Abstract for presentation at SWITS 2024

Security Aspects of TETRA Networks in Sweden: Preliminary results from a case study

Marcus Dansarie[1,2] & Marcus Nohlberg[2]
[1] Swedish Defence University, Department of Systems Science for Defence and Security
[2] University of Skövde, Department of Informatics

Wireless communication systems are used in many fields throughout society, including in critical infrastructures. Previous research on the security of radio communication standards has uncovered issues such as lack of encryption and authentication, broken encryption and security protocols, and implementation issues. Despite this, little research has focused on the impact of security issues to users and those who are otherwise dependent on radio-based systems. The only known exception to this is civil aviation communication, where previous research has found that there exists a gap between users' perception of security in the systems and their actual security. Additionally, it has been shown that many security issues in aviation systems are mitigated by routines and procedures, reducing their impact. To investigate the state of wireless communication security in other fields, a study on the use of the TETRA communication standard in Sweden and the security needs of its users was performed. This presentation describes preliminary results from that study. Semi-structured interviews were conducted with system owners in eleven of the around 40 different organizations that own TETRA networks in Sweden. The interviewees represent a cross-section of users: large and small, public and private. As such, it is the first study into the use of TETRA networks and their users' security requirements. A number of themes are highlighted, including a generally high requirement for availability among TETRA user organizations, the perception that digital communication systems are more secure than analog systems, and the commonality of security-by-obscurity arguments.