Hacking the Wireless World with Software Defined Radio – 2.0
Balint Seeber (Applications Specialist & SDR Evangelist)

balint@ettus.com
balint@spench.net
@spenchdotnet
Getting ready for some serious sampling by the Adriatic Sea
First day of visit to Italy...
**ISEE-3**

- **International Sun/Earth Explorer 3**
- **Launched:** August 12, 1978
- **Heliocentric Orbit**
- **Study interaction between solar wind and Earth’s magnetic field**
ISEE-3

- Renamed ICE: **International Cometary Explorer**
- First spacecraft in halo orbit at an Earth-Sun L1 (Lagrange point)
- First spacecraft to pass through tail of a comet (Giacobini-Zinner)
ISEE-3 ORIGINAL
TRAJECTORY
1978-1985
3D RADIO MAPPING ANTENNA LENGTH (TIP TO TIP)

AXIAL: 14 m
RADIAL: 92 m

SHORT ELECTRIC ANTENNA
SEARCH COIL

AXIAL ΔV AND ATTITUDE CONTROL THRUSTER

RADIAL THRUSTERS

AXIAL ΔV AND ATTITUDE CONTROL THRUSTER

SPIN AND DESPIN THRUSTERS

MEDIUM GAIN 2-GHz (S-BAND) ANTENNA

TOTAL S/C WEIGHT: 479 kg
EXPERIMENTS: 104 kg
HYDRAZINE: 89 kg
DIMENSIONS (MAIN BODY)

DIAMETER: 1.77 m
HEIGHT: 1.58 m

SPIN STABILIZED AT 19.75 RPM
**Old Telemetry Screen**

```
ISEE-C: CPU1: 64:ACN:ORB 000; BUS V 20.29; ES CURR 1.34; NE CURR 6.69
OA 8.0; 0.000 RPM; 0.000 SEC; CMD CTR A:B 86; 79:5/C 337/22:24:49 (30261143)
S/C HSK, PAGE 4                   RESET CTR A:B 640:639; GMT 074/22:18:08.115 78/03/15
--ATTITUDE AND ORBIT CONTROL SUBSYSTEM--  ---- HYDRAZINE PROPULSION SYSTEM----
- ELECTRONICS A -  - ELECTRONICS B - PRI HTRS 1/2 LOW  ACCL CTR 1/2 110
LOGIC PWR ON  LOGIC PWR ON  SEC HTRS 1/2 OFF  ACCL T 1/2 24.4
+28V PWR ON  +28V PWR OFF  ACL PWR 1/2 2.50 T PRI TK HTRS OFF
TSL 010TSL 010100 PRI TK HTRS100100 SEC TK HTRS OFF
SINIT 01100 OFF  SINIT 10110 10001 SEC TK10110 10001 LATCH VALVE OFF
SECT WIDTH 360 SECT WIDTH OFF  LATCH VALVEA OPEN  LATCH VALVEB OPEN
FIRINGS 36 FIRINGS 77 LATCH VALVE CLOS  THERMO CPLF 346.2
RATIO FIRING DIS RATIO FIRING DIS THERMO CPL 248.6 TANK PRESS 2.4
THRUST RATIO 2 THRUST RATIO 114 TANK PRESS 2.7
MANEUVER TERM MANEUVER INIT
MANEUVER COMPL NO MANEUVER COMPL YES
```

 FRAME NUMBER 173
Overview

- Restaurant Pagers
- RDS TMC
- Primary Surveillance RADAR
- RFID
- ISEE-3
50 MHz BW
GSM BCCH & Traffic
Dialplan

• 101 – Registration
  – Text back 4-to-10 digit number to register
• 411 – Info
• 600 – Echo Test
• 777 – Time
• 778 – ANI
• 2103 – Me
Thanks to Frank of ‘radiorausch’ for the first version.

GSM-850

PCS-1900

LTE

Always look for the first strongest peak! Good idea to start with a long duration.

This one is a false peak (artifact) because the signal is not cyclic relative to the sampling window.

See how the remaining peaks are harmonics, decrease in amplitude, and wrap around from the end (offset due to FFT size).
400 MHz Band
50 MHz – 250 MHz (200 Msps, 120 MHz RF BW)
Spectrum Monitoring
Spot the Antennas
Spot the Antennas
Spot the Antennas
Spot the USRPs
Stitched FFTs
Stitched FFTs
USRP B200 & B210

USB 3.0 (bus powered!)
56 MHz bandwidth

70 MHz – 6 GHz
2x2 MIMO
Restaurant Pagers

Hacking the Wireless World with #sdr

@spenchdotnet
Your food is ready?

- Pagers inform waiting customer they can collect their order
  - Assuming their order is ready
- Order & collection rate should be ~same
  - Unless everyone is paged at once
Step 1: Frequency

• Either:
  – Find frequency label on the device
  – Find FCC ID on device and check online
  – Scan spectrum in likely ranges (e.g. 450-470 MHz)
Step 1: Frequency
Step 1: Frequency

Note how often transitions occur (no long runs of ‘0’ or ‘1’). Implies line encoding is in use (helps clock recovery at receiver).
Flowgraph
Step 2: Channel Selection
Step 3: FSK Deviation
Step 4: Quadrature Demod
Step 5: Baud Rate
Step 5: Clock Recovery
Step 6: Line Encoding
Manchester Encoding
Manchester Violation
Step 7: Compare Changing Bits
Step 8: Finding the ID
Modulator

• Reverse the decoding process:
  1. Construct packet
     a) Preamble (wake up receiver)
     b) Magic header (sync & system ID)
     c) Pager number
     d) Checksum
  2. Interpolate (choose samples per bit)
  3. Frequency Modulate
  4. Apply pulse-shaping filter (*ideally*)
  5. Resample for transmitter
Modulator
Modulator Output
Modulator
Remote Control

Web-based XML RPC client controlling GNU Radio application over WiFi
POCSAG

- Other restaurant pager systems adopt a standard
- Decode with gr-pocsag
  - Modified to end frame decoding when squelch closes
POCSAG Decode
POCSAG Frames

----
[00] Address: 001dc168 function: 00000000
[02] (001dc168) Idle
=== SQUELCHED (residue: 5) ===
----
[00] (fffffff) Idle
[01] (fffffff) Idle
[02] (fffffff) Idle
[03] (fffffff) Idle
[04] (fffffff) Idle
[05] (fffffff) Idle
[06] Address: 001dc15b function: 00000000
[08] (001dc15b) Idle
=== SQUELCHED (residue: 5) ===
----
[00] (fffffff) Idle
[01] (fffffff) Idle
[02] (fffffff) Idle
[03] (fffffff) Idle
[04] (fffffff) Idle
[05] (fffffff) Idle
[06] Address: 001dc15b function: 00000000
[08] (001dc15b) Idle
=== SQUELCHED (residue: 5) ===
POCSAG Frame

[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] Address: 001dc15b function: 00000000
[08] (001dc15b) Idle

=== SQUELCHED (residue: 5) ===

5b = 01011011
Pager Frame Construction

• Preamble
• SYNC
• Address: System & Pager
  – Schedule address to appear in correct slot
  – Pad with IDLEs beforehand
• Pager action
• Trailing IDLE
• Apply BCH(31,21) ECC to each slot
POCASG Modulator
ZigBee

- Roles reversed: pager unit transmits
- Pager unit has integrated RFID reader
- RFID chip stuck on underside of each table
- Placing pager unit on table transmits **pager** number and **table** number
- 2.4 GHz ISM band
- Decode with gr-ieee802-15-4
Decoded ZigBee
Decoded Pager

Pagers:

- **38 = 0x26**
- **54 = 0x36**

Table:

- **36 = 0x24**
Hostage Pager

- Pagers get angry when system broadcast (beacon) is not heard within timeout
  - Flash & vibrate until they are returned within range
- Take a pager hostage by broadcasting beacon
RDS TMC

Hacking the Wireless World with #sdr @spenchdotnet
FM Broadcast Band
FM Broadcast Band
Radio Data Service

- Subcarrier on commercial FM stations
- Not audible (filtered out)
- BPSK @ 1187.5 bps
- Listen & decode with gr-rds
Stereo FM with RDS: Receiver
Radio Data Service

103.7 Greatest Hits of All Time

FM Demod

Frequency: 103.70
Station Name: The Bay's 103.7 Greatest Hits of All Time
101.9 MHz
SDR-FM!!
Traffic Message Channel

• Type 8A RDS group message
• Compact representation via look-up table:
  – Event
  – Location
  – Duration
• Examples:
  – Congestion
  – Accidents
  – Road work
Traffic Message Channel
Encrypted Location Codes

• Location codes: 16-bit for a given geographical area
• Encryption keys: 16-bit
• Schedule: One randomly chosen each day from 31 standard keys
• Receiver update: Key ID broadcast constantly
Daily Key ID

- Performing CODEC loopback test... pass
- Asking for clock rate 32 MHz
- Actually got clock rate 32 MHz
- Performing timer loopback test... pass
- Performing timer loopback test... pass
- Setting references to the internal GPSDO
- Initializing time to the internal GPSDO
- Starting...

```
>> bpsk demodulator enter looking
>> gr fir fft: using SSE
>> bpsk demodulator enter locked
Sync State Detected
First ENC ID: 27
```

```
# user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]
  current temperature (Q), location:5953
# user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]
  current temperature (Q), location:5953
# user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]
  current temperature (Q), location:5953
  location:0
```

```
# user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
# user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
  location:0
# user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
  location:0
# user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
# user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
  location:0
# user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
# user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
  location:0
# user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
# user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [1390]
  current temperature (Q), location:5953
  location:0
```

```
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [1160]
  current temperature (Q), location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [1160]
  current temperature (Q), location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [1160]
  location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [1160]
  location:5953
```

```
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1126 [1162]
  (0 probability of) sunny periods, location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1126 [1162]
  (0 probability of) sunny periods, location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1126 [1162]
  (0 probability of) sunny periods, location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1126 [1162]
  (0 probability of) sunny periods, location:5953
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1126 [1162]
  (0 probability of) sunny periods, location:5953
```

```
# user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1152]
  (0 probability of) sunny periods, location:5953
```
Patterns

- Always three unique temperature reports
  - Key: Event ID
  - Value: Location
- Group of three Event IDs always the ‘same’
- Encrypted Location IDs always the same for given Enc ID
- Event IDs identical for period of days/weeks
  - Can vary after some time, but ‘hidden’ (unobserved) value is always the same
‘Temperatures’

- Performing CODEC loopback test... pass
- Asking for clock rate 32 MHz
- Actually got clock rate 32 MHz
- Performing timer loopback test... pass
- Performing timer loopback test... pass
- Setting references to the internal GPSDO
- Initializing time to the internal GPSDO

Starting...

```
>> bpsk demodulator enter looking
>>> gr fir fft: using SSE
>>> bpsk demodulator enter locked
00:00:00 Sync State Detected
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]:current temperature (0), location:5953
First ENC10: 27
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]:current temperature (0), location:5953
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]:current temperature (0), location:5953
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1348 [0]: , location:0

Location: 5953 temperature: 1348

#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:1 segments, event:1349 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:1 segments, event:1349 [0]: , location:0
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [0]: , location:5953
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [0]: , location:5953
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:0 probability of sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:0 probability of sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:0 probability of sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:0 probability of sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:0 probability of sunny periods, location:52939
```
Patterns

<table>
<thead>
<tr>
<th>Days</th>
<th>Key ID (random each day)</th>
<th>Group Period</th>
<th>Hidden Plain ‘Location’</th>
<th>Transmitted over the air:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>P₁</td>
<td>L₁</td>
<td>Event = evt(period, plain location)</td>
</tr>
<tr>
<td></td>
<td>K₁</td>
<td></td>
<td>evt(P₁, L₁) : enc(K₁, L₁)</td>
<td>Location = enc(key of the day, plain location)</td>
</tr>
<tr>
<td></td>
<td>K₂</td>
<td></td>
<td>evt(P₂, L₁) : enc(K₂, L₁)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K₂</td>
<td></td>
<td>evt(P₂, L₂) : enc(K₂, L₂)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K₃</td>
<td></td>
<td>evt(P₂, L₃) : enc(K₂, L₃)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td>evt(P₃, L₁) : enc(K₃, L₁)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>P₂</td>
<td>L₂</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K₂</td>
<td></td>
<td>evt(P₂, L₂) : enc(K₂, L₂)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K₂</td>
<td></td>
<td>evt(P₂, L₃) : enc(K₂, L₃)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K₃</td>
<td></td>
<td>evt(P₃, L₂) : enc(K₃, L₂)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td>evt(P₃, L₃) : enc(K₃, L₃)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>P₃</td>
<td>L₃</td>
<td></td>
</tr>
</tbody>
</table>
Security Analysis

- 16-bit is **very** short
- Identical group of ‘location codes’ are broadcast on a daily basis
  - Unknown but re-used plaintext
- ‘Singular’ events can be correlated from a trusted source
  - Known plaintext
Singular Event from Trusted Source

US-101 S at SAUSALITO LATERAL RD. object on the road

Return
## Input Data

<table>
<thead>
<tr>
<th>Plain ‘Location’</th>
<th>L₁</th>
<th>L₂</th>
<th>L₃</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key ID</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K₁</td>
<td><code>enc(K₁, L₁)</code></td>
<td><code>enc(K₁, L₂)</code></td>
<td><code>enc(K₁, L₃)</code></td>
</tr>
<tr>
<td>K₂</td>
<td><code>enc(K₂, L₁)</code></td>
<td><code>enc(K₂, L₂)</code></td>
<td><code>enc(K₂, L₃)</code></td>
</tr>
<tr>
<td>K₃</td>
<td><code>enc(K₃, L₁)</code></td>
<td><code>enc(K₃, L₂)</code></td>
<td><code>enc(K₃, L₃)</code></td>
</tr>
<tr>
<td>K₄</td>
<td><code>enc(K₄, L₁)</code></td>
<td><code>enc(K₄, L₂)</code></td>
<td><code>enc(K₄, L₃)</code></td>
</tr>
<tr>
<td>K₅</td>
<td><code>enc(K₅, L₁)</code></td>
<td><code>enc(K₅, L₂)</code></td>
<td><code>enc(K₅, L₃)</code></td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

1. Bootstrap: find all possible plain locations & keys that result in `enc(K₁, L₁)`
2. Given those keys, find all possible plain locations recorded with that Key K₁ (i.e. L₂, L₃)
   - Remember pool of possible plain locations for each L & pool of possible keys for K
3. For each remaining K, repeat maintaining pool of possible keys for each K:
   - Find all possible keys given pool of possible plain locations for each L
   - Repeat, filtering pools until only one match remains
   - Remove item from pool when `enc(K, L) ≠` input data
Algorithm

Despite 16 bits, many potential keys/plain locations are generated at the start due to the nature of $\text{enc}(K, L)$.

Possible Plain Location Pools

$L_1$

$L_2$

$L_3$

Possible Key Pools

$K_1$

$K_2$

$K_3$

$K_4$

$K_5$

Iterate & Filter

<table>
<thead>
<tr>
<th>Plain ‘Location’</th>
<th>$L_1$</th>
<th>$L_2$</th>
<th>$L_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$K_1$</td>
<td>$\text{enc}(K_1, L_1)$</td>
<td>$\text{enc}(K_1, L_2)$</td>
<td>$\text{enc}(K_1, L_3)$</td>
</tr>
<tr>
<td>$K_2$</td>
<td>$\text{enc}(K_2, L_1)$</td>
<td>$\text{enc}(K_2, L_2)$</td>
<td>$\text{enc}(K_2, L_3)$</td>
</tr>
<tr>
<td>$K_3$</td>
<td>$\text{enc}(K_3, L_1)$</td>
<td>$\text{enc}(K_3, L_2)$</td>
<td>$\text{enc}(K_3, L_3)$</td>
</tr>
<tr>
<td>$K_4$</td>
<td>$\text{enc}(K_4, L_1)$</td>
<td>$\text{enc}(K_4, L_2)$</td>
<td>$\text{enc}(K_4, L_3)$</td>
</tr>
<tr>
<td>$K_5$</td>
<td>$\text{enc}(K_5, L_1)$</td>
<td>$\text{enc}(K_5, L_2)$</td>
<td>$\text{enc}(K_5, L_3)$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Location #</td>
<td>1 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>4603 11fb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>2 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4401 1131</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>3 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4172 104c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>4 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>5134 140e</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>5 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4193 1061</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>6 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4527 11af</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>7 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4329 10e9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>8 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>5611 15eb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>9 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4538 11ba</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>10 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4303 10cf</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>11 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4223 107f</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location #</td>
<td>12 has</td>
<td>1 possible plain codes</td>
<td></td>
</tr>
<tr>
<td>4834 12e2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>2 has</td>
<td>2 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>3 has</td>
<td>15 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>4 has</td>
<td>5 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>5 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>6 has</td>
<td>3 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>7 has</td>
<td>5 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>8 has</td>
<td>7 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>9 has</td>
<td>2 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>10 has</td>
<td>34 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>11 has</td>
<td>1 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>12 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>13 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>14 has</td>
<td>2 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>15 has</td>
<td>2 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>16 has</td>
<td>3 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>17 has</td>
<td>3 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>18 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>19 has</td>
<td>6 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>20 has</td>
<td>1 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>21 has</td>
<td>2 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>22 has</td>
<td>3 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>23 has</td>
<td>3 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>24 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>25 has</td>
<td>6 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>26 has</td>
<td>1 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>27 has</td>
<td>3 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>28 has</td>
<td>1 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>29 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>30 has</td>
<td>2 possible keys</td>
<td></td>
</tr>
<tr>
<td>Encryption ID</td>
<td>31 has</td>
<td>4 possible keys</td>
<td></td>
</tr>
</tbody>
</table>
Results

• Convergence expedited by addition of ‘singular’ events
  – “vehicle fire(s)”
  – “flooding”
  – “object(s) on roadway {something that does not necessarily block the road or part of it}”

• Even though multiple keys exist for a Key ID, with enough data plain location search yields one match!
Aviation RADAR

Hacking the Wireless World with #sdr  @spenchdotnet
ATCRBS, PSR & SSR

- **Air Traffic Control Radar Beacon System**
  - **Primary Surveillance Radar**
  - **Secondary Surveillance Radar**

**Primary:**
- Traditional RADAR
- ‘Paints skins’ and listens for return
- Identifies and tracks primary targets, while ignoring ‘ground clutter’
- Range limited by RADAR equation \( \frac{1}{d^4} \)
ATCRBS, PSR & SSR

- **Air Traffic Control Radar Beacon System**
  - **Primary Surveillance Radar**
  - **Secondary Surveillance Radar**

Secondary:
- Directional radio
- Requires transponder
- Interrogates transponders, which reply with squawk code, altitude, etc.
- Increased range \(\frac{1}{d^2}\)
<table>
<thead>
<tr>
<th>Icon</th>
<th>Freq</th>
<th>Em Des</th>
<th>Client</th>
<th>Links</th>
<th>Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.85 GHz</td>
<td>5M50P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.65 GHz</td>
<td>5M90P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.47 GHz</td>
<td>2.84725 GHz - 2.85275 GHz, VZN930</td>
<td>THALES ANTENNAS (AN20005)</td>
<td>17000W</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.76 GHz</td>
<td>4M90P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.75 GHz</td>
<td>5M50P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.75 GHz</td>
<td>5M90P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.08 GHz</td>
<td>3M75P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.00 GHz</td>
<td>4M00P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.03 GHz</td>
<td>3M75P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.00 GHz</td>
<td>4M00P0N</td>
<td>Airservices Australia</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Primary Surveillance RADAR

- Transmits a ‘bang’ (the main pulse)
- Listens for returns (echoes)
The Modes

- **A**: reply with squawk code
- **C**: reply with altitude
- **S**: enables **Automatic Dependant Surveillance-Broadcast (ADS-B)**, and the **Aircraft/Traffic Collision Avoidance System (ACAS/TCAS)**
The Modes

• **A**: reply with squawk code
• **C**: reply with altitude
• **S**: enables Automatic Dependant Surveillance-Broadcast (ADS-B), and the Aircraft/Traffic Collision Avoidance System (ACAS/TCAS)

• Mode S not part of ATCRBS, but uses same radio hardware (same frequencies)
  – Increasing problem of channel congestion
Position
Heading
Altitude
Vertical rate
Flight ID
Squawk code
A Typical 747 has...

- 2 x 400 W voice HF
- 3 x 25 W voice/data VHF
- 2 x 100 W 9GHz RADARs
- 2 x GPS, 1.5GHz 60 W voice/data SATCOM
- 2 x 75MHz marker beacons
- 3 x VHF LOC localiser
- 3 x UHF glide slope
- 2 x LF ADF automatic direction finder
- 2 x VOR VHF omni-directional range
- 2 x 1GHz 600 W transponders
- 2 x 1GHz 700 W DME distance measuring equipment
- 3 x 500mW 4.3GHz radar altimeters
- 3 x 406MHz EPIRB
TCAS
Xpndr
High gain SATCOM
Low-gain VHF
VHF
DME
ADF
EPIRB
Marker
RADAR
Altimeter
HF
Mode S Response Encoding

- Data block is created & bits control position of pulses sent by transmitter

Example.— Reply data block corresponding to bit sequence 0010...001

Pulse Position Modulation (AM)
Pulse Position Modulation

• Pulse lasts \textbf{0.0000005 seconds} (0.5 µs)
• Need to sample signal at a \textbf{minimum of 2 MHz} (assuming you start sampling at precisely the right moment and stay synchronised)
• Requires high-bandwidth hardware and increased processing power
• Ideally, oversample to increase accuracy
Mode S Frame
Mode S Response: AM signal
Welcome to Aviation Mapper

Click here for info, feedback and to share - if you like this, let me know.

I need to find a new receiver site near the airport ASAP please help!
Welcome to Aviation Mapper

Click here for help, feedback and to share - if you like this, let me know.

I need to find a new receiver site near the airport ASAP - please help!

22:27:09 AEST
05:27:08 UTC
Mode: OK
ACARS: OK

Auto Balloons
Trail
Trails need more CPU

Google earth
Welcome to Aviation Mapper

Click here for info, feedback and to share - If you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!

H1 ‘System and engineering data’ regarding the (failure of) toilets?

http://maps.spench.net/aviation/
Welcome to Aviation Mapper
Click here for info, feedback and to share - if you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!

http://maps.spench.net/aviation/

International & cross-country flight paths sent as flight plans using IFR waypoints
Primary Surveillance
RADAR

Hacking the Wireless World with #sdr  @spenchdotnet
Moffett Field ASR-9
Primary Surveillance Radar
Primary Surveillance RADAR
Primary Surveillance RADAR
# Dual PRF Mode: Weather

## TABLE 1

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>2.7 GHz</td>
</tr>
<tr>
<td>Peak Power</td>
<td>1.1 MW</td>
</tr>
<tr>
<td>Pulse Length</td>
<td>1 ms</td>
</tr>
<tr>
<td>Pulse Repetition Frequency</td>
<td>Dual PRF (1160 Hz average)</td>
</tr>
<tr>
<td>Antenna Gain</td>
<td>34 dB</td>
</tr>
<tr>
<td>Azimuth Beamwidth</td>
<td>1.4°</td>
</tr>
<tr>
<td>Elevation Beamwidth</td>
<td>4.8°</td>
</tr>
<tr>
<td>Rotation Rate</td>
<td>12.5 rpm</td>
</tr>
<tr>
<td>Range Gate Spacing</td>
<td>116 m</td>
</tr>
<tr>
<td>Azimuthal Resolution</td>
<td>1.4°</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>1 m$^2$ @ 111 km</td>
</tr>
<tr>
<td>System Stability</td>
<td>48 dB</td>
</tr>
</tbody>
</table>

Radar energy entering this trapping layer can be refracted through an effective curve with a radius smaller than that of the Earth, returning to scatter off the surface some distance from the radar. If the layer is of large horizontal extent radar energy scattered back into the atmosphere from the surface after this process can be trapped a second time, and in this way a surface duct can be formed which may carry energy to large distances beyond the unambiguous range of the radar and return multiple-trip echoes by the same ray path. These echoes will display at arbitrary ranges on the PPI (the residual between some multiple of the unambiguous range and the true range to the remote reflector), but at the true azimuth of the reflector. Note however the dual PRF technique employed by the ASR-9 radars, which should eliminate multiple-trip returns.
'Bang'
Magnitude Histogram
Magnitude Histogram
Above Noise Floor
Above Noise Floor
Pulse Length Histogram
Pulse Envelope
Pulse Envelope
Pulse Envelope
Strong Pulse Separation
PRF Histogram
Strong Pulses vs. Time
Strong Pulses vs. Time (zoomed)
Pulse Power vs. Time
Pulse Power vs. Time (zoomed)
Distance Between Pulses
Pulse and echo power over time
Raw RADAR Return Plot

Each scanline is synchronised to an emitted pulse

Scanline is amplitude of samples over time (also range of the return)
LAS ASR-9
Distortion Map

Monostatic

Bistatic

Angle  Distance  2D Offset
Multipath

Hacking the Wireless World with #sdr

@spenchdotnet
PN511
Correlation Peaks
RFID

Hacking the Wireless World with #sdr

@spenchdotnet
FasTrak

- Traffic toll tag
  - Contains your ID
- Interrogation signal in 900 MHz ISM band
  - ‘Wake up’ signal activates tag
  - Pulse-Position Modulated payload
- Tag replies with backscatter modulation
  - Reflects transmitter’s RF energy (tiny amount)
  - Modulates reflection with Frequency Shift Keying
Highway to Hell: Hacking Toll Systems

Nate Lawson
Blackhat USA
2008/8/6
Interrogation Signal

Wake up

Payload

Preamble

Backscatter carrier
Wake Up/Preamble
Interrogation Payload
Backscatter Carrier
Interrogation Signal

(no tag detected)
Received Signal

Interrogation

CW

(no tag detected)
Received Signal

Scope Plot

Response

FFT Plot

147
Received Signal
Frequencies correspond to data bits 0 and 1 respectively. The message information is conveyed by the subcarrier modulation frequencies of the transponder backscattered signal and not by amplitude of phase.

b. Data Bit Rates.
The data bit rate for transponder-to-reader data messages shall be 300 kbps.

c. Field Strength.
The field strength at which a transponder data message is transmitted using backscatter technology is dependent upon the incident field strength from the reader, the transponder receive and transmit antenna gains, and any RF gain internal to the transponder. The transponder and antenna gain taken together shall effect a change in the backscattering cross section of between 45 and 100 square centimeters.

The standard portion of a transponder data message shall consist of a header and transaction record type code. The subsequent length, data content and error detection scheme shall then be established by the definition for that transaction record type.

e. Transponder Data Message Formats for AVI Toll Collection.
There may be numerous transponder-to-reader data message formats. The format is determined by the transaction record type code sent by the transponder. The following is the reader-to-transponder message format presently specified for AVI electronic toll collection applications:

1. Transponder Transaction Type 1 (Data Message)
   Transponder transaction type 1 (data message) allows for unencrypted transponder ID numbers to be transmitted. Type 1 (data messages) shall be structured using the following ordered data bit fields:

   Field Definition                           No. Bits | Hexadecimal Value
   Header Code:                              
   Selsyn                                    8        | AA
   Flag                                      4        | C
   Transaction Record Type Code              16       | 1
   Transponder ID Number                     32       |
   Error Detection Code                      16       |
   Total:                                    76       |

f. Transponder End-of-Message Frame
The End-of-Message signal for transponder data messages shall consist of a minimum of 10 microseconds of no modulation.
Preamble Detection

(no tag detected)
Preamble Detection

Matched Preamble Filter Response

Scope Plot

Counts

Time (ms)

14 7
Slicer Time!

Sample bits

14 17
Reading a Tag Outside
Frequency-domain Amplitude (LF)
Time-domain Amplitude (LF)
Time-domain Amplitude (LF)
Frequency-domain Amplitude (UHF)
Time-domain Amplitude (UHF)
baudline Dual FFT

LF

UHF
GNU Radio ➔ baudline
GNU Radio + baudline
Time-domain Amplitude
Time-domain Amplitude
Time-domain Amplitude
ISEE-3 Reboot Project

Hacking the Wireless World with #sdr

@spenchdotnet
Total Delta V Requirement to Bring ISEE-3 Back to L1

Delta V m/s

Max Fuel

pre-Arecibo

Arecibo Radio Observatory
Ionospheric heaters
Still a good start...
Weak Signal $\Rightarrow$ Low RBW
numpy & matplotlib
After Improving Pointing

- \( \sim 45 \text{ dB C/N} \)
- Moving peak below due to Doppler shift
Verifying Transmitted Signal

B200 receiving ‘leakage’ from dish
Moment of First Contact

Happy Dance
Dual Channel Recording
Raw Captured Baseband

PLL tracking carrier
PLL Lock
Propulsion System
Telemetry: 16 bps
Telemetry: 64 bps
Telemetry: 512 bps
Telemetry: 2048 bps
Telemetry During Thruster Firing
No Thrust
Hydrazine Propulsion System
New Orbit
A SPACECRAFT FOR ALL

The ISEE-3 was launched to study the Sun in 1978, but ended up redefining space flight. Now it's on a new mission to become citizen science's first spacecraft, with data accessible by everyone.

SEE THE JOURNEY  SEE LIVE VIEW
#cyberspectrum
Other Applications

Hacking the Wireless World with #sdr

@spenchdotnet
Blind Signal Analysis
What you need

Dish + LNB + power injector + USRP + GNU Radio

(set-top box with LNB-thru)
D1 TLM1: 12243.25 MHz

Mirror of RHS*

Constant carrier power*

TLM sidebands

Constant sub-carrier

1PPS

Beacon with Phase Modulation* (PM): 1PPS and two telemetry streams (sidebands)
Let’s try one...

- Feed entire baseband spectrum into GR
- Perform ‘channel selection’ to isolate stream of interest (create new baseband centred on stream)
Frame analysis

- Header
  - SYN SYN SYN (EBCDIC)
- Character-oriented encoding:
  - SOH
  - STX
  - ETX
  - CRC (CCITT-16)
- Numbers of fixed-length messages
  - Each contains an ID
Un-pack & find patterns

Message header

16-bit signed

8-bit signed

BCD
Graphing the Data
Software Defined Radio Direction Finding
SDR Direction Finding

RF Hardware

Software-Defined Radio

Direction Finding

Antenna Array

The DUF-Mobile

Mapping Software

Known transmitter location (red X)

Direction measurements

Balint Seeber
http://spencher.net/
QuadRadio: Super-resolution Direction Finding

Gain 1: -16  Gain 2: -16  Offset: -11.0335k

Squelch Threshold: -60  Demod Squelch Threshold: -45

Freq: 900M  DOA: 30.9712905  Fire: 0.0

Audio: 1

FFT Plot

TARGET LOCK

Squelched: 1

Trace Options
- Peak Hold
- Average
- Avg Alpha: 0.5000
- Persistence
- Persistence Alpha: 0.1755

Trace Options
- Trace A
- Trace B

Axis Options
- dB/Div:
- Ref Level:
- Autoscale

FFT
Two WiFi channels, and then some...
FLEX Pagers & Baudline
900 MHz ISM – Smart Meters
3G W-CDMA

Signature of UMTS: repeating data in CPICH at 10 ms intervals
No apparent signal

Cyclic 1023 bit code @ 1.023 MHz chip rate
gnss-sdr: Decoding L1
TETRA

Fast AutoCorrelation

Repeating idle pattern

Scope Plot

Frequency correction burst
The Entire HAM Band
OpenBTS

• Open-source 2G GSM stack
  – Asterix softswitch (PBX)
  – VoIP backhaul
LTE eNodeB on USRP N2xx

- eNB software
- VLC streaming client (me taking photo seen by laptop below)
- Spectrum (waterfall plot) of uplink from LTE dongle
- Webcam streaming via VLC over LTE IP link
- Vodafone Surfstick (consumer LTE dongle)

N210 eNB basestation

Ettus Research
802.11agp (OFDM) Decoding
Automatic Picture Transmission
Automatic Identification System