MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
TERNOPIL IVAN PULUJ NATIONAL TECHNICAL UNIVERSITY
FACULTY OF COMPUTER INFORMATION SYSTEMS AND SOFTWARE ENGINEERING
COMPUTER SCIENCE DEPARTMENT

KARGBO BRIMA

UDC 004.04

AUTHENTICATION PROBLEMS AND ACCESS OPTIMIZATION TO INFORMATION WIFI NETWORKS

124 «System Analysis»

Abstract

diploma work for obtaining an educational degree "Master"

Ternopil
2018

The work was done at the Department of Computer Science Ternopil Ivan Puluj National Technical University Ministry of Education and Science of Ukraine

Surepvisor: Ph. D., Assoc. Prof of Computer Science Department
Roman Zolotyi
Ternopil Ivan Puluj National Technical University,

Reviewer: Ph. D., Assoc. Prof of Department of Informatics and Mathematical Modeling
Nadiia Hashchyn,
Ternopil Ivan Puluj National Technical University,

Defence of a thesis will be held at the Meeting of the Examination Board №29 on december 28, 2018 at 14.00 in Ternopil Ivan Puluj National Technical University (46001, Ternopil, Ruska st.56, building №1, room 702)

GENERAL CHARACTERISTIC OF THE THESIS

Actuality of the thesis lies in the fact that the author has investigated the authentication problems and access optimization to information WIFI networks.

The goal of the work: is to investigates WIFI networks authentication problems and access optimization for best quality of information.

Object, methods and sources of research. An experimental methodology is used which seeks low-level access to message traffic in order to understand the security flaws which may be present in the protocol. The investigation adopts a process in which technologies are studied both in theory and practise. Using low-level traffic analysis tools we investigate the operation of the protocol and identify possible routes for attack. Attacks are implemented under laboratory conditions and then countermeasures proposed in the light of experience gained from the attack implementation.

Scientific novelty of the obtained results: problems with authentication were investigated and recommendations for improving the network's wifi were issued.

Thesis tasks:

The purpose of this study is to answer the following questions:

– What are the security risks present when using wireless networks for public-safety and disaster recovery?

– Which of the identified security risks pose the most serious threat and what can be done to mitigate these threats?

– Identify the problems in authentication for the Wifi networks;

– Investigate the effectiveness of protection for Wifi systems;

– give recommendations to improving the authentication process of the Wifi systems;

– carry out a feasibility study on the decisions taken;

– perform additional sections on occupational safety, emergency and environmental safety.

The practical significance. The results of the work can be used to improve the authentication process of the wifi networks.

Thesis approbation. The results of work were reported on VI scientific and technical conference "Information models, systems and technologies" Ternopil, December 12-13, 2018

The structure of the thesis. The work consists of an explanatory note and graphic part. The settlement and explanatory note consists of an introduction, 7 parts, conclusions, a list of references and appendices. Scope of work: settlement and explanatory note - 97 pages of A4 format.

MAIN CONTENT OF THE THESIS

In introduction the analysis of the relevance of the topic and research tasks was carried out.

In the first section describes the scientific and technical problem.

In the second section all ways to authenticate devices in the network wifi and all possible problems with the authentication process were considered.

In the third section This chapter presents the research question, the associated hypothesis and describes the proposed research method and related procedures. The starting point of the investigation is the literature survey which is intended to uncover attacks which a hostile adversary can conduct to compromise the confidentiality, integrity or availability of the wireless network. The survey identifies the security threats faced by wireless networks in general and, in particular, to wireless mesh networks used for Public-Safety and Disaster Recovery (PSDR) applications.

Fourth section is devoted to recommendations for improving the effectiveness of Wifi systems authentication process.

Fifth section the issues of organization of production were considered and calculations of technical and economic efficiency of design decisions were made..

Sixth section the issue of the safety of life during the implementation of the results of work and safety in emergency situations was worked out..

Seventh section the issues of ecology and environmental protection during the implementation of the results of work were considered.

In general conclusions about the thesis the received technical decisions are given and organizational and technical measures which provide fulfillment of the given task are offered.

CONCLUSIONS

Computer networks are increasingly making use of wireless technologies to provide ubiquitous access. The high data rates available from wireless technologies allow for voice, video and data services to be extended to areas where such services were previously not available. WMNs in particular enable the rapid establishment of wireless coverage with a large service area and the promise of high data rates with a minimum required infrastructure. The collaborative nature of WMNs mean that there are many potential routes along which traffic may flow and provides route redundancy in the event of failures. The routing protocols autonomously discover routes between network nodes and repair them when they become damaged and lead to two of the key properties: that of self-organisation and self-healing. For these reasons WMNs have been suggested as a replacement for traditional network technologies for PSDR applications. The new technologies offer significant improvements in bandwidth, services and coverage when compared to traditional network technologies. The use of WMNs in a public-safety setting, however, raise new security threats and poses security risks that existing wireless security protocols do not adequately address.

The PSDR environment is one in which the availability of service assumes greater importance than in other settings. This is one reason why the self-healing property of the

network is desirable. Unfortunately this aspect of network security has been largely ignored in the existing wireless security protocols and there are a number of serious threats to availability exist as a result. Perhaps the best known of these threats are denial-ofservice attacks based on frame-spoofing. The hostile adversary can inject frames into the network which cause a loss of service because several important classes of frames are not protected by the security protocol. IEEE 802.11w addresses the most serious of these problems and authenticates management frames using the BIP. Despite the progress made by the IEEE 802.11w standards amendment there remain a number of serious concerns about the security protocols that are in use, or have been proposed, for PSDR wireless communications. We have identified cases where the protocols retain significant security defects which can be exploited by an adversary to deny service and to otherwise damage the integrity of the network. These problems are outlined below.

Cryptography is the necessary foundation for ensuring the confidentiality, integrity and authenticity of message traffic. When flaws exist in the design of the cipher system they are often the most significant threats posed to network security. Some flaws, such as those identified by Fluhrer et al. and Klein in the RC4 cipher lead to practical attacks which can undermine the safety of the cipher. The most robust defence at this time is the use of secure ciphers in protocols that have received scrutiny from the research community. In practical terms this means making use of the AES/CCMP cipher system provide an effective cryptographic protection for message traffic.

The ADP cipher system used by P25 makes use of the RC4 cipher but, by virtue of its design, it is not vulnerable to the attack described by Fluhrer et al. . The problems described by Klein are present because there remain correlations between the key and keystream. In practice, the most significant threat comes not from this direction but from the length of the key used by the cipher. This key is just 40 bits which we demonstrated to be vulnerable to recovery by an exhaustive key search using only modest resources. A similar situation exists for the DES/OFB cipher which is also used by P25. It has been known for some time that the DES cipher is no longer secure due to its limited 56 bit key size. The techniques for exhaustive key search have culminated in the use of FPGA devices which can conduct an exhaustive key search of the entire 56 bit key space in a matter of days.

Not all cryptographic flaws lead directly to key recovery. The most serious problems discovered by this investigation are problems associated with frame authenticity. If a message is not known to be authentic then it cannot be trusted but many of the attacks against wireless networks are the result of responding to messages that are not authentic. IEEE 802.11w has extended the security protocol so that the authenticity of management frames can be established but still leaves the acknowledgments unauthenticated and is vulnerable to frame spoofing attacks prior to the establishment of a secure association.

The Mac layer DoS attacks start with carrier-sense “jamming”. This has the benefit of being very simple and requires only that a low-power continuous signal is produced. With this attack there is a high probability of detection because of the continuous signal and the effect is constrained to the immediate vicinity of the transmitter. The virtual carrier-sense jamming attack is similarly simple and requires less energy than carrier-sense. There is a slightly lower probability of detection and the effect is similarly limited to the carrier-sense jamming attack.

Frame injection attacks have the advantage of being targeted towards specific stations. As a result they require limited energy and there is a low probability of detection. The effect can be targeted to disrupt the operation of the network by disabling important stations. Fortunately IEEE 802.11w provides effective countermeasures to this attack but this protection is not widely implemented and most networks remain vulnerable at the time of writing. The TKIP cryptographic DoS is a more difficult attack to affect. This attack requires very little energy and can halt traffic via a particular node. As such it represents a major problem but it affects only networks making use of TKIP. We recommend that this protocol be disabled and that AES/CCMP be used instead.

LIST OF PAPERS PUBLISHED BY THE AUTHOR OF THESIS

1. Brima K. Research of wifi systems protection / K. Brima, I. Opurum, R. Zolotyi // Materials of VI scientific and technical conference "Information models, systems and technologies", December 12-13, 2018. — P. 8. — (information systems and technologies).

ANNOTATION

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.

Key words: WIFI, PROTECTION, EFFICIENCY, RESEARCH, AUTHENTICATION PROCESS.