Pager inSecurity v1.1

Retro (Legacy) Action

© 1995 2014, Andrew Horton
Agenda

• What’s a pager?
• Who is using pagers?
• There is no pager security
• What pager messages look like
• Who is intercepting pager messages?
• Pager protocols (POCSAG & FLEX)
• Receiving pager frequencies (Modifying pagers, Radio Scanning, Software Defined Radio)
• Software to decode pager messages
• Pager frequencies in Australia (how to find them)
• Legal issues
• Online pager databases
• Security issues
• How to decode pager messages
Pagers

Tone/Vibrate Only

Numeric Pagers

AlphaNumeric Pagers

Restaurant Pagers are a different technology
Pager users before
Pager users now

- Healthcare workers
- Emergency vehicles
- Security patrols
- Courier drivers
- System administrators
- Gangstas
- Businessmen
Why are they still using pagers?

TXT messages aren’t reliable enough
TXTs can take hours to deliver, or are never delivered.

Advantages of pagers over TXT messages
– Longer battery life
– Larger coverage area
– Higher availability
– Immediate delivery
– Can set up your own internal pager service
Pager security

There is no pager security

Messages are sent one-way in plaintext across a large geographic area.
<table>
<thead>
<tr>
<th>Address</th>
<th>Time</th>
<th>Date</th>
<th>Protocol</th>
<th>Type</th>
<th>BPS</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>0362617</td>
<td>23:50:00</td>
<td>28-01-12</td>
<td>POCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>KINGSTON 57 CODE 9 13 CASUALTIES 1 TRANSPORT ETA 20 MINS TO DEPOT JULIE 0421-118-962</td>
</tr>
</tbody>
</table>
Who is listening?

Hobbyists who like HAM radio, tracking trains, fire, etc
People monitoring emergency broadcasts
There is a thriving community at www.aussiescanners.com/forum/
Who else is listening?

• Stalkers?
• Towing companies (illegal)
• Private investigators / Journalists
• BlackHat hackers
  – Appeared in Phrack in 1994
• Security consultants
Pager protocols

The main pager protocols are

POCSAG  FLEX  ERMES

• **POCSAG Protocol**
  – Most common in Australia
  – Developed by the British Post Office in 1981
  – TONE Only, Numeric, Alphanumeric
  – Speeds: 512, 1200, 2400 bps
  – FSK Modulation with a +/- 4.5 kHz shift on the carrier.
  – Alphanumeric messages are encoded in 7 bit ASCII.
Pager protocols

• **FLEX protocol**
  – Commonly used in Australia
  – Developed by Motorola in 1993
  – Only AlphaNumeric
  – Speeds: 1600, 3200, 6400 bps
  – 2 Level FSK (1600, 3200)
  – 4 Level FSK (3200, 6400)

  – Believed (erroneously) to to be more secure than POCSAG

• **ERMES protocol**
  – European Radio Messaging System
  – 4 Level FSK
Receiving pager radio frequencies

**Software Defined Radio**
- Costs under $20 on eBay
- Very large frequency range: 100KHz to 1.5GHz

**Radio scanner**
- Costs about $100-$300
- Gaps in frequency ranges
- Optional discriminator mod, and data slicer

**Modified pager**
- Costs about $20-$100
- Fixed frequency
- Output to serial
Hack a pager

- Costs about $20-$100
- Audio or serial RS232 output
- Decode with software
- Requires soldering
- Fixed frequency
- Instructions for Motorola Bravo, Apollo, and many others
Decoding pager messages with a radio scanner

- Costs about $100-$300
- Radio scanner with headphone jack connected to sound card with line-in
- Use software to decode pager messages
- Scanners have gaps in frequencies ranges (not a problem for pagers)

- Unmodified radio scanner
  - Turn squelch off
  - Carefully find best volume for decoding
  - Can’t decode FLEX messages (2400 BPS+)
Discriminator taps for radio scanners

- A discriminator tap provides an unfiltered audio jack
- Bypass squelch and audio filters
- Decode higher data rates (2400 BPS)
- More reliable decoding

- Discriminator.nl has instructions for
  - Uniden Bearcat
  - Realistic
  - Commtel
  - Albercht
  - AOR
  - Atron
  - GRE
  - And many more

Data slicers for radio scanners

- Audio input from radio scanner
- Serial RS232 output
- Better with discriminator tap

- 2 Level FSK data slicer
  - Hamcomm modem
- 4 Level FSK data slicer
  - Faster protocols like FLEX & ERMES

- Instructions at http://discriminator.nl/2-level/index-en.html
- Buy a 4 level FSK for EUR 50.00
SDR (Software Defined Radio)

Costs under $20 on eBay
Cheap SDR units designed for TV

Very large frequency range
   – 100KHz to 1.5GHz
Look for the RTL2832 chipset
Windows and Linux drivers
Thriving open-source community

Can be used for
- Decoding pagers
- Watching TV (HD)
- Listening to the radio
- Satellite TV finder (with dish)
- Radio Astronomy (wish dish)
- Passive RADAR

Software and articles at www.rtl-sdr.com
Pager decoding with SDR

Make audio available to other apps using virtual audio cables
Configuring SDR Sharp

Select Frequency

Narrow band FM

Turn off squelch

Set sample rate 48000

Set AF Gain (high)

Select output audio device (virtual cable)
Pager Decoding Software

- **PDW**
  - Best
  - Windows
  - Open source since 2013
  - Works with audio, data slicers, serial, etc
  - POCSAG, FLEX, ERMES, ACARS
  - [http://www.gsm-antennes.nl/PDW/](http://www.gsm-antennes.nl/PDW/)

- **Multimon**
  - Linux
  - POCSAG, AX.25, DTMF and ZVEI
  - [http://www.baycom.org/~tom/ham/linux/multimon.html](http://www.baycom.org/~tom/ham/linux/multimon.html)
Finding pager frequencies

Frequencies commonly used
43 MHz    148 MHz    450 MHz

Australian Government Frequency Allocation
# Client Details

<table>
<thead>
<tr>
<th>Client Number</th>
<th>20012076</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation Name</td>
<td>Vodafone Hutchison Australia Pty Limited</td>
</tr>
<tr>
<td>Trading Name</td>
<td>Attention : Justin Nelson</td>
</tr>
<tr>
<td>Postal Address</td>
<td>PO Box 1113 NORTH SYDNEY NSW 2060</td>
</tr>
<tr>
<td>ACN</td>
<td>096304620</td>
</tr>
<tr>
<td>ABN</td>
<td>76096304620</td>
</tr>
<tr>
<td>Fee Status</td>
<td>Normal</td>
</tr>
</tbody>
</table>

[ New Client Search ]
[ 400MHz Licences ]

# Licences Held

Results 1 - 50 of 455 licences.

<table>
<thead>
<tr>
<th>Licence No</th>
<th>Licence Type</th>
<th>Licence Category</th>
<th>Callsign</th>
<th>Ship name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1943608</td>
<td>Fixed</td>
<td>Point to Point</td>
<td>VMH960</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1943607</td>
<td>Fixed</td>
<td>Point to Point</td>
<td>VMH959</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1947526</td>
<td>Fixed</td>
<td>Point to Point</td>
<td>VZT823</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1901200</td>
<td>Fixed</td>
<td>Point to Point</td>
<td>VLB229</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1142402</td>
<td>Fixed</td>
<td>Point to Point</td>
<td>AXF287</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1433222</td>
<td>Fixed</td>
<td>Point to Point</td>
<td>VL2HUT</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1143221</td>
<td>Land Mobile</td>
<td>Paging System - Exterior</td>
<td>VNG455</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1143219</td>
<td>Land Mobile</td>
<td>Paging System - Exterior</td>
<td>VNG453</td>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td>1143218</td>
<td>Land Mobile</td>
<td>Paging System - Exterior</td>
<td>VNG452</td>
<td></td>
<td>Issued</td>
</tr>
</tbody>
</table>
### Licence Details

<table>
<thead>
<tr>
<th>Licence Number</th>
<th>1143221</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Vodafone Hutchison Australia Pty Limited</td>
</tr>
<tr>
<td>Status</td>
<td>Issued</td>
</tr>
<tr>
<td>Licence Type</td>
<td>Land Mobile</td>
</tr>
<tr>
<td>Licence Category</td>
<td>Paging System - Exterior</td>
</tr>
<tr>
<td>Callsign</td>
<td>VNG455</td>
</tr>
<tr>
<td>Date of Effect</td>
<td>19-APR-13</td>
</tr>
<tr>
<td>Date of Expiry</td>
<td>18-APR-14</td>
</tr>
</tbody>
</table>

**Advisory Notes:** Conditions applicable to the operation of Paging System station(s) authorised under this licence can be found in the Radiocommunications Licence Conditions (Apparatus Licence) Determination and the Radiocommunications Licence Conditions (Land Mobile Licence) Determination. Copies of these determinations are available from the ACMA and from the ACMA home page (www.acma.gov.au).

**NOTE:** There may be additional text attached to the assignment associated with this licence.

### Assignments for this Licence

<table>
<thead>
<tr>
<th>ID</th>
<th>Frequency</th>
<th>Emission Designator</th>
<th>Site Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>8163797-8157761</td>
<td>148.6375 MHz</td>
<td>16K0F2D</td>
<td>Fire Station Taloom St YELARBON (9000161)</td>
</tr>
</tbody>
</table>
Licence Details

<table>
<thead>
<tr>
<th>Licence Number</th>
<th>1310372</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Crown Melbourne Limited</td>
</tr>
<tr>
<td>Status</td>
<td>Issued</td>
</tr>
<tr>
<td>Licence Type</td>
<td>Land Mobile</td>
</tr>
<tr>
<td>Licence Category</td>
<td>Paging System - Interior</td>
</tr>
<tr>
<td>Callsign</td>
<td>VJF649</td>
</tr>
<tr>
<td>Date of Effect</td>
<td>18-SEP-13</td>
</tr>
<tr>
<td>Date of Expiry</td>
<td>17-SEP-14</td>
</tr>
</tbody>
</table>
| Advisory Notes          | Conditions applicable to the operation of Paging System station(s) authorised under this licence can be found in the Radiocommunications Licence Conditions (Apparatus Licence) Determination and the Radiocommunications Licence Conditions (Land Mobile Licence) Determination. Copies of these determinations are available from the ACMA and from the ACMA home page (www.acma.gov.au).

NOTE: There may be additional text attached to the assignment associated with this licence.

[ New Licence Search ]

Assignments for this Licence

<table>
<thead>
<tr>
<th>ID</th>
<th>Frequency</th>
<th>Emission Designator</th>
<th>Site Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1308222-1306378</td>
<td>148.3375 MHz</td>
<td>16K0F3E</td>
<td>Crown Casino Site SOUTHBANK (100126)</td>
</tr>
</tbody>
</table>
Pager Frequencies in Victoria

• Orange / Hutchison
  – 148.5625 - F1
  – 148.6375 - F2 (Best)

• SAGRN
  – 148.8125 - FLEX 1600

• Hospital Paging (Local)
  – 148.3375

• Emergency Altering System
  – 148.9125 Mhz

• Need to update this list
Sending pager messages

This varies between countries

• Vodafone paging 24 hour call centre
• SMS to pager gateway
• E-mail to pager
• Web to pager
• Via modem and X25
Legal issues

• Each country has it’s own rules regarding pager decoding.

• In Australia and New Zealand you cannot act on the data you decode.

• Illegal ‘acting on information’ includes tow-truck companies that monitor pagers to locate car crashes.
Online pager message databases

• Australia
  – Provided by the South Australian Country Fire Service
  – Live feed, includes Fire, Emergency, Security Patrols
  – paging1.sacfs.org

• Wikileaks
  – 573,000 pager messages from 9/11/2001
  – 911.wikileaks.org
Security issues

• No encryption / messages are in clear-text
• No assurance of message receipt
• No message sender identity assurance

• Message contents can be sensitive
  – Passwords and PIN codes
  – Locations of physical keys
  – Disclosure of names, usernames, IP addresses, hostnames, IT systems used

• Privacy compliance problems
  – Hospitals send personally identifiable information (PII) including names, addresses, and medical details

• Pager messages often fall outside the scope of penetration testing and security assessments.
<table>
<thead>
<tr>
<th>Address</th>
<th>Time</th>
<th>Date</th>
<th>Mode</th>
<th>Type</th>
<th>Bitrate</th>
<th>Monitored Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>0880622</td>
<td>15:01:15</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>512</td>
<td>AUTOMATED TEST PAGE</td>
</tr>
<tr>
<td>0003461</td>
<td>15:01:16</td>
<td>29-03-12</td>
<td>FOCSAG-1</td>
<td>NUMERIC</td>
<td>512</td>
<td>TONE ONLY</td>
</tr>
<tr>
<td>0880692</td>
<td>15:01:36</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>512</td>
<td>TONE MESSAGE FROM 3 MESSAGING</td>
</tr>
<tr>
<td>0544721</td>
<td>15:01:42</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>15:01 Southwark D3 9099 1208 ERN W. - HARDWARE/OTHER — Please call southwark store regarding moving of computer. Ben</td>
</tr>
<tr>
<td>0425580</td>
<td>15:01:49</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>At 15:01:20. The Point UCA4F is in Alarm. Informational Text: Compressed Air Unit No4 has faulted.</td>
</tr>
<tr>
<td>0390590</td>
<td>15:01:44</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>RE: EVENT: F120303366 — STOP MESSAGE RECEIVED</td>
</tr>
<tr>
<td>0407110</td>
<td>15:01:45</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>15:07 23/3 colemae: Recourt’s CTPA report ready? Celina</td>
</tr>
<tr>
<td>0446719</td>
<td>15:01:46</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>H1 Martina, r u still around? 4 admissions coming, one already here. PAW 51433</td>
</tr>
<tr>
<td>0410905</td>
<td>15:01:46</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>stella herland 0404 978896 non urg</td>
</tr>
<tr>
<td>0407092</td>
<td>15:01:49</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>18:07 29/3 matthai: Chris. p446 x4201. Re Curoia 61406 referral re venous/arterial ulcera.</td>
</tr>
<tr>
<td>0390590</td>
<td>15:01:49</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>ALPHA</td>
<td>1200</td>
<td>RE: EVENT: F120303366 — STOP MESSAGE RECEIVED</td>
</tr>
<tr>
<td>0003461</td>
<td>15:01:52</td>
<td>29-03-12</td>
<td>FOCSAG-1</td>
<td>NUMERIC</td>
<td>512</td>
<td>TONE ONLY</td>
</tr>
<tr>
<td>0003461</td>
<td>15:02:19</td>
<td>29-03-12</td>
<td>FOCSAG-1</td>
<td>NUMERIC</td>
<td>512</td>
<td>TONE ONLY</td>
</tr>
<tr>
<td>0003461</td>
<td>15:02:42</td>
<td>29-03-12</td>
<td>FOCSAG-3</td>
<td>NUMERIC</td>
<td>512</td>
<td>TONE ONLY</td>
</tr>
<tr>
<td>0003461</td>
<td>15:02:59</td>
<td>29-03-12</td>
<td>FOCSAG-1</td>
<td>NUMERIC</td>
<td>512</td>
<td>TONE ONLY</td>
</tr>
</tbody>
</table>
Getting set up

• Search eBay for a SDR RTL
Setup: Get PDW

PDW Paging Decoder Software

Introduction
Since 2003, Peter Hunt has developed PDW to the most important (free!) application to monitor FLEX. PDW has many users worldwide, from radio enthusiasts to professionals. After 10 years of development PDW as finished and he has stopped development. Peter, thank you for all your efforts! Made Open Source. You can read more about that below.

As of March 2013, this site is the official host for PDW.

Download
The latest PDW version can be found here:
- PDW v3.12 (zip) - Current Open Source release
- PDW v3.1 (zip) - Final version developed by Peter Hunt
- PDW Manual (pdf)
- LogBrowser (zip) - description
Setup: VB-CABLE

VB-CABLE TECHNOLOGY

VB-Audio CABLE is a Windows Audio Driver working as Virtual Audio Cable. After installing the VB-CABLE driver, a new playback device appears in the audio device list and can be set as default device.

VB-CABLE can be set as default device, as any regular audio device. The Configure and Properties buttons allow to setup multi channel features and device sound quality.

VB-CABLE APPLICATIONS

VB-CABLE allows routing signal from an application to another one. Typical application for the Virtual Audio Cable is to route your sound to an audio software in order to record and analyze it...

From whatever audio sources...

To whatever audio software...

...supporting MME, DX or WDM Audio Device Drivers...

VB-CABLE Driver (Donationware)
Virtual Audio MME, DX, WDM Device Driver (XP, VISTA, WIN7, WIN8 32/64 bits).
VBCABLEDriver_Pass42b.zip (1.01 MB - JUL 2013).

Download
Setup: Get SDRSharp
Setup: The latest SDRSharp ZIP

If you like this software, please support it by donating money, hardware (preferred) or simply write a good documentation and spread the word.

Donate

RECENT POSTS
- ADSB# – A simple and cheap ADS-B receiver using RTL-SDR
- Contributors
- Automatic IQ Correction Algorithm
- Source code

RECENT COMMENTS
- lu3aeo on Welcome
- zabex on Welcome
- lu3aeo on Welcome
- Annunaki on Welcome
- jvdil on Welcome

parts, and under the MS-RSL for the DSP.
As such, **you can:**

- Create, Modify and Redistribute plugins
- Create, Modify and Redistribute the GUI in both forms under a different name (it’s no longer SD copyrights and licenses

But **you cannot:**

- Modify or Redistribute the DSP (SDRSharp.Radio code)

**Important note for RTL-SDR users**
You can use this quick installation script to test the
http://sdrsharp.com/downloads/sdr-install.zip
A step by step installation instructions can be found
http://rtlsdr.org/softwarewindows
http://rtlsdr.org/softwarelinux
To get started with SDR# you may be interested b from Henry (N2VFL):
Setup: Unpack
Setup: Install VB Cable
Setup: Zadig
Setup: SDRSharp
Setup: SDRSharp Output
Setup: PDW Input
Setup: VB Cables
Thank you for listening (in)
Learn more

Buy an SDR
  •  Search ebay for sdr. Look for the RTL2832U chip
Pager Decoding Software
  •  www.gsm-antennes.nl/PDW/
SDR Sharp
  •  sdrsharp.com
RTL SDR
  •  Blog about SDR
Pagers and FLEX
  •  www.nettwerked.net
The Wonderful World of Pagers by Erik Bloodaxe
  •  Phrack Issue Forty-Six
Radio Scanner Discriminator Mods
  •  www.discriminator.nl
Australian Frequency Allocation
  •  web.acma.gov.au
Database of Australian SAGRN Pager Messages
  •  www.sascan.net.au
Live pager messages in NSW
  •  paging1.sacfs.org
Wikileaks pager messages from 9/11/2001
  •  911.wikileaks.org