Air Intercepted Messaging & Electronic Espionage – A Revisit of POCSAG and Radio Privacy Issues

By

Malf0rm3dx & Megalos

A couple of times every year I find myself wading through the boxes of electronic components, parts, wires and miscellaneous odds and ends that I've accumulated over the years. Usually this is done in an effort to make space for new gadgetry or by the demands of my wife whom threatens me with bodily harm should I do not get rid of some the electronic "giblets" that threaten to take over the house. I guess this is common tradecraft for those of us with the hacker gene and love for technology. This periodic purging seemed like all the rest, but while rummaging through the old electronics cables and connectors something caught my eye. From its façade it looked like just a regular RS 232 connector. At closer inspection I realized that I had stumbled across my old *L0pht Heavy Industries* data slicer. Oh the memories! My mind quickly ventured back to the old days when pagers were the prevailing technology for communications. I remembered all the fun and adventure that was to be had with a simple radio frequency scanner and a data slicer. As I thought about all the information that could to be obtained when using these types of devices it occurred to me how significantly society has changed from a privacy perspective. I remember these devices being able to intercept and decode sensitive and extremely personal medical information, personal messages to loved ones, alerts and warnings messages from devices that were being monitored, even detailed data captured from airplanes as they flew overhead. As I pondered all the things that were possible with these devices in the late 90s and early 2000s I wondered, could it still be possible to collect all the same sensitive information today? Were pager systems still a viable technology and something currently used by corporations and institutions? Did they broadcast personally identifiable and privacy information to the world in an unencrypted manner? My curiosity had to know the answers to these questions and I found myself dusting off my old radio scanner and collecting up the necessary cables to find out.

A word about the technology

For those of us who grew up in the years when personal pagers were considered a new consumer technology and were all the rage, the acronym POCSAG is not an unfamiliar term. POCSAG also known as Post Office Code Standardization Advisory Group was born from British telecommunications and was the forefather of numerous other paging protocols including Super POCSAG, Flex, Mobi and several other proprietary ones. POCSAG is a fairly simple Asynchronous Protocol using a Frequency Modulation (FM) known as Frequency Shift Keying (FSK) for transmitting data. Data is transmitted in 32-bit blocks using a frequency shift of +/- 4.5 kHz on the carrier frequency. The frequency shift represents a 0 or a 1 depending on the shift up or down. Originally, this enabled data to be sent at 512 bits per second. 512 bits per second is slow by any standard, but viable when sending plain text. Subsequent versions and predecessors of POCSAG provided significantly more bandwidth. Most notably among these is the FLEX

protocol. FLEX is a proprietary protocol developed by Motorola and is still used on many pager systems today. Similarly to POCSAG, FLEX uses Frequency Shift Keying (FSK) to transmit data. The FLEX pager protocol is able to achieve much higher speeds including 1600, 3200 and 6400 bits per second by using a four level modulation of the carrier frequency.

The transmit frequencies used for pager services spans the gamut of the VHF and UHF frequency bands. Pager services started in the 35 MHz range and go all the way on through the 900 MHz space. Now that pagers are not as widely used by consumers and are more utilized in certain industries and special use groups the frequencies seem to be weighted in a couple areas. 152 MHz to 158 MHz is a hotspot for many medical and hospital paging systems. 420 MHz through 540 MHz is a collage of corporate, industrial and privately owned paging systems. And 920 MHz to 940 MHz seems to be the prevailing frequency for the remainder of consumer pagers. There is no doubt that someone who takes the time and to carefully scan through all the VHF and UHF frequencies they would find additional spots where POCSAG or its predecessors are being transmitted.

A common trait amongst all the pager protocols is their inherent lack of security. As with many communication protocols, those used for paging systems were not designed with security in mind; a topic that has been detailed before amongst the pages of 2600. The two most common protocols POCSAG and FLEX broadcast data completely unencrypted and often over a significantly large geographical area. While this may be fine for simple communications of non-sensitive information it is completely unacceptable for personally identifiable information such as names, social security number, date of birth, address or the specifics of medical treatments being given to a person. The telecommunication companies rely on the fact that transmitted pager data is obfuscated using FSK modulation as a means of security. They also hide behind laws such as “Counterfeit Access Device Law 18 USC 1029” that that make it illegal to use a radio scanner to knowingly or with intent, to eavesdrop on a wire or electronic communication. And let's not forget The Electronic Communications Privacy Act, 18 USC 2510 that prohibits anyone from intercepting messages sent to display pagers both numeric and or alphanumeric. And while these laws are in place there is absolutely no technological means that is stopping a person from accidently or intentionally intercepting these transmissions and using them for personal gain. Knowing that this threat exists, it would be deplorable for companies or any organization to send sensitive information across these systems yet that is exactly what is happening!

The System Setup

Because such tasks would be illegal as defined above I’ll state what a person “could do” and the type of information they “could see” should they be so inclined to intercept POCSAG and FLEX transmissions with a radio scanner and a data slicer. This information is intended to be for educational purposes only and to provide awareness to the issues. The equipment needed for intercepting, collecting and decoding pager transmissions involves three key components. These are a radio frequency scanner, hardware or software data slicer and a software package for interpreting and storing messages.

Radio Frequency Scanner - A programmable radio is the key component to intercepting pager transmissions. The device can be any programmable radio that has the capability of monitoring the frequencies that are used for pager transmissions. Radio scanners, also known as police scanners make an excellent choice as they cover most frequencies used by pager systems and often come with line-level out or signal discriminators that make accessing the raw signal stream transmission significantly easier. With that said, any radio with an earphone or line-out jack that covers the appropriate frequencies can be used in a pinch with a little dedication and patience.

Data slicer - Data slicer's act as the decoder and interpreter of pager transmissions and come in a dizzying array of capabilities and functions. The purpose of the data slicer is to take the received radio transmission, interpret the FSK modulation and converted it to 0s and 1s so it can be converted back to plain text. Data slicers can be obtained in either hardware or software based formats. Hardware data slicers can be purchased or built for very low cost. Hardware data slicers typically come in one of two formats, either 2/level or 4/level modulation decoding. The difference between them will allow you to decode different protocols and at different speeds. A software data slicer can also be used. Software data slicers work in much the same way as hardware data slicers. Software data slicers utilize the line-in jack of a sound card to collect and decode the radio transmissions. While software data slicers have the same capabilities as hardware ones, they are often harder to configure and more prone to error and distortion than their hardware brethren. The majority of pager transmissions that are alpha numeric are typically transmitted at 9600 baud. A hardware 4/level data slicer is required to consistently decode transmissions at these speeds. Many free software data slicers exist including "*Paging Decoder for Windows (PDW)*" available at http://www.gsm-antennes.nl/PDW/pdw.php?lang=eng and "Multimon" for linux available at http://nathan.chantrell.net/old-stuff/radio/radio-scanning/pocsag-pager-decoding/ both applications allow you to use a hardware data slicer or a sound card as input devices.

Decoding Software - The decoding software receives the decoded radio transmission and converted back into text. The primary difference between the decoding software applications is the number and complexity of paging protocols that they support. The two applications mentioned above are both excellent for decoding POCSAG and FLEX transmissions as well as numerous others protocols. Both the applications are capable of decoding and interpreting pager transmissions. There are numerous other good decoding software applications that only work with the hardware data slicers including *"WinFlex"* and *"Pocflex" available at* http://homepages.ihug.co.nz/~Sbarnes/pocsag/. "*Paging Decoder for Windows (PDW)*" is by far the most current and supported pager transmissions decoding application available and it's free!

The Test

As an example setup for this experiment a Uniden BC898T programmable scanner was used along with a 2/level data slicer designed by L0pht Heavy in the early 90's. These were used with *Paging Decoder for Windows (PDW) version 3.1*. The scanner has a 1/8" line-out jack on the front side as does the RS-232 connected data slicer. Application setup is extremely simple. Simply select the hardware interface and

the type of pager protocol to decode. By default the PDW 3.1 will default to using a hardware data slicer on com1 and will decode POCSAG and FLEX at the highest speed supported by the data slicer.

Pager transmissions have a very distinctive sound and are easily found by scanning up and down the various frequency ranges. For this experiment the focus was on low speed alphanumeric transmissions in the VHF range. Low speed transmissions are easier to consistently collect for obvious reasons even with low signal to noise ratios. Medical and hospital pager systems fall into the VHF bands and appear to be concentrated in the 152mhz to 158mhz space. The 150mhz band is very close to the 2 Meter amateur radio band and is supported on a very large range of radios and scanners alike.

A word about tuning and configuration if using software and a sound card as the data slicer. Software data slicers are very temperamental and require some trial and error to get the right combination and consistent results. Start by opening the squelch completely so the signal (and noise) are received by the application. Volume should be set high or full on the radio and on the input for the sound card. This gives the application a loud and (hopefully) clear signal to interpret. Most software applications used for decoding transmissions have a signal meter of some sort, use it! You are going to need at least 60-80% to get discernable and usable data.

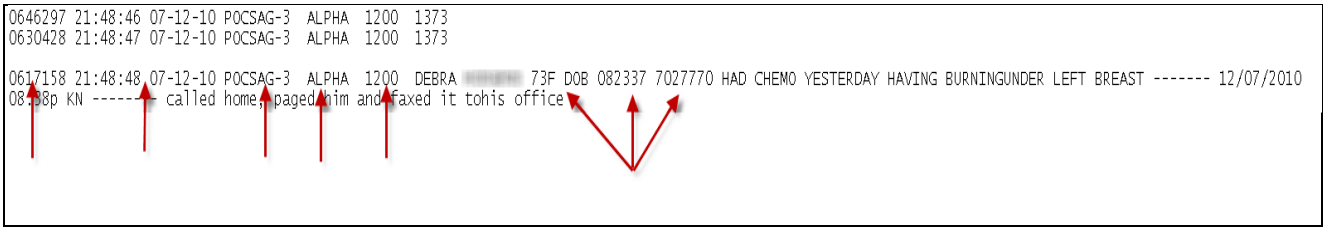
Alright, enough already with the "what" and "why" let's get to the money shot! So what type of data can be collected? With the above defined equipment and configuration, collecting entire transmissions is pretty easy. Most of the software decoding applications parse the data in a fairly clean and straight forward manner.

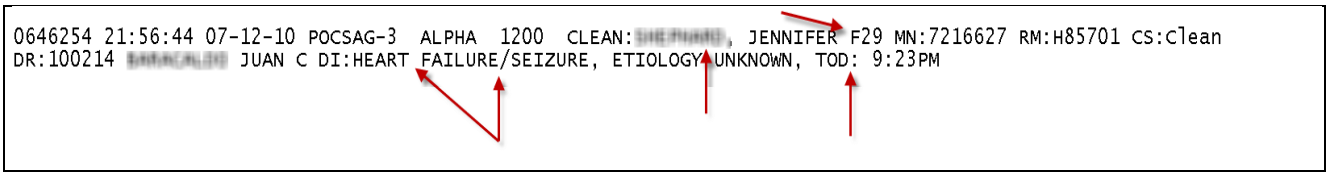
Address:	Channel Access Protocol (CAP) code. Used to uniquely identify each receiving device.
Time / Date:	Yup you guessed it time and date of the received transmission
Mode:	Protocol version used in the transmission e.g. POCSAG, FLEX, etc.
Transmission Type:	Alphanumeric, numeric or tone only
Bitrate:	Baud rate of the transmission
Data:	This is where the actual number or message is contained. Message lengths can vary depending on the receiver and the service provided.

In the below examples I have blurred out the sections of the material to protect the privacy of the individuals, ip addresses and company names. Even so, it is clear that a person can extrapolate all sorts of personal and sensitive information from the intercepted transmissions.

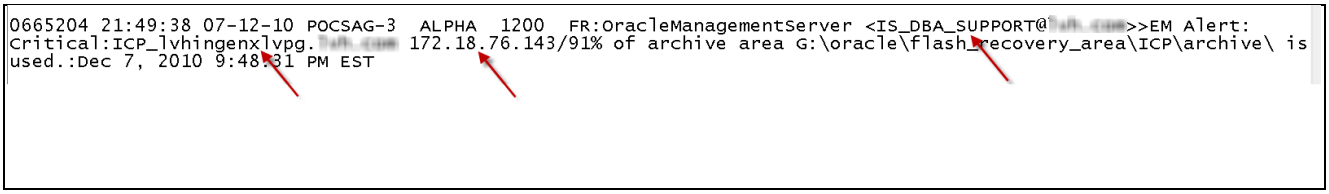
In the first two examples we see the type and details of medical information transmitted by hospitals about their patients. The first details an unfortunate lady going through Chemotheropy and having a hard time with it. Not only are we given her name date of birth and ailment, but enough detail that a

crafty social engineer could wreak all sorts of havoc at the hospital or with her personal life. In the next example we see the personal details of a young woman that suffered heart problems.

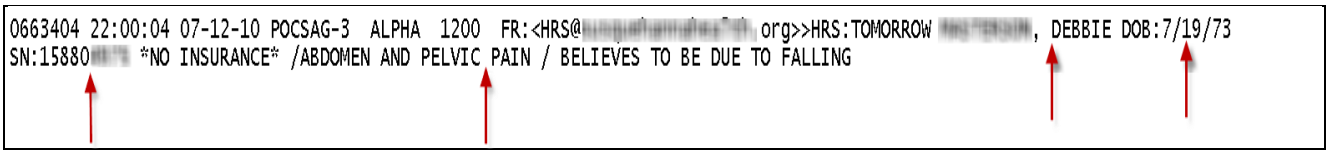


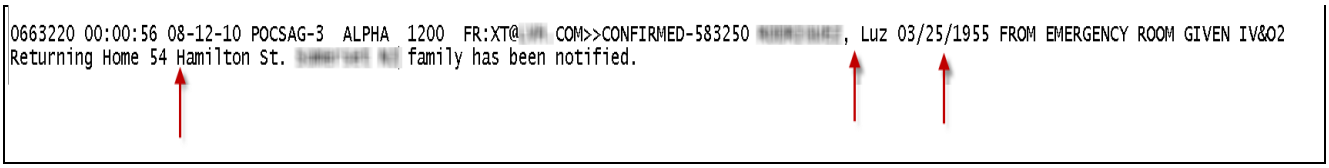


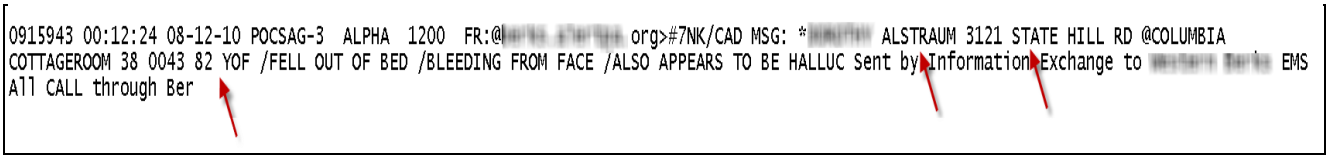
In another example we see an alert message containing an internal ip address, domain name and email address information for an Oracle server that apparently is running out of space.



In these last examples we see a collage of personal identifiable information and company information that could be used for identity theft, credit fraud or as the basis of a social engineering or system compromise attacks.







The above examples are just a taste of the type of data that is constantly being broadcasted across the airwaves with no encryption or security of any kind. While the messages are encoded by the senders for brevity purposes, it's very easy for anyone to decipher the data and fields in the messages. It should be mentioned that a person can very easily discover the frequencies being used by their local stores, companies and hospitals. This details can be found by Googling information discovered in the captured pager transmissions or by searching a particular organizations site or if you are really adventurous by looking at on the back of any of the pagers that you are interested in capturing data from.

Despite the fact that pagers have gone out of vogue as a mainstream communication tools it's very clear that niche industries are stilling using them very heavily. And since the technology not as widely used it's not getting the attention that it should.

In conclusion

I've learned several things while doing this research. First off, just because a technology is old or has been replaced by new tools and solutions doesn't mean that it isn't still viable or being used. More importantly if the technology is of significant age, its compliance to best practices and security are probably sourly lacking. Like most readers of 2600 I take privacy very seriously and I try to do all the right things to protect my identity and my credit. To think that my preventive measures can be thwarted by some jackasses sending my personal information over the airwaves for all to receive is very disturbing to me. This brings up the question of liability. Is a company or hospital liable for sending PII data over the air in an unencrypted manner? Are the telecommunication companies liable for not meeting minimal security practices on a protocol that is decades old? Regardless of these answers the bottom line is telecommunication can not hide behind laws as their justification or safeguard against transmission interception. As long as telecommunications are being sent in an unencrypted manner people will intercept them and use the information for nefarious purposes.