
P25 Security Threats Reported by Researchers:

Fact or Fiction – An EFJohnson Perspective

Author: John Oblak

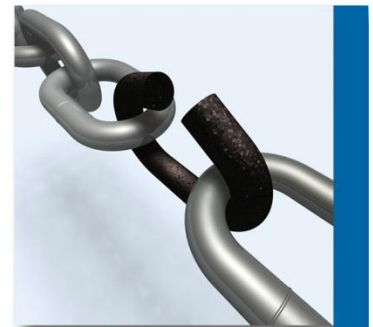
*EFJohnson Technologies Vice President of Standards and Regulatory Affairs
Chair TIA TR-8 Committee on Mobile and Personal Private Radio Standards*

August 16, 2011

There has been much concern expressed recently over news articles that expose the vulnerabilities of Project 25 systems and equipment. The original study of the issue comes from work done at the University of Pennsylvania. The work was sponsored, in part, by a grant by the National Science Foundation. The original 17-page report is entitled “Security Weaknesses in the APCO Project 25 Two-Way Radio System,” and was published in December 2010. It has more recently been sensationalized in various news reports. The following paper is intended to clarify some of the issues associated with Project 25 security.

Several weaknesses were cited by the report. One specific weakness that was identified is related to the possibility of user error in encrypted communications. The argument was made that P25 radios are fairly complicated, and with multiple programming options, programmable user keys, soft keys, and menu operation, the operation of a radio is confusing at best. For their example they used a Motorola XTS-5000. However, they state that any of the available radios would have similar issues. Since P25 allows communications to take place either encrypted or in the clear, there is a possibility of a user making a mistake and transmitting sensitive information in the clear that is intended to be encrypted. They cited several examples of communications that were intercepted over the air that obviously should have been encrypted, but were transmitted in the clear. They blame user confusion with the mistakes. While there may be merit to this argument, there are several best practices that could be deployed to mitigate this concern, as well as opportunities in user interface to mitigate the problem. It is interesting to note that there is nothing inherent in Project 25 that makes this problem any worse than in any other communication system (including analog).

A second area of concern that was stated in the report is of selective jamming. In any narrowband communication system jamming can occur whenever a jamming signal is introduced at a level above the desired signal level. A phenomena known as “capture effect” will cause the stronger signal to overcome the weaker signal, thus effectively jamming the transmission of desired information. The contention of the report is that since Project 25 signaling has in its bit stream localized important signaling bits (such as NAC codes), jamming of only small portions of the bit stream will render the communication inoperative. It is important to note that the jamming signal must still be of a sufficient power to overcome the desired signal. However, since these important bits can be localized in time, the jammer need not be active for long duty cycles. This means that while the instantaneous power during jamming bursts must be of sufficient power to overcome the desired signal, the average power (or energy consumption) of the jammer need not be large. Thus, the jammers can be rather small, and will have lower power supply requirements. The latest news articles reported on the use of a (highly) modified cellular text communicator in the form of a “child’s toy” used as a jammer. However, no specific performance was reported.



There is nothing inherent in Project 25 that makes intercepted communications a bigger problem than in any other communication system (including analog).

All narrowband systems are subject to jamming including analog as well as digital systems. It is important to note also that all narrowband digital systems will have the above characteristic to some degree. The issue really centers not on the resistance to jamming, but the average power consumption of the jammer.

Other issues that were brought up in the report deal with the fact that important link control fields are always sent in the clear mode. This can be used by adversaries to discern radio information, such as radio unit ID. This, in turn leaves a vulnerability to detect the presence and location of radio units. In addition, this can lead to spoofing, where an enemy unit can fool the system into thinking it is a legitimate user. Early on in the Project 25 standards process security vulnerabilities were evaluated. As a result, there has been a plan to address some of these concerns with radio unit authentication and link layer encryption. Both of these are being addressed for future inclusion in the standards.

Given the above stated concerns, the question is, why do these issues exist? It must be remembered that the requirements for P25 was for a radio system to fit into the FCC channel plan of 12.5 kHz of spectrum, with a future requirement for 6.26 kHz. Systems of the form of P25 are a result of this requirement. The report states that the signaling appears to be "ad hoc." This is also a consequence of the required spectral efficiency. It's also instructive to realize that the University of Pennsylvania report would have been substantially the same if the text P25 was substituted with TETRA, DMR, etc. In effect, any type of narrowband digital technology would have similar characteristics. In other words, the report hinted at an expectation of robustness similar to that offered by a spread spectrum type of system. Of course, this would not have met the requirements of existing and narrowband frequency plans.

It is also interesting to note that in all of the analysis, there is no concern shown by the report for the breaking of the AES encryption. While the "child's toy" demonstration may have been misinterpreted as a breaking of the encryption, the report actually affirms that the encryption itself has not been broken, and that no encrypted information is vulnerable.

John Oblak
joblak@efjohnson.com