The World of Pager Sniffing and Interception:
More Activity than one may suspect.

Music: The Cools Kids – Gold and a Pager

The idea is to let the music play while folks enter the room then move on to the next slide.

(Point out the obvious) Pager interception was once well documented and "wildly" done within certain groups. Therefore I’m no trailblazer or am I? Old tech is not bad tech, its dated, its documented, but still useable and interesting. The idea is to re-introduced the activity with some ideas that may of not been available in the early to mid 90’s.

I want to stress again that OLD TECH IS NOT BAD TECH…if anything its tried and tested.

*note* I probably should of removed or just covered up the text in that screen capture… What do you see when you read it.
"Do not go where the path may lead, go instead where there is no path and leave a trail."
- Ralph Waldo Emerson

― "Everything that was or ever is began with a dream."
- Lava Girl

Quote (1) : Pager interception has been done, therefore the path has been made so how does this relate? Things evolve over time this is no exception so I encourage all to find the new path. The challenge to reinvent, rethink, and retool is open to all... amateur SIGINT (radio monitoring) is a blast (expensive) join the ranks and help the hobby.

Quote (2) : Don’t be afraid to think outside of the box. Try your concepts sometime things just work.
Who is this guy?

- **Nicks:**
  Steve from Idaho, Snuffalupagus, NYCMIKE and Dr. Love and a few others.

- **Work History:**
  Busboy at a local banquet hall, Gas station clerk (slurpe tech), Public service.

- **Hobbies:**
  Electronics, SIGINT (explain), making stuff and breaking stuff.

I’m just a guy in love with radio. If you want to drop me some knowledge in this field please do so at one of the following places: irc (irc.2600.net #telephreak/#radio/#make/#ca2600) or the Telephreak voice bridge (www.telephreak.org). Chances are I will not be there under the name NYCMIKE so just ask the question in #telephreak.
Okay off the bat lets agree that with the exception of niche markets pager technology has been replaced. Cost used to be the factor that favored the pager, that is no longer the case. An advantage the pager will have as long as its network is active, is signal penetration and strength. The signal is offset so that gaps or “shadows” are filled. Once you get the setup configured and going you’ll have hours of entertainment (For me this is the case).

There is traffic and it can be juicy; e.g. several companies hold telephone conference calls (which means they page the conf number and pass code, which COULD lead to a non invited party to lurk on the line), SANDIA sends msg similar to “Call Ralph at XYZ corp and here is his number”, DHS could be sending out SA updates, DOT……, BOP offers the happenings of correctional institutes (lock down or hey we found dope in a glassine bag buried in inmate JOHN DOE’s anal cavity), Sporting events (numbers and lines), the hospital data is disturbing due to the amount of info given out (patients name and complaints, not to mention lab results), The phone conferences are just asking to be recorded…

The thing to note is that this mode of communications is still in use and still very much visible. Keep in mind that at face value some data may not seem useful and it may not be to some, BUT the fact is this sort of information is what can be useable in SE operations.
Learning Objectives

- Refreshing on Pager Technology
  - Cap Codes, Protocols (POCSAG/ Flex/ Golay/ Ermes),
- Laws governing the interception and decoding of pager traffic.
- Data Slicers
- Discriminator taps

Q: How do pagers work?
A: RF, A intends to send a msg to B, A's msg enters the network.... sat, transmitters on cell phone towers
Common protocols are pocsag and flex in the US...
These are the two I hear the most, therefore this is what I'll cover.
Q: CapCodes?
A: unique ID’s, unit will only activate when it hears its ID/CAPCODE over the air
Q: Data Slicers?
A: Converts analog and digital (FSK)
Q: Discriminator tap?
A: Base band audio
Q: illegal?
A: Not always

Note I’ve added golay/ermes BECAUSE when listening to online scanners its online thus not limited to US

POCSAG: Post Office Code Standardization Advisory Group
ERMES (European Radio Messaging System)
Basic SIGINT? (I call it SIGINT cause it sounds cool but by definition these techniques are used.)

SIGnals INTelligence

Disciplines:

- **Targeting:** Pager networks need for multiple.

- **Coordinated rcvrs:** (This ideology is explored in the concepts segment of this talk). By deploying “deployable” units or “linking” up with other operations. Not all subscribers have nationwide service, therefore having multi rcvrs would broaden collections.

- **Signal detection:** Know the freq range then use the SA/Band Scope to search for poss. Signal

- **Traffic Analysis:** Again knowing capcodes is important, by doing this you begin to “map” the network, which enhances the entertainment value.

Q: The responsibility of knowledge?
A: You may see things that could be damaging but then again to share would be illegal... BE SMART with what you find.

Q: What is good, what is crap, what may be useful down the line?
A: Research, I think this is the what makes the whole hobby worth wild for me...
Pager Refresher

- The Rise and Fall

- Uses

- US pager protocols

<table>
<thead>
<tr>
<th>Rise/Fall</th>
<th>Uses</th>
<th>US Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of Cell phones and</td>
<td>Professional</td>
<td>POCSAG, FLEX</td>
</tr>
<tr>
<td>Capabilities have pushed</td>
<td>Personal</td>
<td></td>
</tr>
<tr>
<td>Use down</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This will be extremely general assuming that most of this is common knowledge. If the audience shows interest (I will ask), I'll mention the cost versus function factor. The main point is to stress that old tech doesn't mean it's bad tech.
Setting Up the “Station”

- **Antennas:**

  | RCV 25-1300MHz | TRANSMIT | RCV 108-1300MHz |

VHF and UHF signals that have high signal strength, with that said the stock antenna should work fine.

Pre amp, if one where to be used it needs to be located outside at the antenna. For pager signals it is not needed, but it wouldn’t be a bad idea if you’re trying to go after other signal types.

The antennas shown should be higher but due to the community I live in putting them higher is not an option.
NYCMIKE

Setting Up the “Station”

- Cables:

  - 1/8 not 1/4
  - RG-58/59/8
  - RS 232 DB 9

Get the right RCA

Explain the difference in coax (50 ohm/75 ohm)

DB 9 adapters will not work with PDW

I get my cables from www.allelectronics.com
Setting Up the “Station”

Decoding Software:

- **Windows**
- **Linux**
- **DOS**

Multimon decodes using sound card (Also AX.25 – packet radio BBS, DTMF)
- linux

PDW decodes using sound card (Also Flex, ACARS, MOBITEX & ERMES) –
- widows

POC32…

Radioraft…

I strictly use PDW… but that doesn’t mean you should. Sample different apps and find out what works for you.
Setting Up the “Station”

- Radios:

PC Controlled

NON PC Controlled

PC controlled allows the radio to become remote...

NON PC allows the operation to be lower cost...
Setting Up the “Station”

Radios:

Choosing the right fit.
- Cost
- Mobility
- Ease of use

Cost: How much you plan to spend is up to you, but why go overboard when you can buy a mobile within the needed freq range for so much cheaper (pro-84) or a desktop (bd 855 xlt)

Mobility: This may be a concern for me, but it is not.

Ease of use: The Plug and Play (PNP) concept doesn’t always work. In radio there are all sorts of models and not every operator is as skilled as the next.
Setting Up the “Station”

Discriminator Taps:

TK-10421 (Toko America)
Pin 11

www.discriminator.nl

This field has been well documented… Thanks to the late Bill Cheek

Either pin 9 or 11 in most cases where you need to tap off of.
Setting Up the “Station”

Discriminator Taps:

- What is it?
- Why is it needed?
- Finding the Discriminator IC?

What is it:
A physical connection from a pin off the discriminator IC/circuit (the pin varies depending on the chip), this connection allows access to the raw audio so that the rcvd signal can be decoded.

Why is it needed:
In order to decode digital mods the raw signal is needed, raw meaning before it has reached the “audio stage” this is known as “baseband audio”.

Finding the chip:
A large amount of documentation regarding current and pass scanners exist… (go into more detail)
Not very expensive to either make or buy... both slicers can be bought for Lvl2 ($16) and Lvl4 ($24) w/ power adapter, both prices may have changed. (check ebay)

What exactly the data slicer does... kinda like a modem and it decodes FSK...

Note:
Lvl 2 is also known as a hamcomm
Setting Up the “Station”

More or less don’t be a dumb ass.
Operations

- FCC ULS: Know what you are hearing.
- POCSAG (512, 1200, 2400)
  - Post Office Code Standardization Advisory Group
- FLEX (1600, 3200 lvl 2/3200, 6400 lvl 4)
- Scanning the bands using a Band Scope

Audio from http://www.kb9ukd.com/digital/

The ULS DB is grand but its only for the initial search.

Get to know the signals by ear its best when your looking for a solid signal.

The Band Scope will show you activity near the freq you are on.
Operations

Walk thru of the ULS database

Main page
Operations

Universal Licensing System

License Search

The Universal Licensing System allows you to search for a wide range of licenses in the Universal Licensing System. The license search has provided access to the most basic attributes of a license. You can also specify enhanced attributes combinations with the Advanced Search and search within services like Advanced Search using service-specific criteria. Please be aware that some combinations of search criteria may result in a longer wait.

Advanced Search

Want to search for licenses of any radio service type based on combinations of general license attributes?

Advanced License Search includes:
- General Service, Class, and Level
- State, County, and District
- License Status
- Radio Service Code

Service Specific Search

Want to search for licenses within a specific service using criteria relevant to that specific service?

Advanced:
- Station Name, Operator Class, and more.

Specialized Search

Want to use customized criteria to search for a license within a specific service?

Market Based:
- Search for station number, market, channel block, and more.

Site Based:
- Search for station class, frequency, antenna structure registration (ASR) number, and more.

Facility ID:
- Facility ID, facility identification number for
NYCMIKE

Operations

CD - Paging and Radiotelephone
CP - Part 22 VHF/UHF Paging
(excluding 931MHz)
Getting to know an interface (PCR-1000).
Once I have the freq that I will be monitoring I’ll switch the bandwidth from 15k to 50k on NFM.
If the bandwidth isn’t correct or if the signal isn’t clear enough you’ll end up with garbled data.
Operations

- Laws:
  - Communications Act of 1934
  - ECPA of 1986
The idea is gather data to get actionable information or information of interest. As with any sort of collection there needs to be a strong set of ethics laid down first. This data is in the clear but none the less it shouldn’t be abused that’s not the point or is it?
Analyze

“Get to know the Capcodes”
“Get to know the abbreviations”

Example: Looking more into this “AMKC”

After establishing a history of traffic “get to know the capcodes”

Create an archive then go through the logs and disseminate the data e.g., AMKC/GRVC, then run them through an internet resource.
BAM... we found it, now you may want to go one step further and look for an inmate support forum (Spouses, girl friends, boy friends of inmates at Rikers Island have a forum).
The conf bridges seem to be semi-trusted environments. Persons in the room have no real qualms sharing information, why would they, you need a temp login… sure why not you’re suppose to be here remember.
We are only as strong as our weakest link.
IED??? That is obviously a real concern, but the step doesn’t have to include the table top scanner… I just think it looks sexier.

PCR-1000 with serial interface to a palm pilot
Concepts

- Reprogramming inactive pagers with active Cap Codes.

Swapping out the crystals
Concepts

- Utilizing online radio sharing communities
- How does it work?
Concepts

- Decoding digital signals off of online communities like: www.gobaltuners.com

Used to be dxuners.com
Most if not all use the line out off the radio in this community, therefore without the base band I'm going no where BUT it should be do able if setup correctly ( on the pcr 1000 it has a "packet radio" jack which happens to be a discriminator tap. The site also offers different sound qualities:

- Low quality: 16kbit CBR mono 11.025kHz
- Medium quality: 32kbit CBR mono 22.050kHz
- High quality: 32-128kbit VBR mono 44.100kHz
Wrapping Up

- Garbage in will result in garbage out BUT
  if the radio on the far end is setup correctly
  the idea can and will work...
Q&A, which is different than T&A

IF TIME ALLOWS
OR
FIND ME AFTER

Thank you for looking at the slides.