Project 25 Radio Authentication

Jim Holthaus, Vice President, Chief Technical Officer, BK Technologies

Project 25 radio standards now provide a method of authenticating subscriber radios for operation on P25 trunked radio systems. This paper explores the need for and functionality of P25 Link Layer Authentication services on trunked radio systems.

Public safety agencies operating radio communications systems often have an investment ranging from a few hundred thousand dollars to as much as $100 million or more. Often these wide area communication systems can become a tempting target for those that might wish to steal service or in worse cases intend to disrupt or confuse mission critical communications. Most public safety systems can be monitored using commercially available radio scanners, provided the radio traffic is unencrypted. Of course scanners only allow monitoring and cannot be used as a source to steal service and/or disrupt legitimate communications. Of growing concern is the ability to purchase public safety grade communications equipment over the internet. Access to such equipment can provide unauthorized individuals the same access to the radio system as legitimate users.

For decades, public safety communications system operators were protected from unauthorized access through the restrictions that equipment manufacturers placed on radio programming equipment. So even if an unauthorized individual had radio equipment and programming software, without the so called 'system key', programming a radio for an individual radio system was not possible. In general, this level of protection works quite well for many public safety agencies. However, the use of the system key is only as reliable as the methods used to protect unauthorized access to such a key. In practice, this key can take the format of a software file, or can be a hardware based key. Software keys are somewhat more difficult to secure as they can be copied or transferred to unauthorized individuals with relative ease. Hardware key devices provide an increased level of security as they can be copy protected and configured with other security provisions like expiration dates, cycle limits and restricted rights. Additionally, public safety internet forums discuss the existence of software programs designed to replicate some manufacturer's system key files.

In addition to restricting the ability to program subscriber radios via a system key, the radio system itself may prevent access using a registration authorization database that may identify valid or invalid unit IDs. Even so, individuals with access to pirated programming software or system keys could monitor control channel traffic to determine a valid radio ID and program a radio with a duplicate but valid ID.

As the technological abilities of those wishing to steal service or disrupt public safety communications systems expand, additional measures to protect unauthorized access to public safety communications systems are required.

Public safety system operators and radios users have been aware of the vulnerabilities that can be caused by unauthorized radios or radios with duplicate IDs on the system. Despite programming and system level safeguards, illegitimate users present a clear hazard to public safety communications. As such, radio users, through the Project 25 Standards process have requested inclusion of additional measures to prohibit unauthorized access to these systems. The Project 25 standard provides this protection through the use of authentication technology. The Project 25 standard defines a challenge response system that allows the radio system and/or subscriber radio to authenticate itself before service is granted.

In a P25 radio system, authentication services are handled by an authentication facility. Depending upon the system manufacturer, the authentication facility could be a standalone server, or an application service running on an existing system device. Figure 1 shows a P25 radio system with an authentication facility. Authentication uses a secret key which is stored in the radio system and subscriber radio. Each subscriber radio has its own unique authentication key, which is associated with the subscriber radio's unit ID. For subscriber radios that are operating with multiple systems or multiple unit IDs, multiple authentication keys are assigned.

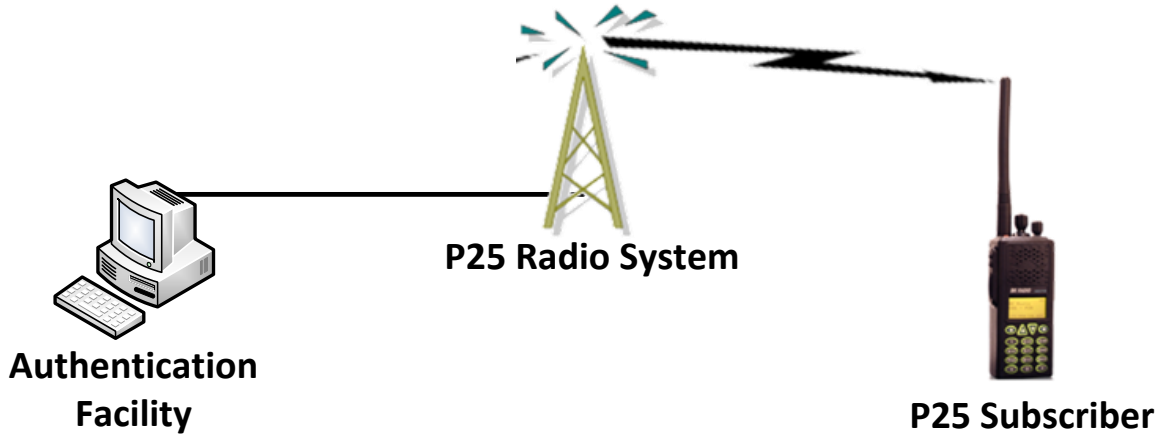

Figure 1 P25 Radio Authentication System

The P25 radio system initiates the authentication process once the subscriber radio registers with the system. This is done by sending an authentication challenge to the subscriber radio. The subscriber radio returns a response to this challenge which requires knowledge of a unique authentication key. The radio system then compares the subscriber radio's response, and if correct the authentication is successful and the subscriber radio is considered valid. If authentication fails, then the subscriber radio is denied access to the radio system. Of course, the system will not interfere with an authenticated subscriber in the event that an invalid radio attempts to authenticate using the same radio ID. While authentication generally occurs at initial registration with the system, the P25 standard allows for authentication commands to be sent to subscriber radios at any time.

If a radio with an authentication key is lost or stolen, the authentication key can be disabled in the authentication facility preventing the unaccounted for radio from gaining access to the system.

The P25 authentication standard also provides support for mutual authentication. If this option is supported, not only can the system authenticate a subscriber radio, but the subscriber radio can authenticate the radio system. Mutual authentication provides protection against adversaries that attempt to disrupt service to subscriber radios by imitating a valid radio system. At present, not all P25 infrastructure providers are offering radio authentication support for mutual authentication.

Authentication services in P25 systems utilize the Advanced Encryption Standard (AES) with a key size of 128 bits. This provides a high level of cryptographic security with over $3.4x10^{38}$ possible authentication key combinations. AES-128 is also approved for use in FIPS-140-2 validated cryptographic modules. Appropriate P25 standards have been updated to ensure the P25 ecosystem supports radio authentication. For example, the P25 Key Fill Device Interface has been updated to support loading of 128 bit AES keys for radio authentication into both subscriber radios and authentication centers.

P25 subscriber and infrastructure manufacturers are currently shipping products with P25 link layer authentication and public safety agencies have successfully deployed link layer authentication on fielded P25 radio systems. P25 link layer authentication is just one of many strategies available to protect P25 mission critical communications systems from unauthorized access.