Gordon Gibby MD KX4Z
Gainesville, FL

July 15, 2019

RE: RM-11831

- Repeated demonstrations of capture of WINLINK messages, proof-of-concept **without software changes**
- Witnesses to final demonstration
- Proves there is no "effective encryption" nor any "encryption"

Sirs:

This comment is an update to a previously made disclosure of an experiment that proved that it is **quite** possible to read WINLINK communications over the air [1], as well as responses to comments from multiple individuals who claimed WINLINK uses encryption.

In total, five WINLINK transmissions have now been intercepted—without even writing a line of code-- to further the proof-of-concept that monitoring WINLINK is not miraculous at all – it just takes suitable engineering expertise. I have now published a book outlining how we did it, as proof-of-concept, or how it could be built, by those so disposed, as a real, working, monitoring system.

It is very likely that much of this discussion is happening because some individuals are not satisfied by having a web-based viewer, which allows all USA-amateur related WINLINK communications which go through the Central Message Server to be viewed immediately after transmission. [2] That viewer even allows for potential misdeeds to be noted and a review and correction process to be initiated – but for some, **even this was not acceptable** and they continued to demand some method to review emails over the air. This work explains how they could do that.

Some of these individuals have continued to claim that the WINLINK system employs some form of encryption, or that ARQ technology (quite common, and legal for many years under FCC regulations) is not usefully employed. These concerns would impact the NTS-Digital service as well (which employs very similar systems, particularly with PACTOR).

[1] Previous submission: https://ecfsapi.fcc.gov/file/10410170249078/FCCRM11831-4.pdf

[2] https://winlink.org/content/us_amateur_radio_message_viewer

To address that demand, one must remember two very clear facts:

1. For years, amateur radio operators have called CQ – and answered – and held contacts with PACTOR modems. While the popularity of this mode has declined, **monitoring frequencies for PACTOR stations and reading their transmissions has obviously been accomplished** for many, many years.
2. WINLINK employs NO ENCRYPTION, and publicly available, literally decades-old data compression and decompression algorithms.

I now report that our group in Gainesville FL has completed additional tests to repeatedly demonstrate that there is no fundamental reason why WINLINK cannot be monitored on the air (by those so motivated), and I personally wonder why it hasn't already been accomplished by those who are so concerned.

A booklet describing why it is only an engineering project to read WINLINK email right off the radio waves has now been written based on this work, and it is now published on AMAZON and also as a KINDLE work, so that all interested persons can learn how.

FREE COPY YOU CAN READ FOR NON-COMMERCIAL USAGE:
https://www.qsl.net/nf4rc/2019/SpyingOnWINLINKV2.pdf

AMAZON PAPERBACK: https://www.amazon.com/dp/1080563199

KINDLE: https://www.amazon.com/Spying-WINLINK-Gordon-Gibby-ebook/dp/B07V664FYK

In that text, I explain how WINLINK systems utilize decades-old and pubic domain LZHUF compression systems,[3] in order to maximally reduce the transmission time required, and thus the usage of radio spectrum. Phil Karn has discussed the fundamental fact that anything done to maximize the efficiency of radio communications makes it more (not less) difficult for an eavesdropper to monitor, and he is certainly correct.

> *Virtually anything one might do to facilitate communications and/or use the radio spectrum more efficiently will have the side effect, intended or not, of making that communication more difficult for some third parties to monitor.* [4]

Just as compressing a hard drive on a computer with an Limpel-Ziv -based compression algorithm dramatically increases the space available and even potentially the speed, it makes it more difficult to read the data on that hard drive.

In the published text, I discuss at some length the history of data compression – and I'm certainly not an expert! – pointing out the advantage to the volunteer developers of WINLINK to use publicly available and liability-free versions of compression that were readily available in the years they were beginning to develop their systems.

In the published text, I provide references to the available coding for LZHUF compression systems which could have easily been utilized by those so intent on having on-the-air capture of WINLINK emails. These include:

[3] https://ethw.org/History_of_Lossless_Data_Compression_Algorithms

[4] https://ecfsapi.fcc.gov/file/10422455216228/rm11831.pdf

The actual routine utilized in the WINLINK system	https://github.com/ARSFI/Winlink-Compression
Source code for another implementation	https://www.pcorner.com/list/C/LH_UNIX.ZIP/LZHUF.C/
The entire source code for John Wiseman's WINLINK-compatible bpq development, which can even operate on a $35 Raspberry pi	https://github.com/g8bpq/LinBPQ
The specific subset of John Wiseman's publicly available code that deals with compression and decompression	https://github.com/g8bpq/LinBPQ/blob/master/lzhuf32.c

In order to gain the highest efficiency, entire messages are compressed in the WINLINK system, from end to end. I'm not an expert on compression, but I suspect the same is true when I zip any set of files to send over wired networks. Thus the entire packet stream must be faithfully captured in order to decompress the text, a fact which we encountered multiple times in our ultimately-successful demonstrations of the fundamental ability to spy on WINLINK messages.

Diversity Receiving

For an on-the-air large-scale all-encompassing spying/monitoring effort against WINLINK, perhaps with the goal of capturing all transmissions from all Gateways within the 97.221(b) narrow slivers, it likely makes the most sense to employ diversity receiver systems so as to have multiple sets of packets from which to pick and choose in order to re-create (in near-real-time) a perfect data stream. The acknowledged ability of the PACTOR modems to provide a "listening mode" makes this a lot simpler. You clearly do not have to know the callsigns of other stations, prior to reading their messages, or it would be impossible to even see a random CQ from a PACTOR user!

As I discuss in the published book, *diversity receiving systems have been used for almost a century.* I was able to find photos of AN-FRR-3A (**vacuum tube-based**) United States Navy diversity receiving systems with a manual dated 1944! [5]

In 1944, the United States Navy did not have the advantage of a widespread Internet, which would allow volunteer stations to instantly connect, providing readily-available packet streams for a central system to compile. However, one barely even needs to develop a group of volunteers because now there are freely available web-based SDR receivers which can be easily utilized to build the diversity receiving network. [6]

Acknowledgment / Request for Repeat

Since the beginning of amateur radio, whether by CW, or phone, or digital, amateur radio operators have used acknowledgments of reception ("QSL") and requests for "fills" – and this is an extremely well-recognized tool for accurate communications. Incorrect statements about commercial usage of Forward Error Correction without ARQ, or assertions that Forward Error Correction alone would suffice for accurate transmissions were effectively answered by Mr. Karn.[7]

> *This is simply incorrect. The commercial wireless industry uses both FEC and ARQ in combination.*

[5] http://www.tmchistory.org/PressWireless/manuals/prewi_frr-3a_manual.pdf

[6] For an example of a group with 160 web SDRs, see http://websdr.org/

[7] Imagine trying that assertion during a Contest – give your exchange twice [a rudimentary FEC] , and refuse to even listen whether the other station received it?

> *This is true for both commercial wireless services and for 802.11 (WiFi) wireless LANs. In addition, every Internet user also uses the ARQ built into the Transmission Control Protocol (TCP).*[8]

And

> *Rappaport claims: "The ARSFI/Winlink methods that rely on ARQ and compression are most likely less spectrally efficient than if they used FEC (e.g. Viterbi decoding)." This reveals a profound ignorance of how this system actually works. Once again, both ARQ and FEC are used.*[9]

It is important that the Federal Communications Commission relies on **accurate** information.

Astonished at these claims that FEC alone could provide safe and accurate communication of non-trivial messages – when errors may be humanly costly – prompted me to initiate a discussion on a popular amateur radio Internet forum. Not a single person was willing to assert that forward error correction alone would suffice.[10] Apparently most recognize from practical experience the truth of what Mr. Karn explains and the other expert stands alone in his views.

<u>Creating A Monitoring System</u>

In our case, we lack the ability and time to modify the existing public-domain software to do on-air full time WINLINK spying, merely to duplicate what is already available on the WINLINK web viewing page. Some of the persons demanding such a system, however, by their own credentials, have both the ability and the resources to accomplish precisely those goals.

<u>Our Proof That It Is Possible</u>

Nevertheless, I set about to demonstrate that it was indeed possible – that there is NOTHING encrypted (or even "effectively encrypted") within the WINLINK system. This was patently obvious to those skilled in the art[11], and many such statements were made in a public web-based forum where this was discussed at great length, yet I wished to demonstrate that fact.

It only requires ONE correct capture of a WINLINK message in order to disprove the assertion that it is impossible to do on the air monitoring – or even that it is "effectively" impossible.

As is described in the published text, it has now been done at least **five** times.

<u>Proof Without Even Writing A Line Of Code</u>

In order to accomplish this *without even writing one single line of software*, I had to exploit the freely available WINLINK software itself. Indeed, this software obviously correctly handles roughly 50,000

[8] https://ecfsapi.fcc.gov/file/10513525129724/rm11831-rebuttal-to-rappaport.pdf

[9] https://ecfsapi.fcc.gov/file/10513525129724/rm11831-rebuttal-to-rappaport.pdf

[10] https://forums.qrz.com/index.php?threads/forward-error-correction.665519/

[11] Karn objects to the improper characterization of WINLINK as "effective encryption" and points out the solutions demanded by the opponents could be created by suitable hardware and software developments. https://ecfsapi.fcc.gov/file/10513525129724/rm11831-rebuttal-to-rappaport.pdf

messages per month, so it is obviously quite capable. The only question was whether it could be tricked into doing my bidding.

In order to get the software itself to demonstrate the fallacy of the claim that it is impossible to monitor WINLINK, I had to get a snooper station, employing the public WINLINK software, to stealth-monitor an ongoing WINLINK message transfer, as if the stealth station were really the station receiving the message – and yet I had to have the stealth station never make any transmission whatsoever, and have all acknowledgments and replies carried out by the intended recipient station.

To do that requires that the stealth station stay in perfect lockstep with the intended recipient throughout the message transfer – *a requirement that would not apply at all to an engineered monitoring effort where the designer would simply utilize the PACTOR monitoring mode and sit back and watch the packets flow.* This is precisely what any PACTOR user does when they scan the band for stations calling CQ, not having any advance knowledge at all of the other station's call sign – in preparation for answering them.

PACTOR appears actually to be a useful candidate for such a snoop-without-even-writing-code effort as I proposed, since it sends out equal-length packets one right after the other. My problem was the dramatic disparity in age (and likely calibration) of my modest collection of equipment.

So, as described in a previous FCC filing, I set up

Station #1 – the peer-to-peer initiator
Station #2 – the peer-to-peer intended recipient
Station #3 – the Snooper Station, not allowed to transmit and needing to stay in perfect lock step with the second station.

Three PACTOR stations set up in a hallway. The ICOM-725 (farthest in the picture) had to be replaced with another ICOM 718 for the last test due to frequency inaccuracies.

Peer to peer mode was much easier for me to use for this **no-code-even-written proof of concept demo**, because then I only have to perform one initiation of Station #1 – and Stations 2 and 3 will hear the signal of Station #1 and at least at the beginning, be in lock-step.

Note that peer-to-peer mode utilizes *precisely the same compression and decompression systems* utilized in the client-server mode.

Remaining in lock-step requires some luck, as I explain in the published text, because Station #3 thinks it is transmitting, so it goes back and forth between receive and transmit mode, over and over and over, and always having the chance of differing in timing from Station #2 – nevertheless, we have now seen five successes. An engineered solution would simply monitor and assemble the packet stream.

Success #1 was reported in a previous filing to the FCC. [12]

Successes #2, #3, and #4 were accomplished on Friday, July 13th, one right after another – and then something changed and I was not able to keep the Snooper Station locked in.

For the final attempt, two additional amateur radio operators, both Extra Class, Leland Gallup AA3YB and Jeff Capehart W4UFL joined me. As described in the book, we spent almost an hour setting up the equipment and going through how this demonstration would serve simply to disprove the assertion that there was ANY form of encryption (real or effective) at work in the WINLINK system.

As the day before, we were initially unable to get Snooper Station to even connect when allowed to transmit. There was a problem with the older transceiver which appeared to have a receive/transmit offset. We switched to a used Icom 718 and had far better frequency alignments.

Nevertheless, Station #2's modem and Station #3's modem were a couple decades apart in age and we had difficulties getting them to stay perfectly synchronized for the time needed for the connection (something that should be completely unnecessary for a station with engineered software simply capturing packets). The majority of the time the stations would be in sync for the beginning of the connection, but then something would go off, and Station #3 (Snooper Station) would indicate a "repeat" of some sort on its screen – and the lock was lost. However, it finally happened that they stayed in lock for the entire transmission and **we obtained my 5th perfectly received WINLINK message** – received not only on the intended recipient Station #2, but also on the non-transmitting Station #3 – not even using modified software, just using off-the-shelf WINLINK freely available software. Not a single line of code written.

After that success, we made two short videos, sent the shorter out by email to friends as documentation, and I proceeded to finish the published text describing how to spy on WINLINK over the air.

Clearly there is no encryption—not even "effective" encryption-- when you can snoop without even writing code, and any statements to the contrary should be ignored. A designer can obviously simply capture the packets, run them through the freely available decompression software, and have a working WINLINK SNOOPER I have now demonstrated five times where it was done even without writing a single line of code.

- No "proprietary techniques" are needed to read WINLINK transmissions as alluded by Robert W. Rennard, Ph.D.[13]

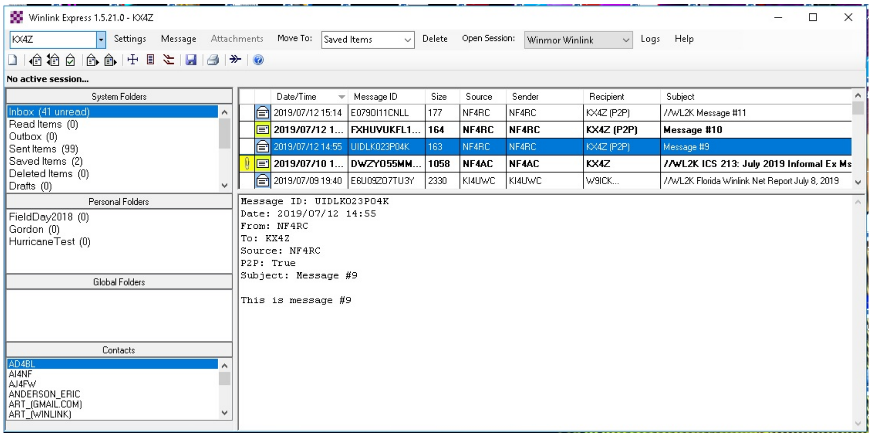
[12] https://ecfsapi.fcc.gov/file/10410170249078/FCCRM11831-4.pdf

[13] https://ecfsapi.fcc.gov/file/10618019918014/N7WY%20comments%20regarding%20RM-11831.pdf

- There is simply NO undecodable data transmission / communication as alleged by Joe Fitter.[14]
- There is NO proprietary encryption as alleged by Jose Castillo.[15]
- It is not "effectively encrypted" as fallaciously claimed by T. Rappaport Ph.D.[16]
- It is not encrypted as alluded by Robert Steenburgh.[17] and claimed by Allen Brown.[18] and insinuated by David Schmocker.[19], claimed by Mark Hoffman[20]
- Robert Putala[21] took the same "effectively encrypted" error proposed by T. Rapport, while David Phillips alludes to WINLINK using encryption.[22] as does Mark Tattenbaum.[23]
- John Long asserted WINLINK encrypts and cannot be read by anyone other than the intended recipient (which we manifestly disproved five times). [24]
- Donald Schliesser comes right out with an accusation: "Automatically Controlled Data Stations (ACDS) have been operating illegally, by using proprietary encryption which can not be monitored by anyone, including the FCC …." which is now demonstrated as patently false for the case of WINLINK and NTS-D.[25]

One has to wonder – how did all these 13 persons become so confused and mistaken?

If WINLINK were encrypted...we would not have been able to intercept a single transmission.



Date/Time	Message ID	Size	Source	Sender	Recipient	Subject
2019/07/12 15:14	E079OI11CNLL	177	NF4RC	NF4RC	KX4Z (P2P)	//WL2K Message #11
2019/07/12 1...	**FXHUVUKFL1...**	**164**	**NF4RC**	**NF4RC**	**KX4Z (P2P)**	**Message #10**
2019/07/12 14:55	UIDLK023P04K	163	NF4RC	NF4RC	KX4Z (P2P)	Message #9
2019/07/10 1...	**DWZYO55MM...**	**1058**	**NF4AC**	**NF4AC**	**KX4Z**	**//WL2K ICS 213: July 2019 Informal Ex Ms**
2019/07/09 19:40	E6U09Z07TU3Y	2330	KI4UWC	KI4UWC	W9ICK...	//WL2K Florida Winlink Net Report July 8, 2019

```
Message ID: UIDLK023P04K
Date: 2019/07/12 14:55
From: NF4RC
To: KX4Z
Source: NF4RC
P2P: True
Subject: Message #9

This is message #9
```

Screen Capture from Snooper Station Computer, showing Message #9, one of three successfully snooped

[14] https://ecfsapi.fcc.gov/file/10606109321772/RM_FCC_2019.docx

[15] https://www.fcc.gov/ecfs/filing/106060716526365

[16] https://ecfsapi.fcc.gov/file/10429199250117/FCC%20Letter%20Reply%20to%20Comments%20RM%2011831.pdf

[17] https://www.fcc.gov/ecfs/filing/1042758374569

[18] https://www.fcc.gov/ecfs/filing/104261468401350

[19] https://ecfsapi.fcc.gov/file/1042235942086/This%20comment%20supports%20RM.pdf

[20] https://www.fcc.gov/ecfs/filing/10420094129357

[21] https://ecfsapi.fcc.gov/file/104180962221970/RM-11831.pdf

[22] https://www.fcc.gov/ecfs/filing/10416944920333

[23] https://www.fcc.gov/ecfs/filing/10414956923602

[24] https://www.fcc.gov/ecfs/filing/1041056168575

[25] https://www.fcc.gov/ecfs/filing/1033179521395

on July 12 2019.

Leland Gallup AA3YB (foreground, retired Army Judge) and Jeff Capehart W4UFL (Alachua County Emergency Coordinator and Asst. Section Manager), witnesses to the final success!

I hope now that everyone will recognize *and admit* that there is **no encryption of any sort in WINLINK**, just good engineering to make efficient usage of radio spectrum, and therefore it is imminently possible – an engineering project, now – to have on-the-air monitoring of WINLINK exchanges. This could be a project for a graduate student. **If there is a group requesting free software to do so, it would appear they have the necessary resources and education to carry out the development of such systems, all by themselves should they still feel it necessary.**

Respectfully submitted,

Gordon L Gibby MD KX4Z