Software Radio and the Future of Wireless Security

Michael Ossmann
Institute for Telecommunication Sciences

ITS Institute for Telecommunication Sciences

Boulder, Colorado

in the next hour

- what is software radio?
- why is software radio taking over the world?
- what does this mean for the future of wireless security research?
- how can I get started with software radio tools today? (radio for software people)
- demos

not in the next hour

- groundbreaking vulnerabilities
- specific wireless protocols

I. what is software radio?

analog signals surround us

- sounds
- images
- radio waves
- tides
- heart rhythms
- seismic waves
- anything that changes over time

digital signals

- a digital signal is simply a sequence of values
- analog signals can be sampled to produce digital signals

the digital audio revolution

- once upon a time, all sound was analog:
  - vinyl records
  - analog tape
  - analog synthesizers
  - analog effects
  - Plain Old Telephone Service

the digital audio revolution

- the revolution began slowly:
  - Digital Audio Tape (DAT)
  - Compact Discs (CDs)
  - digital synthesizers
  - digital effects
  - digital telephone switches
- individual digital components replaced traditional analog components
- professional equipment used by professionals

the digital audio revolution

- then the explosion:
  - hard disc recording
  - home recording studios
  - MP3
  - peer to peer (Napster, Skype, etc.)
  - analog modeling digital synthesizers
- personal computers delivered professional audio tools to the masses

digital audio today

- many of today's hits are recorded in home studios
- old school record labels struggle to compete with new distribution channels
- VoIP services challenge incumbent telephone companies

why the explosion?

- digital audio circuitry had existed for many years
- personal computers enabled wide distribution of software-based digital audio processing
- digital audio brought incremental change, but **software audio** was the true revolution

digital radio

- nearly every recent radio technology is digital:
  - 802.11
  - HD radio and TV
  - mobile phones
  - Bluetooth

software radio

- a signal is a signal (if it can be done with audio, it can be done with radio)
- personal computers are now fast enough for many radio processing functions

ideal software radio receiver

- antenna -> ADC -> CPU

ideal software radio transmitter

- CPU -> DAC -> antenna

practical software radio

- RF front end (analog circuit) is typically required
  - frequency conversion
  - amplification
  - filtering
  - bias

software radio products

- more and more closed source commercial devices use software (or firmware) radio techniques
  - amateur radio equipment
  - WiMAX equipment
  - mobile phone base stations
  - a few mobile phones
- several commercial software radio products for PCs
  - most are RF front ends for sound cards

The Universal Software Radio Peripheral (USRP)

http://www.ettus.com/

- open source design
- can receive and transmit
- multiple RF front end daughterboards
- ADC/DACs
- FPGA
- USB
- GNU Radio interface

II. why is software radio taking over the world?

advantage: flexibility

- software radios can have many operating modes without many circuits
- software radios can perform like multiple radios simultaneously

advantage: reconfigurability

- software radios can implement new software at any time
  - new protocols
  - adaptive filtering
  - new frequencies
  - bug fixes
  - hacks!
- with open source, new radio functions can easily be shared online

advantage: cost

- two ways to build a sophisticated radio device:
  - lots of expensive analog components (and often some digital stuff too)
  - a few cheap analog components plus a computer
    - consider Moore's Law
    - software can make up for deficiencies in the analog circuitry

the future

- consider the commercial advantages of software radio
- consider the current emergence of open source mobile phones and hand-held platforms (OpenMoko, Android, etc.)
- consider that mobile phones using (closed source) software radio technology are starting to arrive
- we will all have hackable software radio platforms in our pockets

the future

- all (okay, most) radios will be software radios
- new wireless protocols will include software reference implementations during development
- all wireless security tools will be software radios

the Wi-Fi lesson

- 802.11b shipped with severe vulnerabilities
- vulnerabilities were ignored until practically demonstrated
- practical attacks were made easy by cheap, ubiquitous, hackable hardware:
  - monitor mode
  - raw frame injection

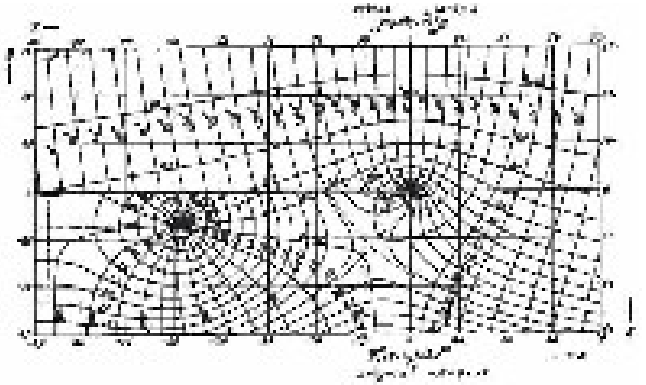
what if every new wireless technology arrived with inexpensive hardware capable of monitor mode and raw frame injection?

III. software radio in security research today

GSM

http://wiki.thc.org/gsm

- USRP/GNU Radio
- decoded GSM signals
- related project: A5/1 decryption



GSM™
The wireless evolution

27 MHz keyboards

http://www.remote-exploit.org/advisories.html

- sound card with RF front end
- decrypted keystrokes

Bluetooth

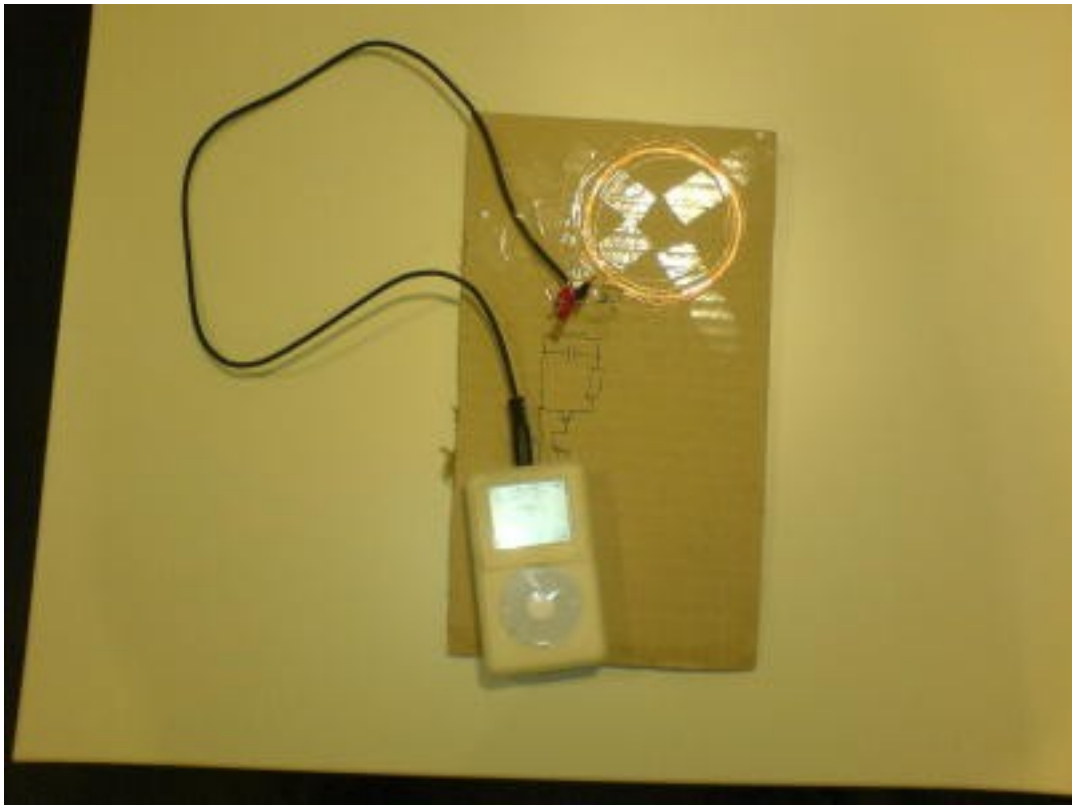
http://www.usenix.org/event/woot07/tech/full_papers/spill/

- USRP/GNU Radio
- single channel sniffing and decoding

RFID

http://events.ccc.de/congress/2006/Fahrplan/events/1576.en.html

- USRP/GNU Radio
- decoded low frequency RFID signals
- iPod replay



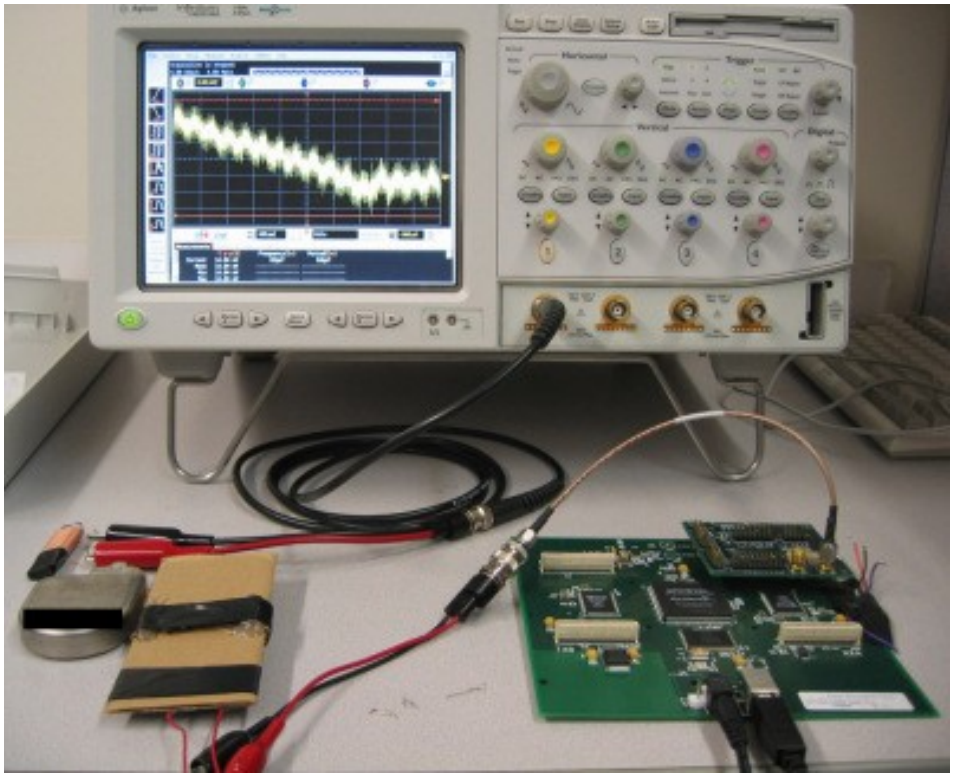
mobitex

http://www.toolcrypt.org/

- sound card with RF front end
- decoded mobitex signals

medical devices

http://www.secure-medicine.org/icd-study/icd-study.pdf



- USRP/GNU Radio
- active and passive attacks against implantable cardioverter defibrillators

demonstration

IV. radio for software people

software radio topics

- RF propagation
- antenna design
- digital signal processing
- RF circuit design
- FPGA programming
- GPU programming
- information theory
- calculus
- abstract algebra
- error correction coding
- SIMD programming
- Fourier theory
- DSP programming
- sampling theory

fortunately. . .

- only a small subset of this knowledge is required to get started using software radio for useful security tasks:
  - practical implementation of theoretical attacks
  - reverse engineering
  - development of new attacks

RF basics

- radio waves are electromagnetic radiation in the range of about 3 Hz to 300 GHz (wavelengths of 100,000 km to 1 mm)
- most practical applications are between 30 kHz and 30 GHz (wavelengths of 10 km to 1 cm)

antenna basics

- most jobs don't require an optimal antenna
- longer wavelengths require bigger antennas
- it's better to go too big than too small
- low frequency applications (like 125 kHz or 134 kHz RFID tags) require loops

Goldilocks and the Three Bands

- kHz: These wavelengths are too long!
  - antennas are unwieldy
  - bandwidth is limited
- GHz: These wavelengths are too short!
  - propagation is poor
  - short range, LOS, or directional applications only
- MHz: These wavelengths are just right!
  - manageable antennas
  - reasonable bandwidth
  - good propagation

remember the Fourier transform?

- taught in Calculus courses
- essential for DSP
- important principle: any waveform can be precisely represented as a sum of sinusoidal components
- Fast Fourier Transform (FFT) is the common digital equivalent
- invertible function

“bandwidth”

- the word “bandwidth” is overloaded but has a particular meaning in the RF/DSP world:
  - the width (in Hz) of the range of frequency components of a signal
- wider bandwidth signals have greater channel capacity (they can carry more bits per second)
- spread spectrum technologies intentionally squander channel capacity in exchange for resistance to interference

visualize, visualize, visualize

- GNU radio
- gnuplot
- various audio tools
- my favorite: baudline (free but closed source)

sampling theory

- in order to capture a signal, your sampling rate must be greater than twice the bandwidth of the signal
- example: to capture a 25 kHz wide analog FM transmission, your ADC must acquire no less than 50,000 samples per second

aliasing

- frequency components of sampled signals are ambiguous
- example: a 150 kHz sinusoid sampled at 192 ksps is indistinguishable from a 234 kHz sinusoid sampled at 192 ksps (both are 42 kHz away from the sample rate)
- anti-aliasing filters must be present in the analog domain

convolution

- a simple and useful operation best illustrated by example:
- convolve [1,1,1] with [0,1,2,3,2,1,0,1,2,3,2,1]:

```
[1,1,1] * 0 = [0,0,0]
[1,1,1] * 1 =   [1,1,1]
[1,1,1] * 2 =     [2,2,2]
[1,1,1] * 3 =       [3,3,3]
[1,1,1] * 2 =         [2,2,2]
...
sum up:       [0,1,3,6,7,6,3,2,3,6,7,6,3,1]
```

convolution as a filter

- The convolution of [1,1,1] with [0,1,2,3,2,1,0,1,2,3,2,1] is a moving average and can be thought of as a filter:
  - [0,1,2,3,2,1,0,1,2,3,2,1] is the signal
  - [1,1,1] is a crude low pass filter
- “low pass” means that it filters out high frequency components but allows the low ones to pass through
- low pass filters result in smoother, rounder, waveforms

FIR filters

- convolution of a signal with a static sequence is called a Finite Impulse Response (FIR) filter
- the elements of the static sequence are called the coefficients of the filter
- FIR filters can be used to emphasize arbitrary frequency components or remove others
- High pass, low pass, and band pass are common, but more complex shapes are possible
- FIR filters can be fast (SIMD, DSP chips, etc.)

filter design

- common routines are available to “design” (produce the coefficients for) filters based on the required shape in the frequency domain (the filter's “frequency response”)
- always test filters

modulation

- there are only three basic types of modulation:
  - amplitude modulation
  - frequency modulation
  - phase modulation
- there are many combinations and variations of these three
- digital modulations are often referred to as “keying”

symbols

- a symbol is the shortest segment of a signal that represents a discrete value of the digital data being transmitted
- example: Binary Frequency Shift Keying (BFSK) uses one frequency for “0” and another for “1”
- the symbol rate (or “baud rate”) is the number of symbols transmitted per second

software re-use

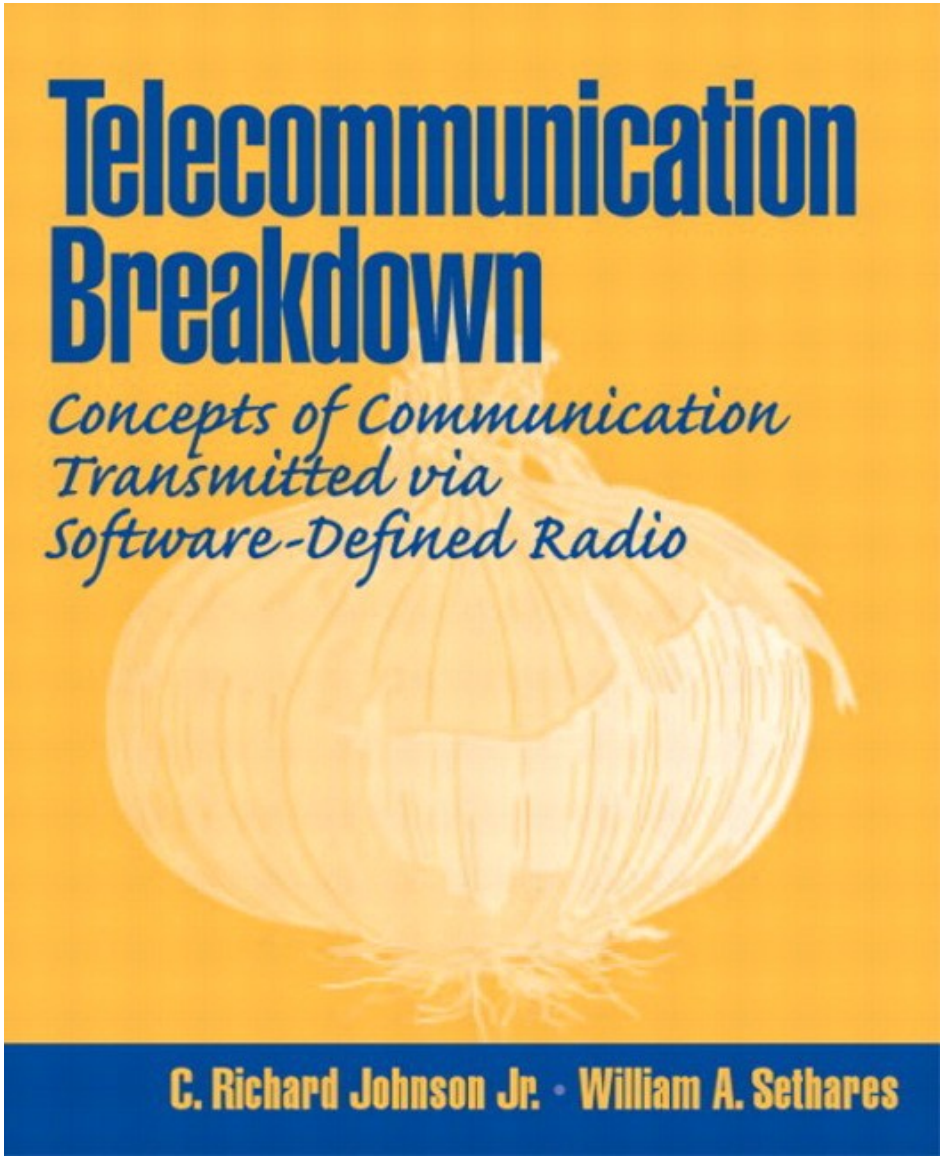
- GNU Radio and other frameworks include code for:
  - filters
  - filter design functions
  - resampling
  - frequency conversion
  - modulation
  - demodulation
  - and much more

hardware options

- USRP
- HPSDR
- sound card with RF front end
- anything with ADC/DAC
  - DAQ boards
  - TV tuners
  - video cards
- hack off-the-shelf software radio equipment
- you can even get started without hardware!

a good book

http://eceserv0.ece.wisc.edu/~sethares/telebreak.html



be a good neighbor

- know your laws
- don't transmit anything over the air without being sure of what you are doing
  - you can often use cables instead (but don't forget attenuators)
- common transmission mistakes:
  - failure to filter noise outside of the intended signal bandwidth
  - failure to filter aliases

beyond radio communications

- Van Eck phreaking
  - radio
  - audio
  - visible light
- wired applications
  - wired communications
  - power consumption and other side channel attacks
  - often requires attenuation or other small analog circuitry

questions

credits (books)

- C. R. Johnson, Jr. and W. A. Sethares. Telecommunication Breakdown: Concepts of Communication Transmitted via Software-Defined Radio. http://eceserv0.ece.wisc.edu/~sethares/telebreak.html

credits (tools)

- GNU Radio: the gnu software radio. http://gnuradio.org/trac
- The Universal Software Radio Peripheral (USRP). http://www.ettus.com/

credits (security research)

- The GSM Software Project
  http://wiki.thc.org/gsm
- Max Moser and Phill Schrödel. 27Mhz based wireless security insecurities.
  http://www.remote-exploit.org/advisories.html
- Dominic Spill and Andrea Bittau. BlueSniff: Eve meets Alice and Bluetooth.
  http://www.usenix.org/event/woot07/tech/full_papers/spill/
- Henryk Plötz. RFID Hacking.
  http://events.ccc.de/congress/2006/Fahrplan/events/1576.en.html

credits (more security research)

- olleB. Mobitex Network Security.
  http://cansecwest.com/csw08/csw08-olleb.pdf
  http://www.toolcrypt.org/
- Daniel Halperin, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.
  http://www.secure-medicine.org/icd-study/icd-study.pdf