WillowFalls
Consulting Limited

Is P25 Secure?

There are several reports on the Internet indicating P25 encryption and system security are flawed, putting users at risk. While there are things to learn and improve based on these reports, the situation is not as bad as it sounds.

The three key things to know are;

1. None of the reports are about actually breaking AES 256 Bit encryption.
2. Good Standard Operating Procedures (SOP) can mitigate most of the risk.
3. Changes can be made to the P25 specification to improve security.

Three Reports Found On The Internet;

1. **From a group of researchers at the University of Pennsylvania;**
   Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System

   P25 Security Mitigation Guide

2. **From NICTA researchers in Australia;**
   Insecurity in Public-Safety Communications: APCO Project 25

   NICTA (National ICT Australia Ltd) is Australia's Information and Communications Technology Research Centre of Excellence.

3. **The Daily Telegraph, Australia;**
   Hi-tech hackers crack NSW police force $22 million encrypted radio system

   There is not a lot of information available about this story, other than the original story and multiple sites on the Internet with links or copies of that story. While the headline says "Hi-tech hackers crack NSW police force $22 million encrypted radio system", it appears the Police were not changing their encryption keys and were not auditing their procedures, so someone was either selling encrypted police radios, or selling encryption keys.

   Changing keys regularly, with routine auditing of key management process compliance would probably have kept this from happening, or would have made it nearly impossible to maintain the security breach.

Lessons Learned

1. Good Standard Operating Procedures (SOP), with routine audits, training and practice are critical to keep encrypted communications secure.
2. Threat Risk Assessments (TRA) are an important tool for understanding the risks and impacts, which is important for building and getting support for a good Security and encryption plan.
3. Audits are an important part of an Encryption Management Plan, to identify any leaks as soon as possible. They are also important to identify radios that are missing, but have not been reported.
4. Changing encryption keys regularly is important, to ensure that if an outsider does get access to monitor the system, it will not continue for long.

Responses To P25 Security Questions

- Public Safety Communications Research (PSCR)
- EF Johnson: P25 Security Threats Reported By Researchers