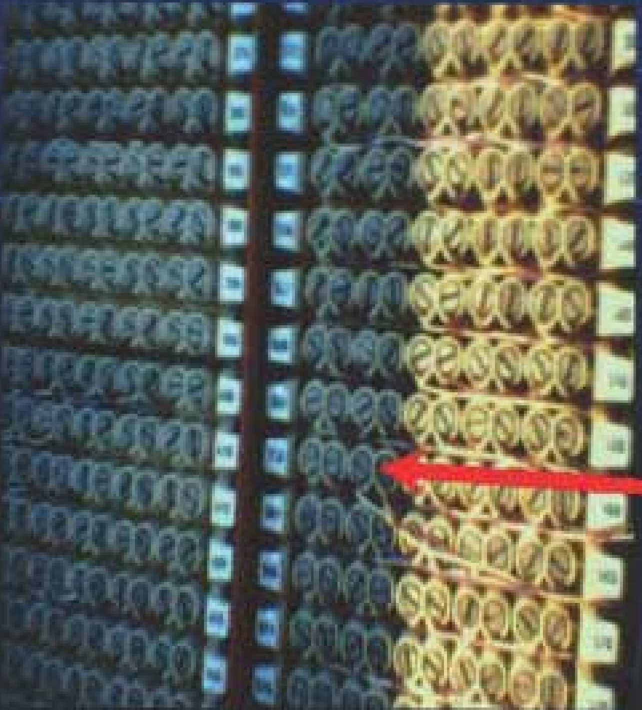
Typical Hardwired Wiretapping

Twisted Connections

1. 2nd Pair Exploit
2. Microphone
3. Patch Cable
4. Tape Recorder
5. RS Job
   - BL-WH - OK
   - OR-WH – Bad
   - Grey – to SPY



Hardwired Wiretap



Tapped
Pair 557

Disneyland for Eavesdroppers

- No Doors Locked
- No Alarms Present
- No Encryption

- Everything Wide Open

- Physical Access is Required

- Lots of Physical and Electronic Evidence

Picture of Cordless Phone Eavesdropping

"The Sound of One Hand Clapping"

Cordless Phone

1. Costs Under $20
2. Zero Security
3. 4 Primary Bands
4. RS Scanners
5. Really Bad News
6. Self Bugging
7. Clueless User

Cordless Phone Eavesdropping

- Catching the Spy
  - Spy Hunter Looks for
    - Equipment the Eavesdropper is Using
      - Intermediate Frequency Leakage
      - Mixer Circuit Leakage

Spy vs. Spy vs. Spy

Cordless Phone Eavesdropping

- Eavesdropper Complain:
  - Not Fair, that They Got Caught
    - The Spy Hunter Measured:
      - Scanner from 900 feet away
      - Scanner Listening to Neighbors Cordless Calls
      - Victim 75 feet Away from Eavesdropper
      - Spy Hunter Measuring, But Not Eavesdropping

Spy vs. Spy vs. Spy

Cordless Phone

1. Defense Industry
2. Zero Security
3. 900 MHz, Analog
4. Board Room Secrets
5. Self Bugging
6. Inside Spy
7. Transmitting Over the Air All the Time

Auditing Telephone Instruments

- What Kind of Phones
- "Soft Under-Belly"
- What Should It Normally Do
  - Is It a Risk?
  - Is It a Threat?
  - Hostile Manipulation?

Feature, Hazard, or Risk?

Technical Details

Where is the Attack Surface?

Cordless Phone Frequencies

Seven (7) Officially Allocated USA Bands

1.7 MHz	(allocated pre-1976)
27 MHz	(allocated in 1980)
43–50 MHz	(allocated in 1986)
902–928 MHz	(allocated in 1990)
1880–1900 MHz	(DECT, non-US usage)
1920-1930 MHz	(DECT, allocated 2005)
2.4 GHz	(allocated in 1998)
5.8 GHz	(allocated in 2003)

Cordless Phone Frequencies

1.7 MHz Band

- 1974 – 1986 era
  - Heavy Ferrite Bar Antenna
  - Huge Battery, Short Life
  - AM Modulated
  - Massive Interference
  - Often Illegal Power Levels
  - Banned by Phone Company
  - Unless you rented a WECO unit from them
  - Very Congested Spectrum Area
  - Phased Out in 1984
  - Your Parents Cordless Phone (or grand parents)

Cordless Phone Frequencies

27 MHz Band

- 1980 – 1986 era
  - Basically a Two Channel CB Radio
  - Long Telescoping Antenna
  - Huge Battery, Little Life
  - AM Modulated
  - Massive Interference
  - Often Illegal, 5 watt+
  - Very Congested Spectrum Area
  - Often Paired with 1.7 MHz
  - Huge $$$ Long Distance Bills
  - Phased Out in 1984
  - Your Parents Cordless Phone (or grand parents)

Cordless Phone Frequencies

43-50 MHz Channels

#	Base	Handset
1	43.720	48.760
2	43.740	48.840
3	43.820	48.860
4	43.840	48.920
5	43.920	49.020
6	43.960	49.080
7	44.120	49.100
8	44.160	49.160
9	44.180	49.200
10	44.200	49.240
11	44.320	49.280
12	44.360	49.360
13	44.400	49.400
14	44.460	49.460
15	44.480	49.500
16	46.610	49.670
17	46.630	49.845
18	46.670	49.860
19	46.710	49.770
20	46.730	49.875
21	46.770	49.830
22	46.830	49.890
23	46.870	49.930
24	46.930	49.990
25	46.970	49.970

- 1984 to Present
- Often Large Antenna
- Very Congested Spectrum Area
- Being Phased out in Favor of 900 MHz Band

Cordless Phone Frequencies

902-928 MHz ISM Band

- 1990 – Present Era
  - Short Antenna, 6-8”
  - Spectrum Congested
  - Extremely Cheap NFM Modulation
  - Single Chip Solutions
  - Decent Distances
  - Usually FM Modulation
  - Poor Choice for Digital Modulation
  - Sometimes FHSS or DSSS
  - Originally $400 - $500 for a 900 MHz Phone
  - Did Not Become Cost Effective Until Prices Dropped
  - <$150 per System was the Breaking Point
  - Now <$20 per system

Cordless Phone Frequencies

DECT - Digital Enhanced Cordless Telecommunications

- 2005(U.S.) – Present Era
  - 1880-1900 MHz (DECT, non-US usage)
  - 1920-1930 MHz (DECT, allocated 2005)

  - Internal Antenna
  - Only 10 MHz of Spectrum Allocated in U.S.
  - Congested, but Digital Signal Optimizes Spectrum

  - GFSK Modulation (1.152 Mbit/Sec)
  - International Standard
  - Very Cheap Due to Huge Quantities Being Made
  - Extended Range, 1000+ ft common
  - Long Battery Life

Cordless Phone Frequencies

2.4 GHz ISM Band

- 1998 – Present
  - 2.4–2.483 GHz
  - Usually Internal Antenna
  - Congested Band
  - Cheap, Consumer Grade
  - Good Choice for Digital Modulation
  - Digital and Analog Hybrids or SS
  - Could be FM Modulated
  - Could be paired with 900 MHz
  - 802.11 Interference Issues
    - Becoming Less Popular Due to WLAN and BT Issues

Cordless Phone Frequencies

5.8 GHz ISM Band

- 2003 – Present
  - 5.725 – 5.850 GHz
  - Internal Antenna
  - Uncongested Band (for now)
  - Cheap, Consumer Grade
  - Extremely Bad Signal Propagation
  - Digital and Analog Hybrids or SS
  - Digital Modulation is Pricey
  - Could Be, Often Is FM Modulated
  - Could be paired with 2.4 GHz
  - 802.11 Interference Issues

Cordless Phone Frequencies

European and Asian Cordless Phones

- Illegal to sell or use in the US
- Not FCC Approved
- Frequency Ranges
  - 864.1 – 868.1 MHz
  - 885 – 887 MHz
  - 930 – 932 MHz
  - 959 – 960 MHz
- Similar is size, function, features, cost, and appearance as legal 900 MHz Units

Cordless Phone Frequencies

Asian PHS "Handy Phones"

- Illegal to sell or use in the US
- Not FCC Approved
- Frequency Range
  - 1895 – 1906.1 MHz
- Third Generation Cordless Phone
- Similar Operation as Cell Phones

Cordless Phone Frequencies

Japanese 254/380 MHz Phones

- Illegal to sell or use in the US
- Not FCC Approved
- Frequency Ranges
  - 253.85 – 255 MHz
  - 380.2 – 381.325 MHz
- Paired Frequencies
- US Military Hunts Abusers

Cordless Phone Modulation

- Used to Be Amplitude Modulation
  - 1.7 and 27 MHz
    - Not Practical
    - Except on Shortwave Bands
    - Very Limited Channels (10 maybe)

Cordless Phone Modulation

- Narrow Band Frequency Modulation
  - 43-50 MHz
  - 900 MHz
  - 2.4 GHz
  - 5.8 GHz
    - **Extremely Cheap** to Do
    - Ineffective Use of Spectrum
    - Huge Amount of Wasted Bandwidth

Cordless Phone Modulation

- Typical NFM Modulation

Cordless Phone Modulation

- Spread Spectrum
  - Needs Bandwidth
    - Frequency Hopping
    - Direct Sequence
      - Signal In The Noise (Pseudo Noise Actually)
      - Very Efficient Use of Spectrum
      - Code Domain Modulation
  - Shared Channels
  - Low Level Privacy

Attack Surface

The Fancier the Cordless phone, the More Attack Surface it Provides the Eavesdropper

Attack Surface

Digital Control “Features”

  - Intercom
  - Paging
  - Three Way Calling
  - Listen-In
  - Barge-In

- Base or Remotes Can Seize Control

FCC Security Requirements

- **47 CFR § 15.214 Cordless Telephones**
  - (d) Cordless telephones shall incorporate circuitry which makes use of a digital security code to provide protection against **unintentional access** to the public switched telephone network by the base unit and **unintentional ringing** by the handset. These functions shall operate such that each access of the telephone network or ringing of the handset is preceded by the transmission of a **code word**.
  - Access to the telephone network shall occur only if the code transmitted by the handset matches code set in the base unit.
  - Similarly, ringing of the handset shall occur only if the code transmitted by the base unit matches the code set in the handset.
  - The security code required by this section may also be employed to perform other communications functions, such as providing telephone billing information. This security code system is to operate in accordance with the following provisions.
    - (1) There must be provision for at least **256 possible discrete digital codes**. Factory-set codes must be continuously varied over at least 256 possible codes as each telephone is manufactured. The codes may be varied either randomly, sequentially, or using another systematic procedure.
    - (2) Manufacturers must use one of the following approaches for facilitating variation in the geographic distribution of individual security codes:
      - (i) Provide a means for the user to readily select from among at least 256 possible discrete digital codes. The cordless telephone shall be either in a non-operable mode after manufacture until the user selects a security code or the manufacturer must continuously vary the initial security code as each telephone is produced.
      - (ii) Provide a fixed code that is continuously varied among at least 256 discrete digital codes as each telephone is manufactured.
      - (iii) Provide a means for the cordless telephone to automatically select a different code from among at least 256 possible discrete digital codes each time it is activated.
      - (iv) It is permissible to provide combinations of fixed, automatic, and user selectable coding provided the above criteria are met.
    - (3) A statement of the means and procedures used to achieve the required protection shall be provided in any application for equipment authorization of a cordless telephone
    - Blah, Blah, Blah... Blah, Blah, Blah

What does all of this really mean?

FCC Security Requirements

47 CFR § 15.214 Cordless Telephones

Bottom Line:

1) Zero Privacy
2) Minimal 8-bit Security
3) Controls Accidental Access
4) Illusions of Privacy
5) It is a Door Knob, Not a Lock

Access Security

- Small Number of Access Codes
- As few as 8-bits, could be hundreds
- Not Actual Security
- Just Minor Traffic Control
- Keeps the Neighbors Off “Your Line”
- Is Not Encryption

Access Security

- False and Misleading Advertising
  - "56 Bit Security"
    - Really Means 56 bit **Access Code**
      - **1,000,000 Private Digital Security Codes**
    - Zero Actual Encryption
    - Just FM Modulation
    - RS Scanner Vulnerable
      - Panasonic KX-TC2100
      - 46/49 MHz

Transmission Security

- Not Practical on Consumer Devices
  - Requires Expensive Parts
  - Signal Bandwidth Issues

- Digital Modulation Provides Limited, but not Good Privacy

- Even Spread Spectrum and Frequency Hopping is not Private
  - The hopping codes, algorithms, and patterns are widely known and openly published

Interception Basics

- Base Station is Usually More Powerful then Mobile (just like with cell phones)
- Uplink and Downlink May or May Not Even Be Within Same Band
  - Remote = 910.5 MHz
  - Base = 2419.75 MHz
- Often Cheaper to Stay Within Band
  - Remote = 904 MHz
  - Base = 918 MHz

Interception Basics

43-50 MHz Channels

#	Base	Handset
1	43.720	48.760
2	43.740	48.840
3	43.820	48.860
4	43.840	48.920
5	43.920	49.020
6	43.960	49.080
7	44.120	49.100
8	44.160	49.160
9	44.180	49.200
10	44.200	49.240
11	44.320	49.280
12	44.360	49.360
13	44.400	49.400
14	44.460	49.460
15	44.480	49.500
16	46.610	49.670
17	46.630	49.845
18	46.670	49.860
19	46.710	49.770
20	46.730	49.875
21	46.770	49.830
22	46.830	49.890
23	46.870	49.930
24	46.930	49.990
25	46.970	49.970

- Two Cheap $50 Radio Shack Scanners
  - Handset Dedicated
  - Base Dedicated
- 25 Channels Each
- Radio Shack Pro-82
  - 200 Channel
  - PN 20-315
  - 29-54 MHz

Interception Basics

- Base Station and Mobile Must Be Isolated in Free Space at Higher Frequencies

- Eavesdropper Points Interception Antenna at Targeted Base and Mobile

Interception Basics

- Eavesdropper Proximity To Target
  - To Within a Few Hundred Feet
- The Spy Can Use Cheap Equipment
- Distance Increases Cost
- Distance Complicates Methods

Interception Basics

Radio Shack or Wal-Mart Scanners

- <$150 Total Investment
- Intercept and Demodulate at 900 MHz
- 100 Feet Away (Maybe), Rubber Ducky
- 300+ Feet, External Antenna

Interception Basics

Mid Range Scanners

- <$600 Total Investment
- Intercept and Demodulate at 900 MHz
- 200-500 Feet Away, Rubber Ducky
- 1000+ Feet, External Antenna

Interception Basics

High End Receivers

- >$2400 Total Investment
- Intercept and Demodulate at 900 MHz
- 300-1200 Feet Away, Rubber Ducky
- 3000+ Feet, External Antenna
- Antenna is High Mounted on Mast

Interception Basics

High End "Purpose Built" System

- >$10,000 Total Investment
- Intercept and Demodulate at 900 MHz
- 6000+ Feet, External Antenna
- Antenna on Mast, and Directional

Analog Cordless Phones

- Virtual Zero Security
- Usually Zero Encryption
- Narrow FM Modulated Signal
- Tough Not to Trip Over Signal
- Two Signals on Spectrum

Intercepting Analog

- As simple as $79 Radio Shack Police Scanner

- As complex as a $40,000 Pro-Grade Receiver

Intercepting Analog

- Identify Band "Edges"
- Program into Scanner in Seek Mode
  - i.e.: 902 – 928 MHz
- Set Steps to <¼ Expected Signal BW
  - 2.5 kHz for a 10 kHz BW
  - Smaller is better, but slower
- Adjust for Best Audio
  - Use AFC and AGC
- Find the "Other Half" of Signal
  - Second Scanner

Intercepting Analog

An amateur eavesdropper may only have a single cheap receiver to follow multiple signals

- Listens to Only a Single Side of a Single Conversation at a Time
- Misses a lot of Conversations

Intercepting Analog

A professional eavesdropper watches **all signals** in a band at the same time with a single receiver.

- May split detection and intercept operation between two different systems
- Misses nothing

Intercepting Digital

- Not within the Realm of a Consumer Grade Radio Shack Police Scanner

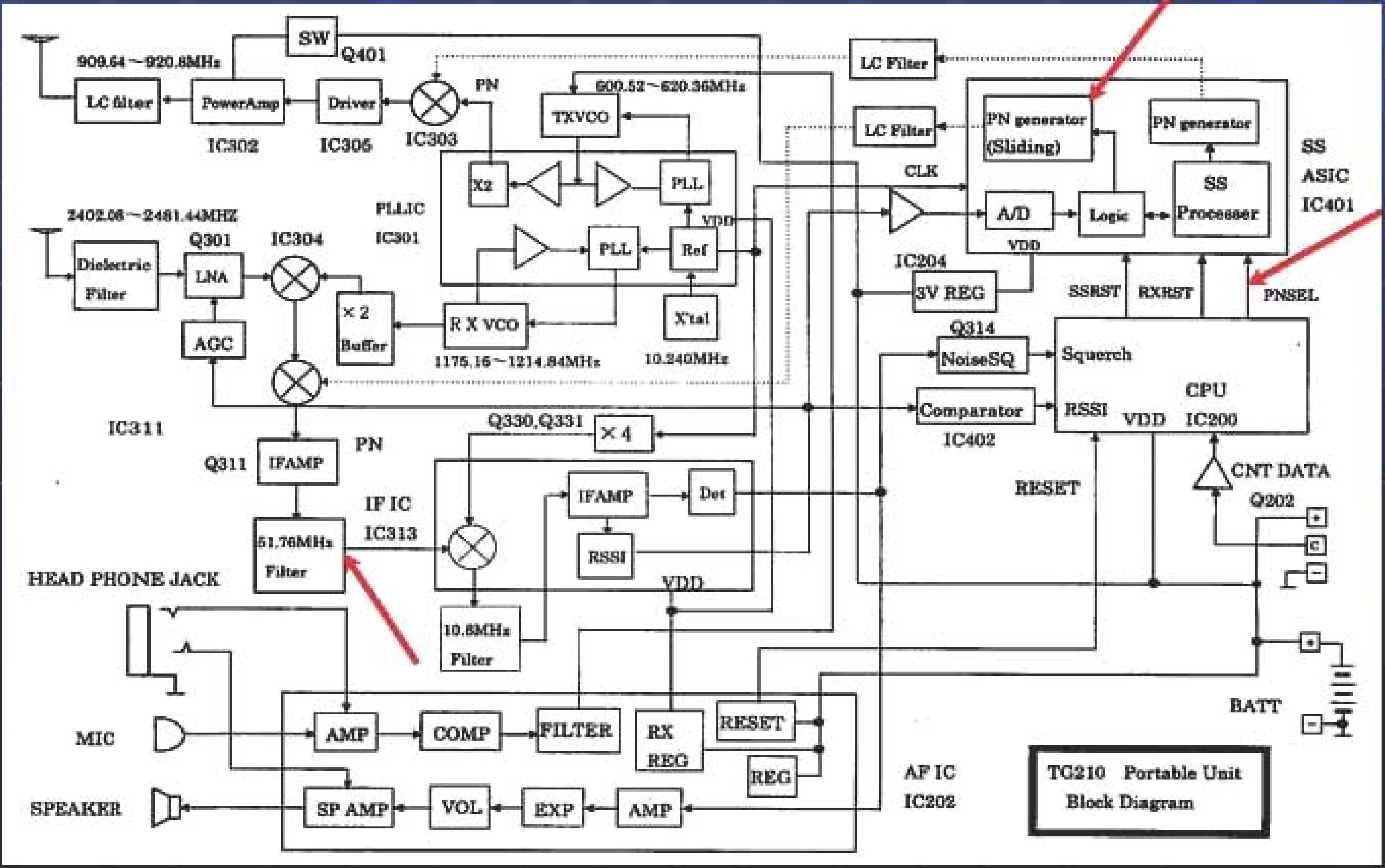
- Often another Modified Digital Phone
  - Even cheaper then a Police Scanner
  - Eavesdropper Programs Extra Phone as Extension on Victims Cordless System
  - Used to “drop in” onto existing calls

Intercepting Digital

- Cheap Receiver or WLAN Card Used as a Primitive Tuner

- Modified 2.4 or 5.8 GHz WLAN Card
  - Card Used As Tuner and Spectrum Analyzer
  - The I-Q Signal is Tapped
  - I-Q Digitized
  - Signal Reconstructed in Software
  - Basic Software Defined Radio
  - Very High Error Rates
  - Narrow Bandwidth

Intercepting Digital



Intercepting Digital

Optimal Professional Solution

- Vector Signal Analyzer

Detecting Frequencies

How to Detect Any Wireless
Signal, on Any Frequency

Why?

Eavesdropper May Not Know:

- If a Cordless Phone Being Used
- Where the Phone Is Located
- May Not Be on a "Legal Frequency"
- May Be Rarely Used
- Modulation Unknown
- Digital Modulation

When?

- Does Not Know the Frequency
- Knows the Frequency, but not the Modulation Method
- Knows Neither the Frequency, nor the Modulation Method
- Knows Both the Frequency, and the Modulation Method, But Lacks Code Domain Elements, Cipher, or Scrambling Method

How?

Spectrum Analyzer

- Sweeps Large Segments of Spectrum
- Shows Signal Spikes
- Fast Detection Over Large Area
- Can Miss a Signal
- Extremely High Resolution of Frequency

How?

Broadband Monitor

- Dedicated to a Single Band
- Detects Any Signal Activity
- Misses Nothing Within Band
- Does Not Specify Frequency
- Easily Confused

How?

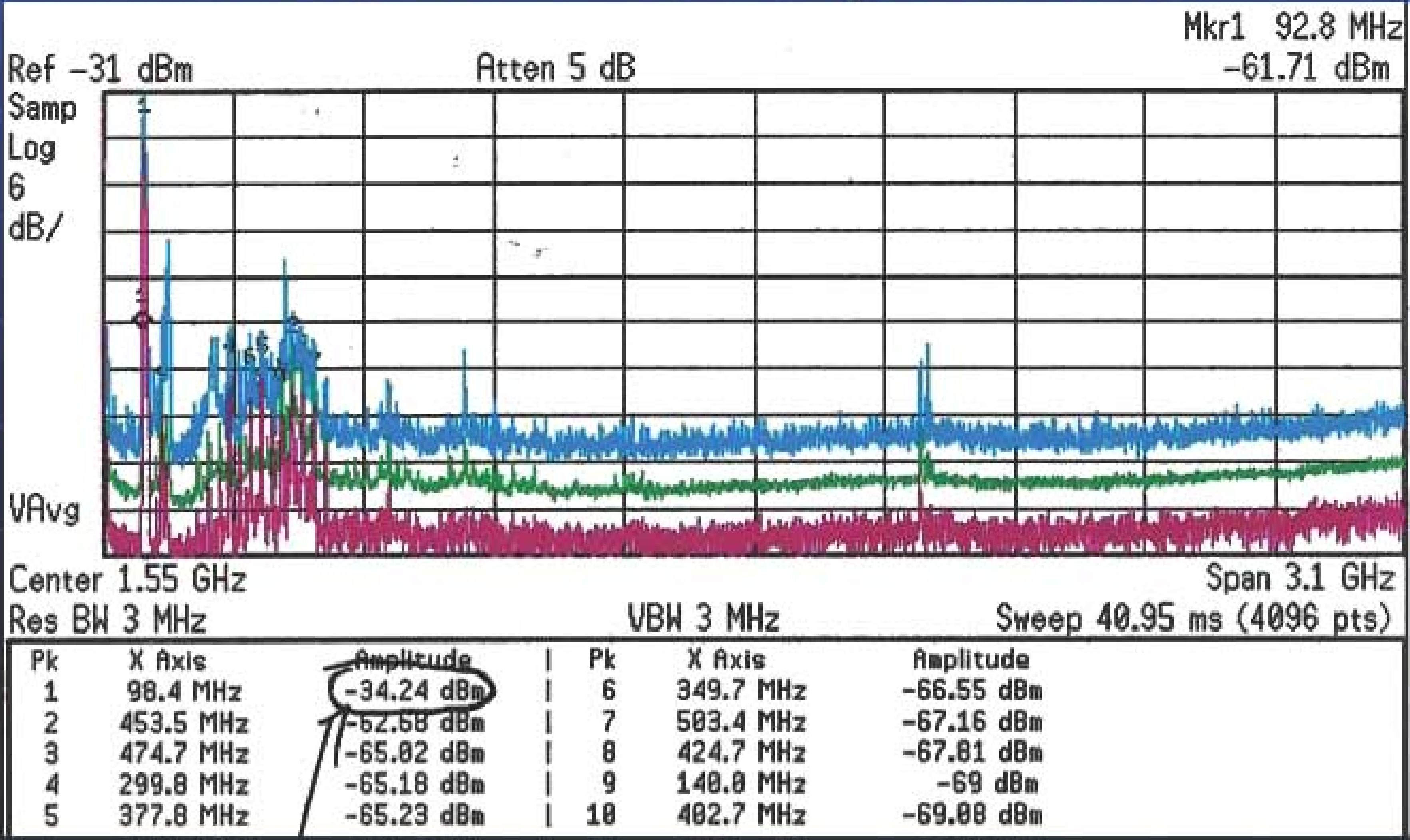
Instantaneous Bandwidth Receiver

- Commonly a Software Defined Radio
- Grabs Entire Band of Interest
- Over 30 MHz of Bandwidth is Expensive
- Perfect for Band Activity Detection
- Requires Secondary Hand-Off Receivers

Spectrum Hunts

Now Let’s Hunt Signals

Full 3.1 GHz Spectrum



Mkr1 92.8 MHz

Ref -31 dBm   Atten 5 dB   -61.71 dBm

Samp
Log
6
dB/

VAvg

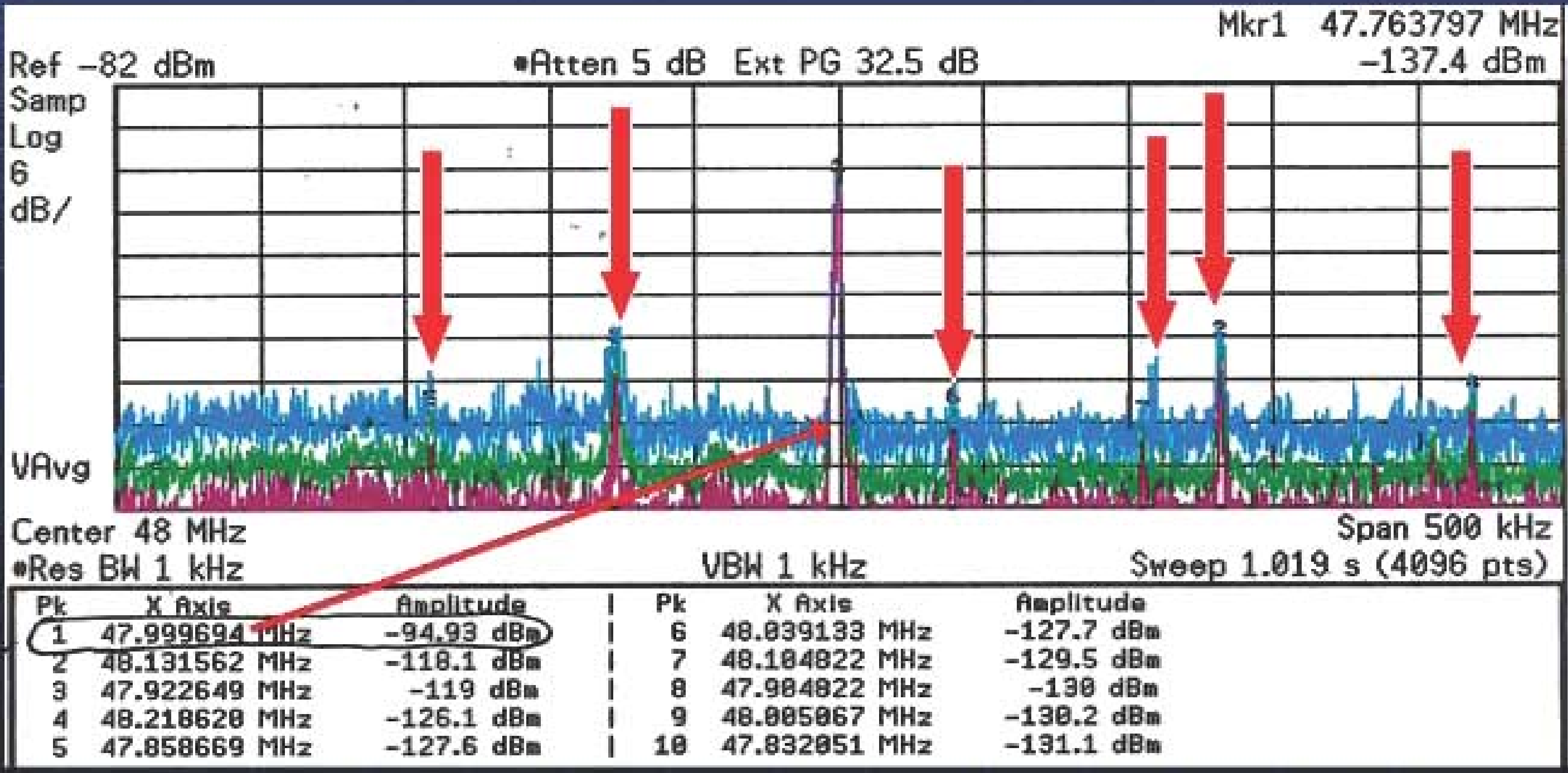
Center 1.55 GHz   Span 3.1 GHz

Res BW 3 MHz   VBW 3 MHz   Sweep 40.95 ms (4096 pts)

Pk	X Axis	Amplitude	Pk	X Axis	Amplitude
1	98.4 MHz	-34.24 dBm	6	349.7 MHz	-66.55 dBm
2	453.5 MHz	-62.60 dBm	7	503.4 MHz	-67.16 dBm
3	474.7 MHz	-65.02 dBm	8	424.7 MHz	-67.01 dBm
4	299.0 MHz	-65.10 dBm	9	140.0 MHz	-69 dBm
5	377.0 MHz	-65.23 dBm	10	402.7 MHz	-69.00 dBm

48 MHz Cordless

- Seven Viable Cordless Signals (CF+6)



Mkr1 47.763797 MHz
-137.4 dBm

Ref -82 dBm   *Atten 5 dB   Ext PG 32.5 dB

Samp
Log
6
dB/

VAvg

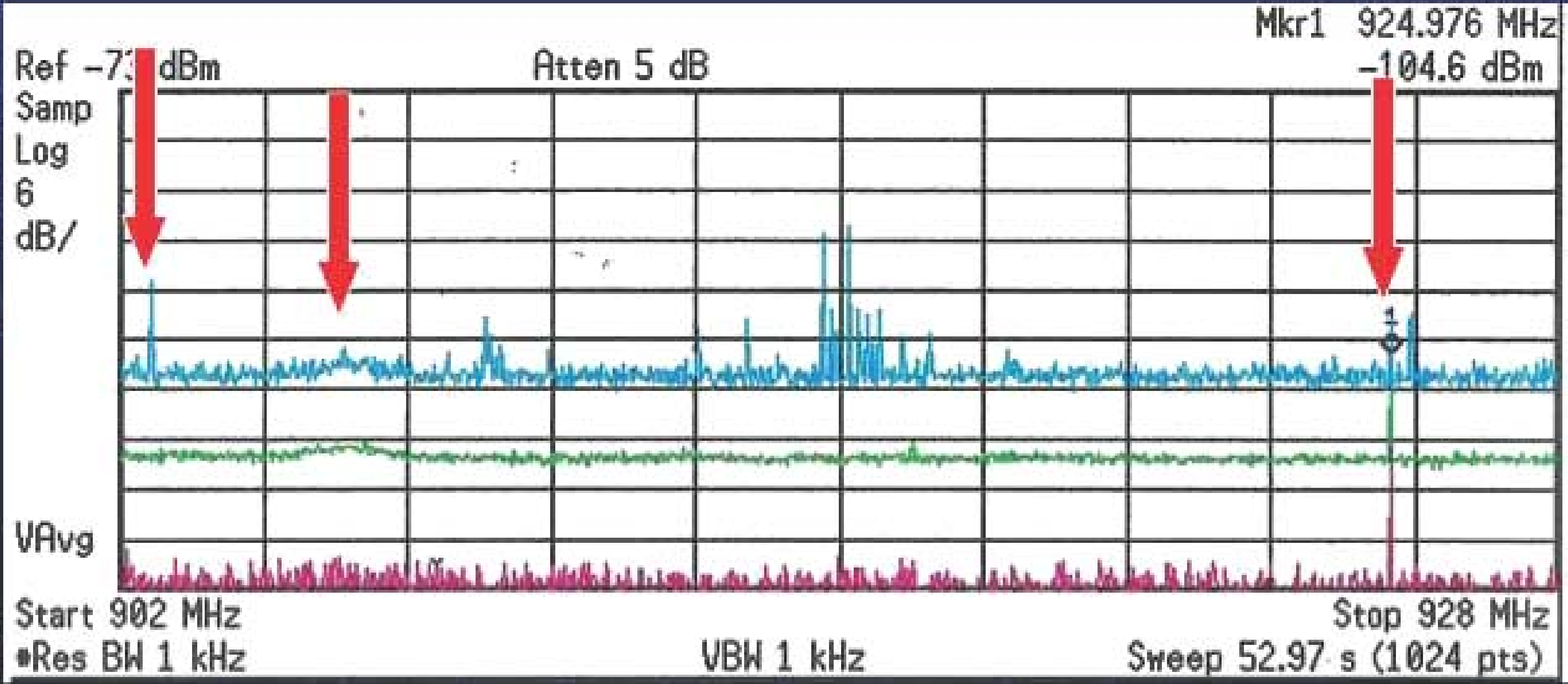
Center 48 MHz   Span 500 kHz

*Res BW 1 kHz   VBW 1 kHz   Sweep 1.019 s (4096 pts)

Pk	X Axis	Amplitude	Pk	X Axis	Amplitude
1	47.999694 MHz	-94.93 dBm	6	48.039133 MHz	-127.7 dBm
2	48.131562 MHz	-118.1 dBm	7	48.184822 MHz	-129.5 dBm
3	47.922649 MHz	-119 dBm	8	47.984822 MHz	-130 dBm
4	48.218620 MHz	-126.1 dBm	9	48.005067 MHz	-130.2 dBm
5	47.858669 MHz	-127.6 dBm	10	47.832051 MHz	-131.1 dBm

900 MHz Cordless

- Two Cordless Systems Live



Mkr1 924.976 MHz

Ref -73 dBm Atten 5 dB -104.6 dBm

Samp
Log
6
dB/

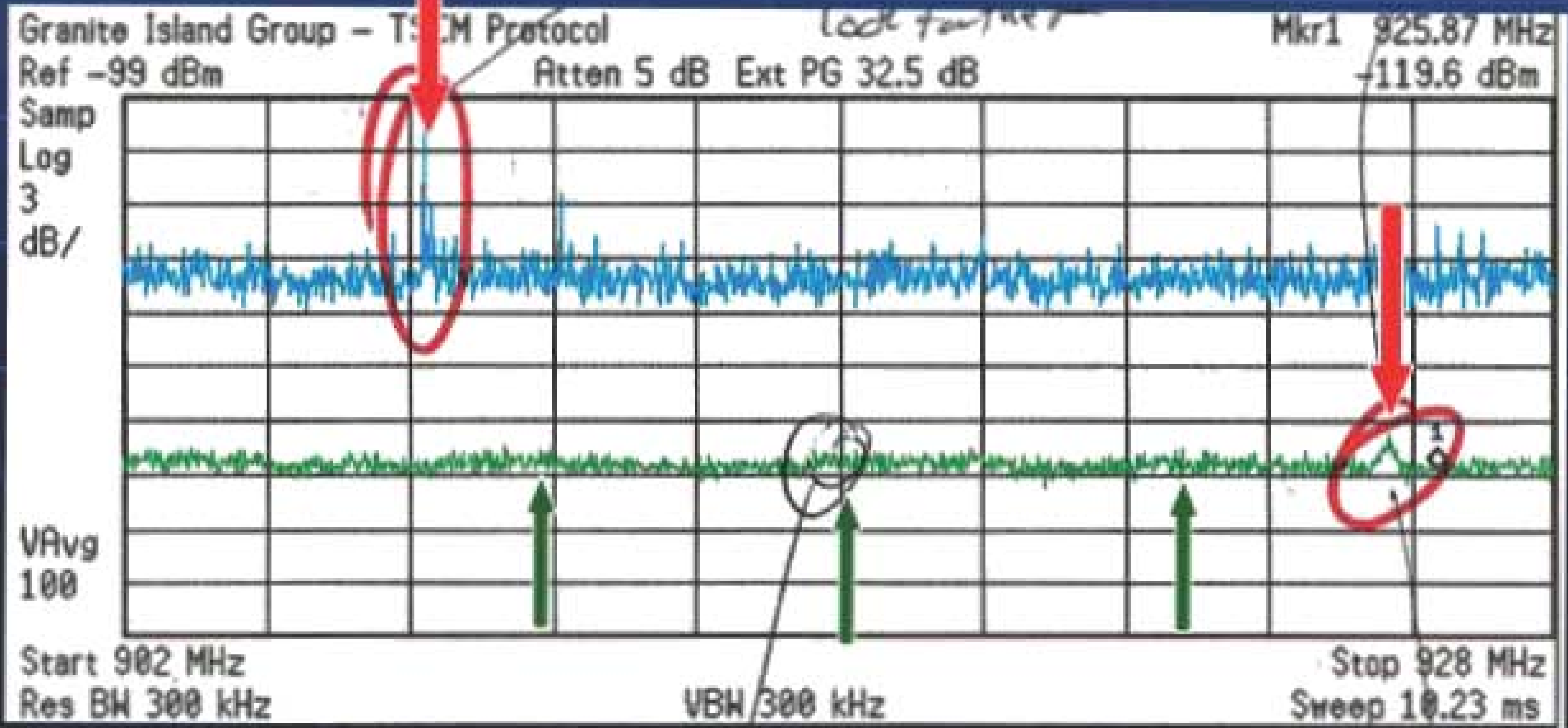
VAvg

Start 902 MHz Stop 928 MHz

#Res BW 1 kHz VBW 1 kHz Sweep 52.97 s (1024 pts)

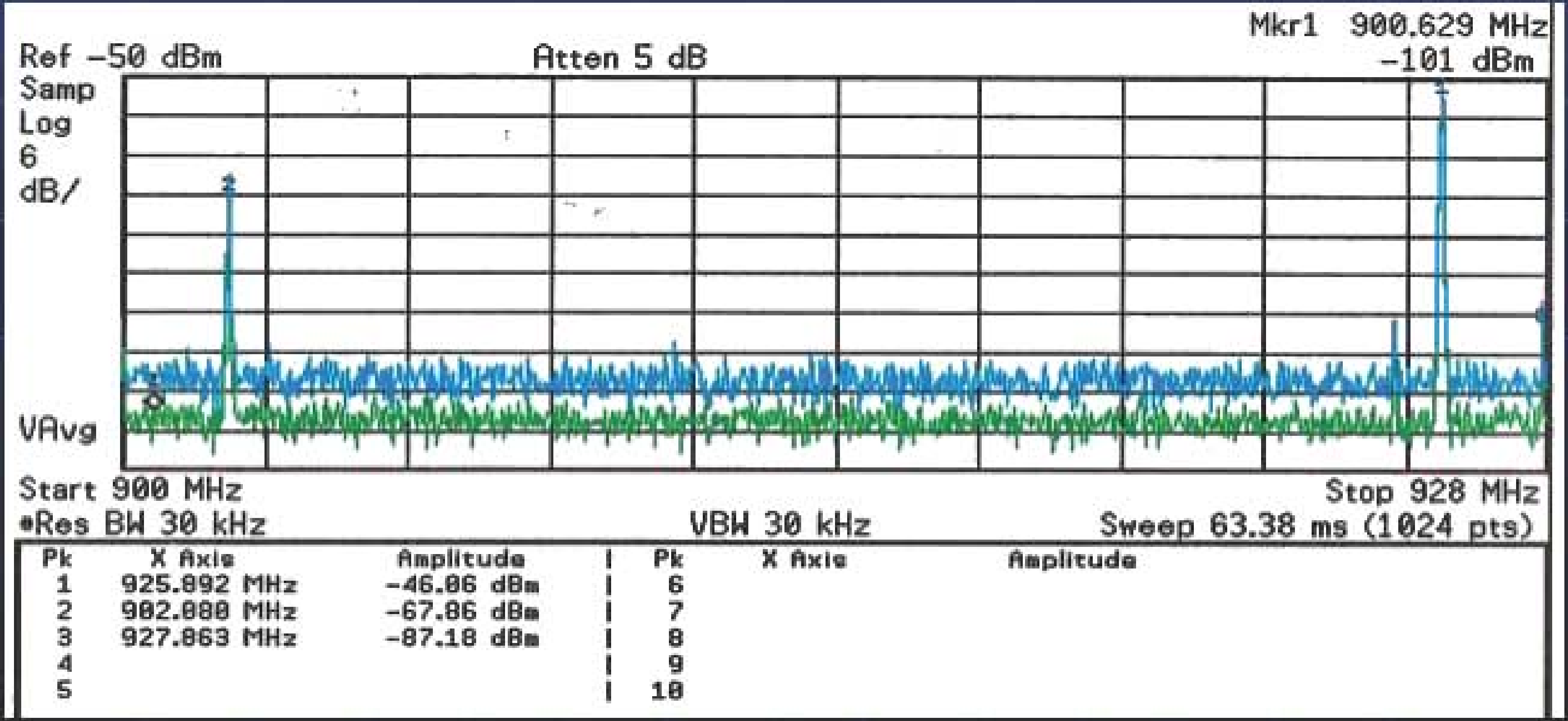
900 MHz Cordless

- 2 Analog, 3 Digital



900 MHz Cordless

- Strong Base and Remote Signals



Mkr1 900.629 MHz
-101 dBm

Ref -50 dBm Atten 5 dB

Samp
Log
6
dB/

VAvg

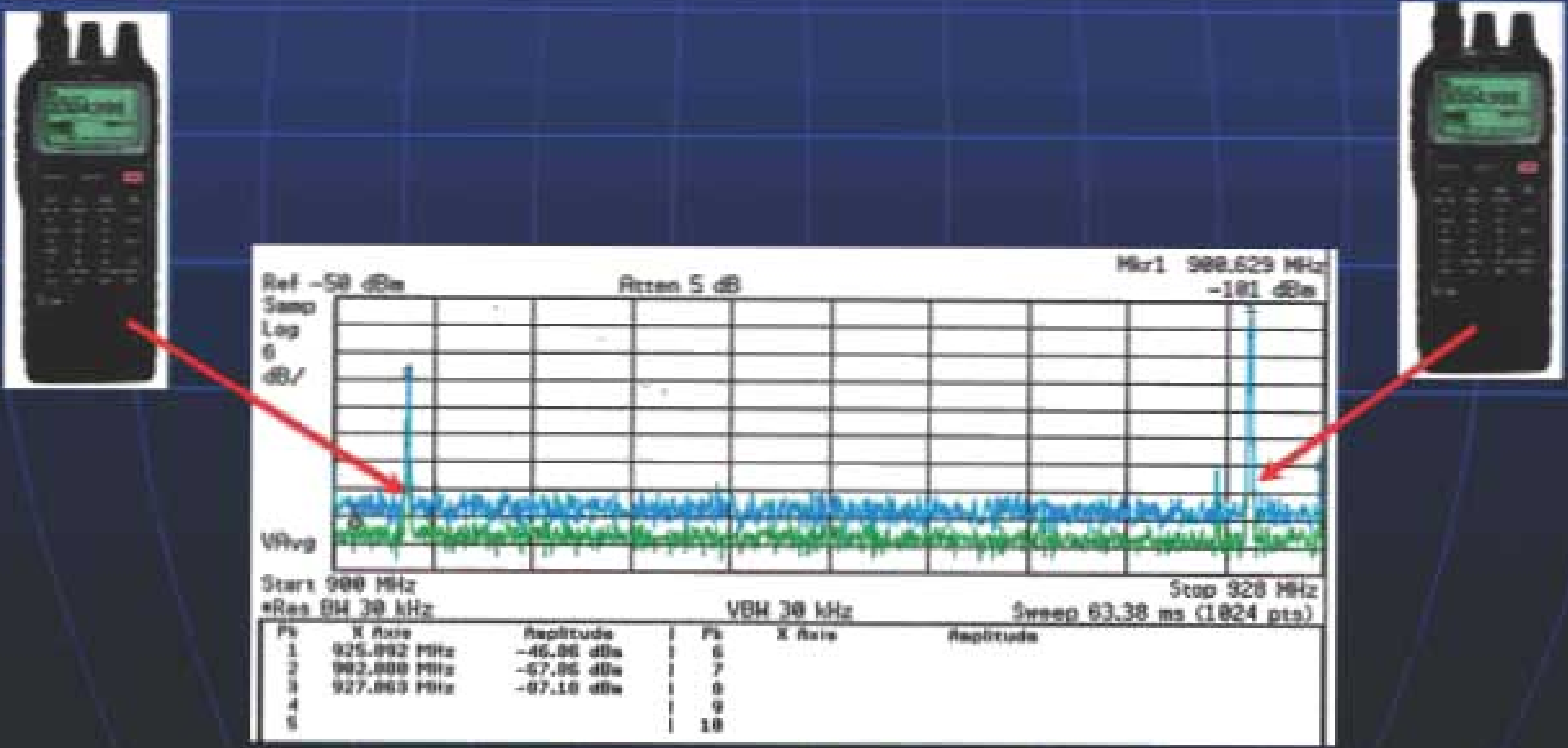
Start 900 MHz Stop 928 MHz

#Res BW 30 kHz VBW 30 kHz Sweep 63.38 ms (1024 pts)

Pk	X Axis	Amplitude	Pk	X Axis	Amplitude
1	925.892 MHz	-46.06 dBm	6		
2	902.000 MHz	-67.06 dBm	7		
3	927.863 MHz	-87.10 dBm	8		
4			9		
5			10		

900 MHz Cordless

- One Icom R-20 Scanner per Signal



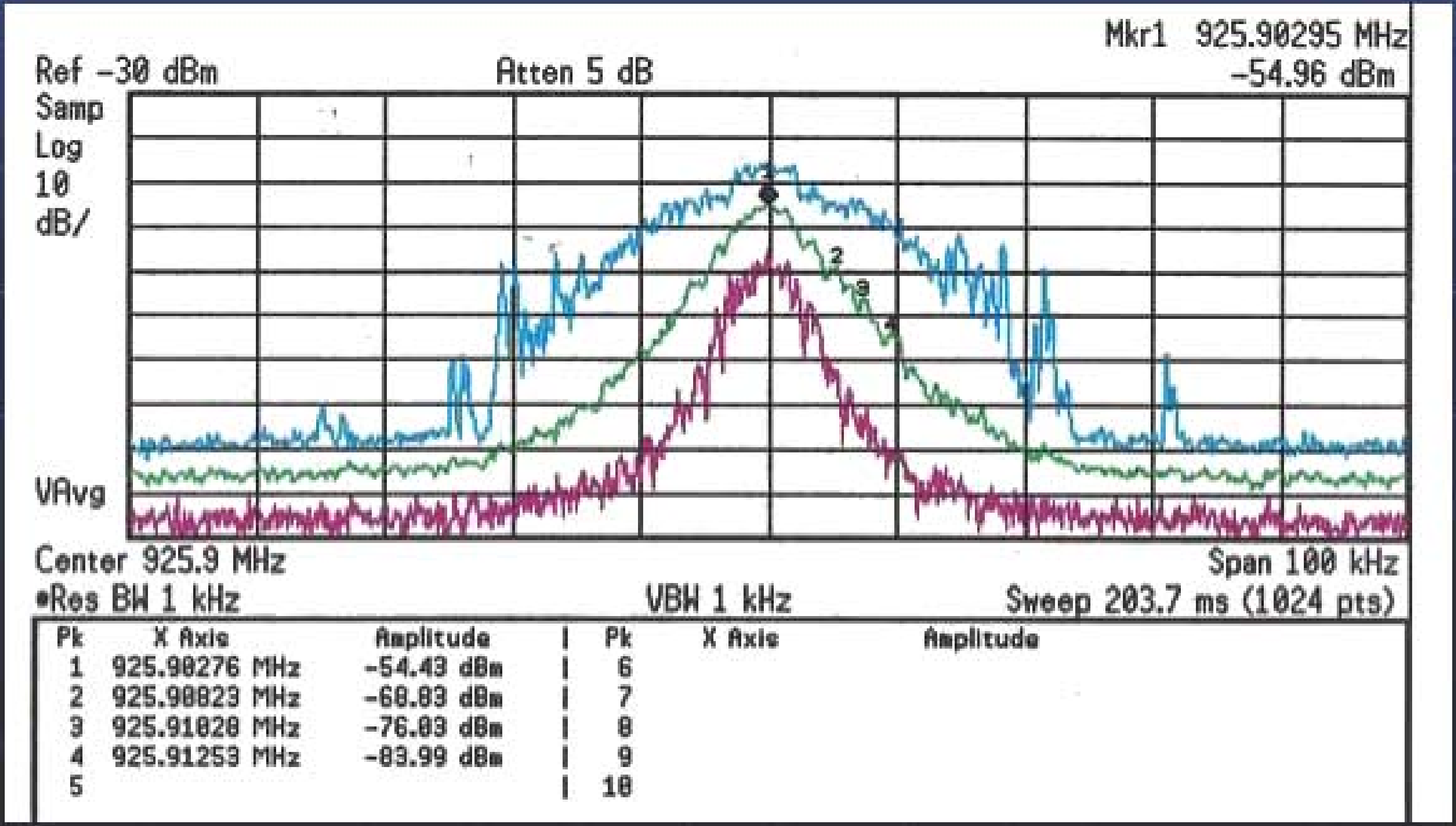
Ref -50 dBm   Atten 5 dB   Mkr1 900.629 MHz
-101 dBm

Start 900 MHz   Stop 928 MHz
#Res BW 30 kHz   VBW 30 kHz   Sweep 63.38 ms (1024 pts)

Pk	X Axis	Amplitude	Pk	X Axis	Amplitude
1	925.092 MHz	-46.06 dBm	6		
2	902.000 MHz	-67.06 dBm	7		
3	927.063 MHz	-87.10 dBm	8		
4			9		
5			10		

900 MHz Cordless

- Typical 50 kHz Signal Bandwidth



Mkr1 925.90295 MHz
-54.96 dBm

Ref -30 dBm Atten 5 dB

Samp
Log
10
dB/

VAvg

Center 925.9 MHz Span 100 kHz

#Res BW 1 kHz VBW 1 kHz Sweep 203.7 ms (1024 pts)

Pk	X Axis	Amplitude	Pk	X Axis	Amplitude
1	925.90276 MHz	-54.43 dBm	6		
2	925.90823 MHz	-60.03 dBm	7		
3	925.91028 MHz	-76.03 dBm	8		
4	925.91253 MHz	-83.99 dBm	9		
5			10		

Analog Intercept Considerations

From the Spies Perspective

1. Very Cheap to Eavesdrop
2. Know Which Bands to Watch
3. Band Edge Scans
4. Spectrum Analyzer to Detect
5. Hand Off to Dedicated Receivers

Advice

How to Deal with Cordless Phone Vulnerabilities

Advice

- Stay Away From Anything that is not 100% Digital Modulation
- Direct Sequence Spread Spectrum
  - Discourages Casual Eavesdropping
  - Do Not Put Too Much Faith In It
- Minimize Use of Non Digital Phones
- Do Not Assume that Digital is Secure

Advice

- DECT is Vulnerable, Use with Caution
- DECT is Better then Old Analog
- 900 and 2.4 GHz Migrations

Advice

- **No Cordless** Use is Even Better
- Hard Wired Phones Are More Secure
- Hard Wired + Crypto is Most Secure

Advice

- Do Not Use Cordless Phones on Higher Floors of Buildings

- Height Drastically Extends Range

  (the eavesdropper will thank you)

- Keep Base Station in Basement or in Middle of House, and Down Low

Advice

- Consider the Use of Dummy Phones

- Keep Dummy Phone on Upper Level
  - On a Fake Call
  - Feed It with TV Audio

Advice

- Wireless LAN “House Rules”
  - Bait Hubs
    - High Altitude
    - Omni Directional Antenna - Outward
    - Strong Signals
    - Exterior Skin of Building
    - Lots of Range
  - Actual Hubs
    - As Low As Possible
    - Direction Antenna – Up, Not Out
    - Low Power Signals
  - Same Usage Rules Apply To Cordless Phones

Advice

- Frustrate the Cordless Eavesdropper
  - Waste Time
  - Waste Resources
  - Lose Interest

- Keep Cordless Phone Base Station That You Actually Use At a Low Height

- Keep Power Levels Really Low
  - Make the Spy Really Struggle
  - Less Range is Best

Advice

- Use a Cordless Phone Only When You Absolutely Need a Wireless Phone For Short Periods
  - Mowing the Grass
  - Doing Yard Work
  - Playing with Dogs

  - Use When Not in Cell Phone Range
  - Keep The Conversation Short

Advice

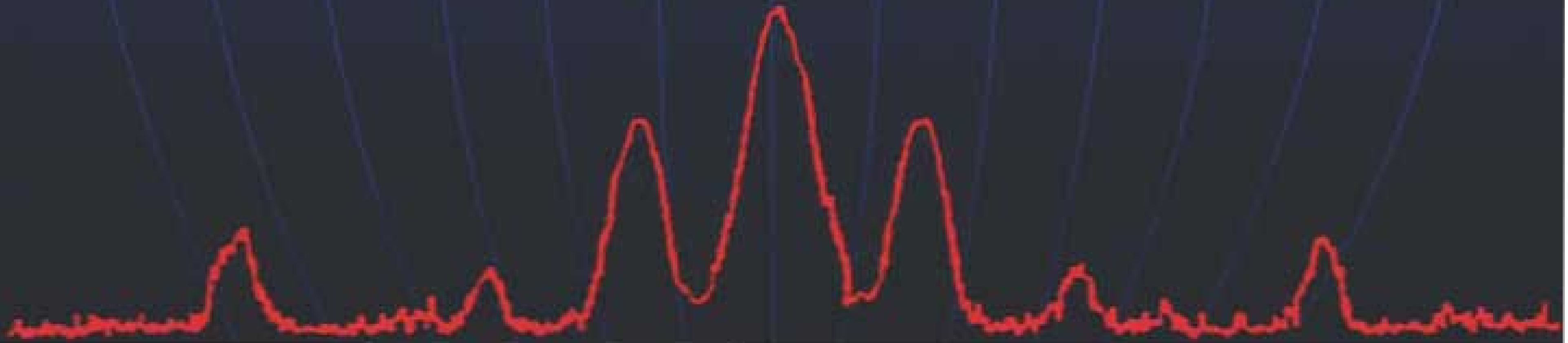
- Do Not Use a Cordless Phone For Anything For Which You Desire Privacy of Any Kind

You Never Know Who Might Be Listening…

? ? ? ? ? ?

Questions?

Thank You



Jim’s Cardinal Rule

Convenience and Privacy are Inversely Proportional™

Please Keep In Touch

(But Not by Using a Cordless Phone)

www.tscm.com