The POCSAG Problem - Issues From Treating Pagers As Secure Communication

Daniel Walter
TNE30009 – *Network Security and Resilience*
Swinburne University of Technology
Melbourne, Australia
102093015@student.swin.edu.au
dan@zeph.tech

***Abstract* — Where other unencrypted communication has slowly been phased out (HTTP to HTTPS, telnet to SSH, FTP to SFTP, etc.), POCSAG and the radio pagers that use POCSAG have not. This paper will discuss how and why this is an issue, and look at methods and changes that could address this.**

I. Introduction

Pagers are still being used in medical and emergency service contexts all around the globe. Doctors, nurses, and other such health professionals, along with fire and ambulance servicemen and women still either have a pager or "beeper" on their hip or in their vehicle. These pagers use a protocol called POCSAG to transmit data to one another – data such as directions for an ambulance responding to a medical emergency; a patient transfer team updating their movement status; internal hospital memos and patient details; doctor-to-doctor conversations, just to give a few examples.

In the early 80s, the ITU Radio-communication Sector (ITU-R) accepted what was then called the 'Radiopaging Code No. 1' [8] - this is what became POCSAG, and it has not changed since. POCSAG is unencrypted and has no checks against unauthorised users sending POCSAG packets or receiving packets that were not meant for them. The Emergency Services Telecommunications Authority (ESTA), define POCSAG as 'telecommunication' [1], akin to cellular phone communication, internet networking and landline telephony. The assertation that POCSAG is telecommunication is flawed.

Cellular networking employs encryption. 3G uses the KASUMI block cipher, which does have a few issues [2], but they remain academic, rather than practical, and 4G LTE uses the SNOW 3G stream cipher [3]. Domestic wireless networks utilises encryption based on the widely used and respected AES block cipher. Wired networking and communication has the benefit of the information being constrained to wherever the wire is, so landlines, internet networking, and other wired communication types are inherently more secure than wireless communication.

Wireless communication however can be picked up by anyone with an antenna, and if it is unencrypted, decoded by anyone with a computer. The ESTA defining POCSAG as 'tele-communication', and thus making it against the law to publish intercepted messages [4], is not an effective method of securing the data being sent. There is a reason why police radio and cellular connections are encrypted, even though it is illegal to intercept them. Encryption is necessary to stop people from intercepting information they should not have access to. The ESTA define POCSAG as telecommunication, which makes it fall under the Telecommunications Act 1979 [4]. However, it is my opinion, plus the opinion of several others [1], that POCSAG is radiocommunication, as opposed to tele-communication. This is due to it using wireless technology to communicate, but lacking authentication, authorisation or accounting for any POCSAG traffic. Essentially, this means that anyone can read messages from, or send messages to, anyone else, pretending to be anyone, and there is no way of knowing for certain who is who, and who sent what – similar to a handheld radio, which is undeniably radiocommunication.

II. POCSAG Technical Summary

POCSAG uses Binary Frequency Shift Keying, where +4.5kHz is a zero, and -4.5kHz is a one. To begin a message, there is always at least a 576-bit preamble – this is to indicate that there is an incoming message, while also letting the device synchronise with the incoming message. Synchronisation is important, as there are three different POCSAG modes which identify the bitrate; 512, 1200, and 2400. The synchronisation stage identifies the bitrate.

Following the preamble are the batches, which contain the data to be sent. Each batch starts with the 'Frame Synchronisation Code' (the FSC) which is a predetermined value used to further synchronise the recipient to the incoming message. The FSC is then followed by 8 'frames', each made up of 2 'codewords'. The codewords can either be an address codeword, or a message codeword. The address codewords signify the intended recipient(s), and the message codewords contain encoded 7-bit ASCII data. These batches then repeat for as many times as needed until the entire message has been sent/received.

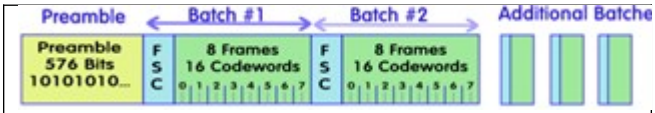

Fig. 1. Annotated breakdown of POCSAG transmission
Source: Adapted from [5]

In the following section we take a closer look at the individual codewords:

A. *Address Codeword*

For an address codeword, the first bit must be a zero. The bits 2 through to bit 19 are the address bits – this contains the address(es) of the recipient or recipients. Bits 20 and 21 are the function bits and indicate the type of message being sent. Bits 22 to 31 are BCH check bits that contain the error-correcting BCH code that can correct up to 2 errors in an entire codeword. Finally, bit 32 is an even parity bit, for very simple extra error detection. An even parity bit will be either a 1 or a 0 to make the total amount of 1's in the binary string even. See included annotated image:

Fig. 2. Annotated breakdown of address codeword.
Source: Adapted from [5]

B. *Message Codeword*

For a message codeword, the first bit must be a one. The bits 2 through to bit 21 are the message bits. In the case of an alphanumeric message, this contains the 7-bit ASCII values the sender desired to send. Bits 22 to 31 are BCH check bits, and bit 32 is the even parity bit. See included annotated image:

Fig. 3. Annotated breakdown of message codeword.
Source: Adapted from [5]

III. Why It's Still Being Used

The fact that we are still using pagers to this day tends to come as a surprise to people, but there are reasons for this.

A. *Coverage*

A major reason is that POCSAG radio messages have a huge coverage. POCSAG radio transmissions have a similar coverage to FM radio, so even if you are tens or even hundreds of kilometers (in some cases potentially a thousand kilometers) away, you can still receive crucial information without the need for an internet connection, be that via cellular or satellite.

B. *Ease of Use*

Pagers are generally rather robust devices – they are made to be able to live on the hip of an emergency services worker. The pager and the POCSAG protocol are also smart – or at least as smart as they could have made it in the 80s. They were designed to be especially energy-efficient, waking up only when it detects very specific address messages that the pager knows it needs to listen to. This smart energy and battery management allows a pager's battery to last up to 2 – 3 weeks of "typical pager activity" [9]. Compare that to a typical smartphone that needs charging every night or every second night, depending on usage.

C. *Existing Infrastructure and Methods*

More than just human-to-human messages are sent using POCSAG – it has been built into some automated infrastructure alert protocols. Using a software defined radio, I captured some POCSAG traffic in the Melbourne area for analysis for this paper. Not only are there emergency alert messages, but there are messages about servers going offline and online; the status of electrical generators; the status of building fire alarms; plant room status and conditions. Entire workflows and systems have been built around using POCSAG as a method of communication.

D. *Apparent (But Misleadingly So) Security*

The majority of people that use pagers do not know that it is a wholly insecure method of communication that should not be used to transmit sensitive PII (personally identifiable information) [6] or thought that other methods of communication could "potentially compromise patient data security" [10]. This is due to two main factors; a passive reluctance to update hardware and methodology in favor of the solution that "just works", and a miscommunication or lack thereof about how pagers function, and that they are not a secure channel for communication.

In the following section we will look at potential methods of how to address the issues brought about using POCSAG, and methods that are already being employed.

IV. Solutions

Solutions can be broadly defined as part of two different categories – making POCSAG secure, or ditching POCSAG for something else entirely.

A. *Securing POCSAG*

Encryption could be grafted onto the POCSAG protocol - there is already a precedent of integrating an encryption and/or security framework on top of an existing but unencrypted and/or unsecure protocol. For example, SFTP is just FTP over SSH, HTTPS is just HTTP over what was Secure Sockets Layer, but is now Transport Layer Security, DNSSEC is just a series of Security Extensions to DNS. It would be akin to how police radio has been encrypted to prevent snooping or spoofing.

The issue with this approach is the need to recall, upgrade, and redistribute every pager. This would take significant collaborative effort, and there would have to be a backup system to tide over the multiple different industries and services while this change takes place. The benefits to this approach are that the previously discussed benefits and reasons for pagers still being in use (coverage, ease of use, and existing infrastructure and methods) would still apply. This saves time in areas such as policy creation and retraining staff, as this process would comprise of an - albeit lengthy and difficult - drop-in replacement for pagers that ensures security of communication.

B. *Employing a Different System*

Alternatively, POCSAG, and the pagers that use it could be dropped completely and replaced with either personal smartphones using SMS, or running applications like WhatsApp, Signal, Wickr, or another such custom-made communication application built with the interest of privacy in mind. Or it could be replaced with a purpose-built modern interpretation of the pager with its own up-to-date, dedicated protocol for radiocommunication.

These two approaches bring varying pros and cons.

1) Replace With Personal Smartphone

Replacing the functionality of the pager with a personal smartphone lends itself well to swift adoption, and as there is an abundance of end-to-end encryption protocols and applications that make use of them, finding an application that sufficiently meets the needs of sensitive information communication should be relatively easy. The major downside to this solution is that both a smartphone and cellular reception is required – the total coverage will be reduced which in some small circumstances having wide-reaching coverage is crucial.

2) Replace With Modern Pager

Either in-house or out-of-house, a modern, purpose-built interpretation of the original pager could have a market. A new protocol that incorporates encryption, authorisation, authentication, and accounting can be designed and implemented. This does not have the disadvantage that the smartphone solution has of requiring an internet connection to send or receive messages, plus it retains the previously discussed benefits and reasons for pagers still being in use, *plus* there does not have to be a 'downtime' while the infrastructure is upgraded – both the old pagers and new pagers can be used at the same time as the old pagers are slowly retired. The biggest disadvantage of this option is the cost of development, production, and distribution.

V. Conclusion

POCSAG is old technology, and pagers are even older, and while they may currently still be used and useful for communication, one thing is clear – the use of the insecure POCSAG protocol is not suited to the task it is being used for and should be retired if nothing more than for the sake of patient confidentiality. It is my opinion that a combination of both the personal smartphone and the modern purpose-built pager solutions would be optimal. Metropolitan nurses and doctors, or fire servicemen and women do not necessarily need a pager anymore and could switch to a smartphone-based communication method. Yet, ambulances and rural/regional areas where wide coverage and message reliability are crucial could do from a new, modern pager.

References

[1] D. Walter, "Pocsag", Zeph.tech, 2021. [Online]. Available: https://zeph.tech/pocsag. [Accessed 05 June 2021].

[2] C. Blanchard, "Security for the Third Generation (3G) Mobile System", Network Systems & Security Technologies, p. 9, 2003. [Accessed 5 June 2021].

[3] M. Bartock, J. Cichonski and J. Franklin, LTE Security – How Good Is It?. National Institute of Standards and Technology, 2015.

[4] Telecommunications (Interception and Access) Act 1979. Australian Parliament, 1979.

[5] A. Hickerson, THE POCSAG PAGING PROTOCOL. Raveon Technologies Corp.

[6] E. Wicklund, "That Pager Isn't as Secure As You Might Think", mhealthintelligence.com/, 2016. [Online]. Available: https://mhealthintelligence.com/news/for-mhealth-messaging-that-pager-isnt-as-secure-as-you-might-think. [Accessed: 06- Jun- 2021].

[7] M. Prochaska, A. Bird, A. Chadaga and V. Arora, "Resident Use of Text Messaging for Patient Care: Ease of Use or Breach of Privacy?", JMIR Medical Informatics, vol. 3, no. 4, p. e37, 2015. Available: https://medinform.jmir.org/2015/4/e37/. [Accessed 6 June 2021].

[8] RECOMMENDATION ITU-R M.584-2, CODES AND FORMATS FOR RADIO PAGING. ITU Radiocommunication Sector, 1982.

[9] P. Wattingen, "How long do batteries last in the pagers and nurse call devices?", PalCare, 2020. [Online]. Available: https://www.palcare.com/avada_faq/long-batteries-last-pagers-nurse-call-devices/. [Accessed: 09- Jun- 2021].

[10] M. Baqai, U. Hani, N. Shahzad and R. Alvi, "Beep or alert: evaluating WhatsApp vs pagers for communication between hospital staff", British Journal of Healthcare Management, vol. 27, no. 1, pp. 32-38, 2021. Available: https://www.researchgate.net/profile/Ummey-Hani/publication/348277959_Beep_or_alert_evaluating_WhatsApp_vs_pagers_for_communication_between_hospital_staff/links/5ff7ec9845851553a02b03f4/Beep-or-alert-evaluating-WhatsApp-vs-pagers-for-communication-between-hospital-staff.pdf. [Accessed 9 June 2021].