УДК 004.9
K. Brima, I. Opurum, R. Zolotyi
(Ternopil Ivan Puluj National Technical University)

RESEARCH OF WIFI SYSTEMS PROTECTION EFFICIENCY

Wireless networks are becoming ubiquitous and can be found in domestic, commercial, industrial, military, and health care applications. One application of particular interest is that of emergency communications where an Incident Area Network (IAN) can be rapidly deployed at an incident site. Wireless networks are well suited to such applications because they can be rapidly established and facilitate the exchange of voice, video and multimedia content such as detailed maps, building plans and photographs. The experience of Hurricane Katrina, the Asian Tsunami and Black Saturday demonstrates the importance of effective communications in saving lives following a catastrophic event.

The security of an emergency communications network is extremely important because a breach of confidentiality, integrity or availability may result in the loss of human life. Ensuring security presents a thorny problem because communication in a wireless network uses a shared medium without the benefit of a physical security perimeter. To address this problem wireless security protocols use cryptographic techniques to protect the network but the results have not always been successful. Serious flaws have been discovered in the design, implementation and operation of widely deployed wireless security protocols and attacks developed to exploit these flaws.

Our investigation adopts the viewpoint of a hostile adversary to identify and exploit vulnerabilities that remain in wireless security protocols. Purpose-written software tools have been created to facilitate the investigation, conduct attacks and assist in the identification of the underlying causes of the security flaws. Remedial measures are then proposed, implemented and evaluated for the most serious threats.

This method is applied to an investigation of the security problems present in both current Land Mobile Radio (LMR) systems and next-generation wireless mesh networks. iii Firstly, the analysis of the APCO Project 25 LMR system was undertaken using tools developed for the purpose. These tools made use of a software-defined radio approach to provide full access to the wireless data link and allow for traffic to be captured, analysed, modified and injected. The utility of the software-defined radio (SDR) approach is that the code can be used to achieve goals which are not possible in commercially-available protocol analysers. The same code base can be used as the basis for prototyping remedial measures as well as to provide backward-compatibility for next-generation systems. This project has grown into a small free software project with a number of volunteers both professional and amateur and users in several countries including government agencies. The investigation into APCO Project 25 has uncovered a number of serious security flaws and, where appropriate, proposed remedial actions. These flaws include:

A denial of service attack that exploits the anti-theft mechanism that allows a hostile adversary to completely disable selected mobile radios.

A flawed authentication and access control mechanism that can be bypassed trivially by a hostile adversary.

A number of shortcomings in the design of the cipher system that can compromise the authenticity, integrity and confidentiality of message traffic.