Hacking With GnuRadio

How to have fun with wireless transmissions!
David M. N. Bryan

- Info Security Consultant
- CISSP
- HAM
- Hacker
- DEFCON

netSPI
RISK COMPLIANCE SECURITY
Hacker Spaces!!!

Thanks to CCCKC – Sweet Hacker Space!
What is this?
Is that a hot pack in your pocket?
Counter Measures?

Mind the gap!
Disable the use of RTE
Crash bar
Push to exit
Hacking With GnuRadio

What is GnuRadio?

What you need

Requirements

Costs
What is GnuRadio?

Software – Python = byte code = good!

Hardware -

Universal Software Radio Peripheral

Field Programmable Gate Array

4 DAC
4 ADC

TX / RX Daughter boards from 0.1Mhz to 5.8Ghz
USRP v1.0
USRP Board
Daughter Boards
How Can I use it?

Get Hardware – USRP
Install Ubuntu – or other Unix like OS

USRP Interface Requirements
v1.0 USB 2.0
v2.0 Gigabit Ethernet
Why should I use it?

Wireless Signal Receiving and Generation

Circuit logic

Oscillator

Other methods are painfully slow for prototyping
Cost

USRP1 $700
USRP2 $1400
Daughter Boards $75-$400
Screws/Case $20
Not specifically FCC Part Licensed

Owning your neighborhood SCADA- Priceless!
So what can we do with it?
Wireless Attacks

RFID Payment Cards
Global System Mobile (GSM)
Bluetooth (Frequency Hopping)
Multiple Access System (MAS)
RFID Attacks
RFID Tag reading
Boston Subway Hacks
MiFare Card Attacks
Long Range Tag Reading
GSM Attacks

wiki.thc.org – A5 GSM Cracking
Base station – call routing?
Cell free zone?
Bluetooth Attacks

Frequency Hopping Spread Spectrum
Follow “hop” patterns
USRP V2 Only – v1 lacks bandwidth
Using 8 v2 USRPs
MAS System

Multiple Access System

Computer Applications in Power, IEEE

Volume 5, Issue 4, Oct 1992 Page(s):29 - 32

Digital Object Identifier 10.1109/67.160043

Summary: The use of 900 MHz radio for supervisory control and data acquisition applications was investigated by the Houston Lighting and Power Company (HL&P). Multiple address system applications in the 928/952 MHz band were evaluated. (etc....)
MAS System Attacks

Simple 1992's Repeater

Head End

Repeater

Yagi Ant

netSPI
MAS System Attacks

Request Status

Head End

Repeater Omni

Input Freq

Yagi Ant

Yagi Ant

Yagi Ant
MAS System Attacks

Status Reply

Head End

Repeater Omni

Input Freq

Yagi Ant

Yagi Ant

Yagi Ant
MAS System Attacks

Request Status

Head End

Evil Hax0r

Input Freq

Repeater Omni

Yagi Ant

Yagi Ant

Yagi Ant

netSPI
MAS System Attacks

Request Status

Evil Hax0r

Repeater Omni

Input Freq

Head End

Input Freq

Yagi Ant

Yagi Ant

Yagi Ant

netSPI
USRP - First Attempt
USRP - Second Attempt
MAS System Attacks

Request Status

Head End

Input Freq

Repeater Omni

Evil Hax0r

Input Freq

Yagi Ant

Yagi Ant

Yagi Ant

Yagi Ant
USRP - Third Attempt
USRP - Third Attempt
USRP - Third Attempt
USRP - Third Attempt
## Alarm Summary

<table>
<thead>
<tr>
<th>Ack</th>
<th>Time In</th>
<th>Date In</th>
<th>Tagname</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12:16:09.785</td>
<td></td>
<td>PLCD1COMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>2</td>
<td>12:15:32.691</td>
<td></td>
<td>O1COMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>3</td>
<td>12:15:25.566</td>
<td></td>
<td>AIRCOMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>4</td>
<td>12:14:52.551</td>
<td></td>
<td>FAILCOMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>5</td>
<td>12:13:59.598</td>
<td></td>
<td>COMMFAIL</td>
<td>0</td>
<td>comm fail</td>
</tr>
<tr>
<td>6</td>
<td>12:13:50.395</td>
<td></td>
<td>PLCD1COMMFAIL</td>
<td>0</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>7</td>
<td>12:12:22.318</td>
<td></td>
<td>COMMFAILFAIR</td>
<td></td>
<td>ALARM failed</td>
</tr>
<tr>
<td>8</td>
<td>12:04:13.525</td>
<td></td>
<td>AIRCOMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>9</td>
<td>12:04:13.526</td>
<td></td>
<td>AIRCOMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>10</td>
<td>12:03:21.498</td>
<td></td>
<td>FAIRCOMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>11</td>
<td>12:03:21.498</td>
<td></td>
<td>AIRCOMMFAIL</td>
<td>1</td>
<td>COMM FAIL!!!!!!</td>
</tr>
<tr>
<td>12</td>
<td>11:32:46.199</td>
<td></td>
<td>FCOMMFAIL</td>
<td>1</td>
<td>comm</td>
</tr>
<tr>
<td>13</td>
<td>08:11:37.152</td>
<td></td>
<td>SOUTHDISQUALIFIEDALM</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>08:08:24.027</td>
<td></td>
<td>BCOMMFAIL</td>
<td>1</td>
<td>comm</td>
</tr>
<tr>
<td>15</td>
<td>10:19:35.262</td>
<td></td>
<td>SOUTHDISQUALIFIEDALM</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>09:20:04.167</td>
<td></td>
<td>LO7LEVELHIGH</td>
<td>High</td>
<td>Lime Silo 7 Level High</td>
</tr>
<tr>
<td>17</td>
<td>13:49:46.829</td>
<td></td>
<td>DOORTS</td>
<td></td>
<td>Well F RTU door open</td>
</tr>
<tr>
<td>18</td>
<td>13:49:44.782</td>
<td></td>
<td>MP7LOSSOFPRIME</td>
<td>1</td>
<td>pump no. 7 loss of prime</td>
</tr>
<tr>
<td>19</td>
<td>13:49:44.641</td>
<td></td>
<td>LO3LEVELHIGH</td>
<td>High</td>
<td>Lime Silo 3 Level High</td>
</tr>
</tbody>
</table>

Total Alarms: 19  
Filter: NOT (Tagname = "*oos*")  
Sort: Time In, Descending
MAS System Attacks

Request Status

Evil Hax0r

Head End

Repeater Omni

Input Freq

Yagi Ant

Yagi Ant

Yagi Ant

Yagi Ant
MAS Radio Issues

Wide Open
No Authentication
No Integrity
Single In / Multiple Out “Repeater”
Poor Design
MAS Radio Fixes

- Use encryption
- Use 802.11 type networks
- Use routing protocol for link failures
- Out of band management
Demo ?
How Can I Contribute?

Join a hacker space
Post
Play
Have Fun!
Thank you!

My wife, Heather
References

- www.gnuradio.org
- http://www.ettus.com/
- www.ece.vt.edu/swe/chamrad/crdocs/CRTM09_060727_USRP.pdf
- http://www.rfidhackers.com/