Articles

Overview of the Course in "Wireless and Mobile Security"

Maryna Yevdokymenko, Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine. E-mail: marina.ievdokymenko@nure.ua

Volodymyr Sokolov, Department of Information Cybersecurity, Borys Grinchenko Kyiv University, Kyiv, Ukraine. E-mail: vladimir.y.sokolov@gmail.com

Abstract — This paper provides an overview of "Wireless and Mobile Security" course. The course offers practical study of security issues and features concerning wireless security. The program of the course efficiently interleaves systematic theoretical knowledge and practical work. The theoretical part of the course includes basic information about the architecture of wireless networks, as well as available in this area to modern standards and protection mechanisms built into the equipment for wireless networks. It is also proposed an effective method for integrating a wireless network with the existing network infrastructure, taking into account all aspects of security. More than 50 percent of teaching time is devoted to practical work on the protection of wireless networks.

During the course skills to work with software NetStumbler, Kismet, AirSnort, Aircrack, and other monitoring wireless and network tools will be acquired. Particular attention is paid to the use of the most common tools of audit wireless networks, both commercial, and open source. In conclusion, a comprehensive approach to wireless security will be offered for each wireless technology.

Keywords: *Wireless Network; Wireless Security; Wireless Threats; Arduino IDE; Bluetooth; DECT; ZigBee; Rogue Access Point; RADIUS; WPA; WPA2; AES; TKIP; PEAP; TTLS; EAP-FAST; PololuWixel; Access Point, Spectrum Analyzer.*

INTRODUCTION

Wireless and mobile networks are rapidly extending their capabilities. One of the most beneficial features of wireless networks is that they support user mobility in a convenient way. The downside is that wireless networks are more susceptible to attacks than their wired counterparts. This increased vulnerability mainly stems from the lack of physical connections and the broadcast nature of radio communications. It is, therefore, important to provide appropriate security measures for wireless networks, which ensure the robustness of their operation even in case of malicious attacks.

In practice, many companies and organizations still use and deploy vulnerable wireless gear, often in their default configurations. This is most often due to poor security awareness or a lack of understanding of the risks and ramifications. Home computer users and businesses that lack security are putting themselves at risk of many serious problems, including (but not limited to):

- Identity theft and all the problems caused by it.
- Corruption of important files and data, installing viruses, etc.
- Other people reading your private details and information.
- Stealing of credit card numbers, bank account details and secure information.

- Large bills for the download of huge amounts of data by other people.
- Being reported for the download of illegal or copyrighted materials.
- Having your computer used as a part of a network to attack others.
- Handing control of your computer to those with unwelcome agendas.

Early wireless networks heavily leaned on Virtual Private Networks to provide Layer 3 security, which — aside from the additional overhead of encapsulation and challenges of roaming, Quality of Service, client support and scalability — left the IP network vulnerable to attacks.

Today current security features are ineffective, costly, or non-Universal. Home users want something they can figure out that works without having to purchase anything extra. Network administrators also consider cost, but their primary concern has to be making the network available to most of their users while still offering authentication and protection from intruders.

The goal of the course in "Wireless and Mobile Security" is to provide an overview of what is required to provide a secure communication channel in a wireless environment. The focus is on the security techniques available for wireless local area networks and for wireless devices used to access the Internet. This course assists in understanding wireless security requirements and their implementation.

A non-exhaustive list of topics to be taught includes:

- Security basics of the wireless network;
- Wireless data collection and Wi-Fi MAC analysis;
- Wireless tools and Information analysis;
- Client, crypto, and enterprise attacks;
- Bluetooth, DECT and ZigBee attacks;
- Advanced Wi-Fi attack techniques;
- Wireless security strategies, and implementation;
- Protection methods in mobile technologies.

Also, the purpose of the course is to provide knowledge in the security architecture of wireless and mobile communication systems, information threats models, vulnerabilities and protection abilities in wireless networks. After the course in "Wireless Security" the students will obtain practical skills in penetration testing of wireless networks and using various protection methods and will be able to:

- Design a wireless infrastructure;
- Choose wireless configuration;
- Create security policies;
- Set permissions rankings;
- Conduct an audit of the service network;
- Match the current network with other wired and wireless networks;
- Ensure the availability and scalability of the wireless network;
- Protect a mobile device and communication channels against cyberattacks.

So, the main contributions of the course in "Wireless and Mobile Security" are summarized as follows. Firstly, in this course a review of security threats and vulnerabilities at different protocol layers and commencing from the physical layer up to the application layer is presented,. Secondly, the family of security protocols and algorithms used in the existing wireless networks are summarized, such as the Bluetooth, Wi-Fi, WiMAX, and Long-Term Evolution (LTE) standards. Additionally, course provides a review on various wireless sniffers and tools as well as their detection and prevention techniques and proposes some of the open challenges in wireless security.

A. Security Basics of the Wireless Network

Security is especially important for Wi-Fi wireless networks. Hackers can easily intercept wireless network traffic over open air connections and extract information like passwords and credit card numbers. Several Wi-Fi network security technologies have been developed to combat hackers, of course, although some of these technologies can be defeated relatively easily.

As wireless communication and the Internet become truly interoperable, users will want this communication channel to be secure and available when needed. For a message sent using this communication channel, the user expects assurance of:

- Authentication (the sender and receiver are who they say they are).
- Confidentiality (the message cannot be understood except by the receiver).
- Integrity (the message was not altered).

The goal of this course is to provide an overview of what is required to provide a secure communication channel in a wireless environment. The focus is on the security techniques available for Wireless Local Area Networks (WLAN) and for wireless devices (e.g. cell phones and PDA's) used to access the Internet.

Wireless networking provides many advantages but it is also coupled with new security threats and alters the organization's overall information security risk profi le. Although implementation of technological solutions is the usual response to wireless security threats and vulnerabilities, wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identifi ed threats.

The wireless networks consist of such basic com-ponents: the transmission of data using radio frequencies; access points that provide a connection to the organizational network and/or the client's devices (laptops, PDAs, etc.) and users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamen-tal security objectives of confi dentiality, integrity, and availability.

Wireless Threats. Wireless networks are exposed to various threats and vulnerabilities. Wireless networks are vulnerable because of their open medium nature. The networks have dynamically changing topology and also there is no centralized monitoring and management. Generally, a threat model is used to classify threats or attacks. The attacks are classified into two categories namely passive attacks and active attacks.

Passive Attacks. Passive attacks are those attacks that only snoop the traffic without modifying the data or traffic between the two nodes. In this the attacker does not disrupt the normal routine, but only tries to gather valuable information from snooping the traffic. Examples of passive attacks are Eavesdropping, Man-in-the-Middle attack, Traffic Analysis etc. Active attack categories are WEP key cracking, evil twin AP and AP phishing, etc.

Active attacks. Active attacks are those attacks that either modifi es the data being exchanged or dropping of packets in network. Following are a list of active attacks in WLAN technology: Unauthorized Access, Rogue Access Point, Man-in-the-Middle Attack (MITM), Denial-of-Service, Reply Attack, Session Hijacking.

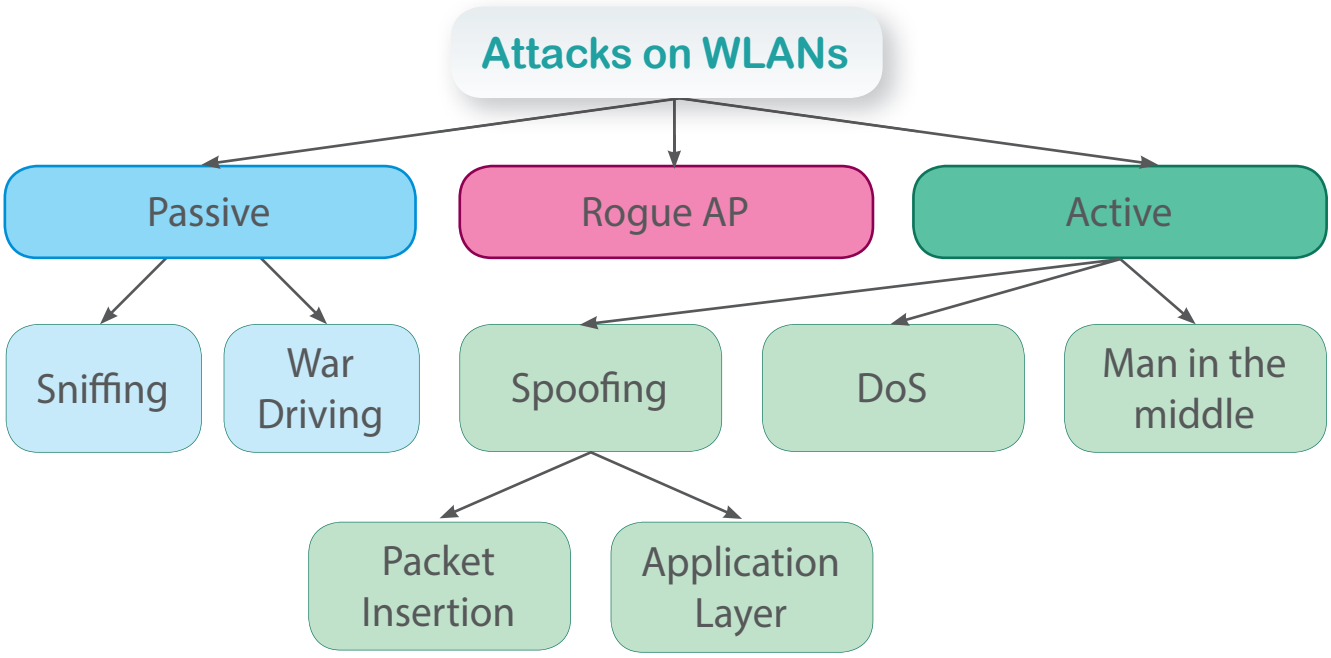

Fig. 1. Attacks on WLANs

There are also attacks against the various layers of TCP/IP protocol stack. The attacks can be shown as follows (*see Table I*).

Table I. Attacks against the various layers of OSI model

Layer	Attacks
Application	DoS, WORM, CSRF, SQL, Injection, Viruses
Transport	Session hijacking, covert channel
Network	Black hole, Byzantine, Wormhole, Rushing, Sybil
MAC layer	Signal jamming, sniffing

Application layer:

The application layer is responsible for running the services. The attacks that are made against this layer are Denial of Service, executing malicious code, worms, etc. The defense mechanism for this layer is proper maintenance of sequence numbers and also maintaining the routing information to avoid denial of service.

Transport layer:

The transport layer is vulnerable to session hijacking which can lead to an attacker taking over the session of a legitimate user and perform malicious actions. Another attack is the covert channel, i.e. hiding information in network header and using a channel for communication that goes undiscoverable. The defense mechanisms for the session hijacking are change of session ID immediately after logging into a session.

Network layer:

The attacks on network layer mainly involve the attacks on the various routing protocols used in ad hoc networks such as Ad hoc On-Demand Distance Vector (AODV) protocol and the Dynamic Source Routing (DSR) protocol. The various attacks taking place on these routing protocols are Black hole, Byzantine, Sybil and Wormhole attacks. These attacks are discussed in detail further.

MAC layer:

The attacks on MAC layer are associated with the channel allocation for the wireless medium. Various attacks such as signal jamming can lead to denial of service. Sniffing can lead to modification of the packets being transferred in the wireless medium. To avoid sniffing packets can be encrypted at the sender side and decrypted at the receiver side. There are various encryption techniques and the standards being used include WPA and WEP.

Multi-layer:

The attacks that occur in any layer of the network protocol stack come under this category. The attacks included are spoofing attacks, denial of service attack etc.

This section mainly focuses on:

- Wireless impact on traditional security approaches;
- Signal exposure threats;
- Common misconceptions in wireless security;
- Wireless LAN and MAN signal leakage;
- Information disclosure threats;
- DoS attacks;
- Rogue AP attacks;
- Wireless protocol deficiencies;
- Anonymity attacks;
- Home user threats.

Thus, in the first part of the course, all existing attacks in wireless networks will be analyzed.

In addition, the following issues will be discussed:

- Wireless standards bodies, role of the WiFi Alliance for interoperability testing, capabilities and features of WPA and WPA2, IETF standards, RADIUS, and EAP protocols.
- Enterprise impact of security-pertinent wireless standards including: 802.11z "Direct Link Setup", 802.11ac "Gigabit over Wi-Fi", 802.11af "Wi-Fi in TV White Space".
- Information about standards bodies work and working group resources.

As a result, the first section of the course "Wireless and Mobile Security" will cover all the principles of wireless LAN organizations, standards and the wireless threats.

Also, the risks and threats using BYOD will be discussed, as it can lead to data breaches and increased liability for the organization.

B. Wireless LAN Assessment Techniques

The second section of the course will present the important question of the wireless LAN assessment techniques.

In fact, companies should conduct regular, periodic security reviews to ensure that changes to the WLAN don't make the system vulnerable to hackers. A review once each year may suffice for low risk networks, but a review each quarter or more often may be necessary if the network supports high risk information (e.g., financial data, postal mail routing, manufacturing control functions, etc.).

When performing a wireless LAN security assessment, consider completing the following steps:

1. Review existing security policies.
2. Review the system architecture and configurations.
3. Review operational support tools and procedures.
4. Interview users.
5. Verify configurations of wireless devices.
6. Investigate physical installations of access points.
7. Identify rogue access points.
8. Perform penetration tests.
9. Analyze security gaps.
10. Recommend improvements.

In the course different methods and analysis for a WLAN audit will be discussed. For example, the application of the method of fingerprinting is associated with the fact that identifying devices connected to a network (i.e., device fingerprinting) has become of critical importance to ensure, among other security services, access control to the network. In the same vein, there has also been a need to understand the type of a device that is connected to a network (i.e., device type fingerprinting). Device fingerprinting seeks to uniquely identify devices on a network without considering existing easily forgeable identifiers (e.g., IP and MAC addresses). On the other hand, device type fingerprinting can be used to determine if a device belongs to a particular cohort. This method includes three categories: OS fingerprinting, host fingerprinting, and device type/driver fingerprinting.

The following WLAN assessment techniques will be described: client post-processing analysis with Kismet XML files, identifying the authentication and encryption options used on the WLAN with Kismet and Wireshark, techniques for mapping the range of indoor and outdoor WLANs, assessing traffic captured in monitor mode for information disclosure, identifying multicast protocols with MAC analysis, evaluating encrypted traffic and proprietary encryption functions, etc.

After the course the students will have a full understanding of the Rogue AP Analysis (*Fig. 2.*).

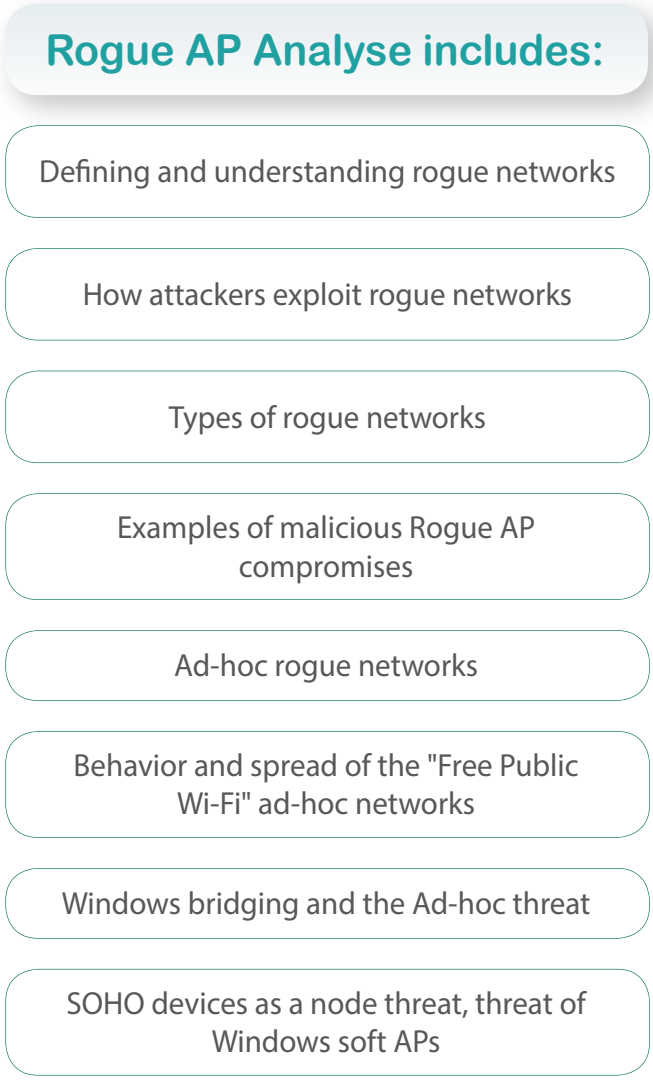

Fig. 2. Rogue AP analysis

Based on the analysis, different techniques will be offered for identifying rogue devices (such as: wired-side AP fingerprinting, wired-side MAC prefix analysis, wireless-side warwalking, wireless-side client monitoring, wireless-side IDS, Nmap rogue AP scripting analysis) and for preventing rogue APs (*Fig. 3*).

Establish strict rules and make sure they are well published	Change the rogue classification rules	Eliminate benign access points from the rogue list so that real rogues stand out
Add known intruders to the rogue list	Use strong security	Use active access points scanning in addition to passive scanning
Make sure the Juniper wireless signature is enabled and change it on a regular basis	Make sure logging is enabled and check log messages and traps for suspicious activity	Immediately investigate wireless bridge frames and eliminate the sourse
Consider using static IP addresses instead of having them assigned by a DHCP server	Use managed switches on your network and use their port-based security to allow only certain MAC addresses or disable unused ports	Immediately investigate ad-hoc access points and either add security to them or eliminate them

Fig. 3. Preventing rogue access points

Currently, there is already a number of different methods of protection:

- Encryption protocol WEP;
- WPA encryption protocol;
- WPA2 protocol;
- 802.1X security standard;
- Filtering by MAC address;
- Hiding the SSID;
- Denying access to the settings of the access point or router through the wireless network.

However, there is no difficulty in overcoming a wireless network security system Therefore, it is necessary to use a comprehensive approach to protect a wireless network. For this, the course will consider all methods of protection, starting with methods from Client, Crypto, Enterprise and finishing Advanced attack.

C. Client, Crypto, Enterprise, and Advanced Attacks

If in a wireless network of small dimensions using standard security methods is usually enough, in large networks, it is necessary to use a more thorough approach to security issues.

For a more detailed understanding of Enterprise attacks, the course will look in detail at the following issues:

- Understanding the risks and challenges of legacy authentication sources, how PEAP addresses this weakness using TLS.

- Understanding TLS tunnel establishment exchange and validation, behavior of PEAP Phase 1 and PEAP Phase 2 connections, identity disclosure in PEAP supplicants.
- Differences between WPA2-PSK and WPA-Enterprise authentication, EAPOL-Key distribution and use, PMK generation and delivery from RADIUS, PTK derivation and key rotation mechanisms.
- Attacks against PEAP networks including authentication attacks, Man-In-The-Middle attacks, EAPOL key-distribution attacks, client-specific attacks.
- Exploiting weaknesses in certificate validation mechanisms in Windows, Apple iOS, and Android platforms.
- Protecting PEAP networks, WZC recommended supplicant configuration properties, mitigating PEAP username disclosure with third-party supplicants, client firewall devices and wireless security recommendations.

Advanced Wi-Fi attack techniques are discussed in more detail. The most compatible wireless hardware configurations nowadays are WPA + WPA2 Mixed Mode, WPA-TKIP, WPA2-AES and WPA-AES, WPA2-TKIP.

D. Wireless Security Strategies and Implementation

The main goals of the course in "Wireless and Mobile Security" is to provide modern methods and techniques of preventing different types of existing attacks. Part of these methods are using Intrusion Detection System (IDS)/Intrusion Prevention System (IPS). The WIDS is the software that detects an attack on a wireless network or wireless system. A network IDS (NIDS) is designed to support multiple hosts, whereas a host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

1. *WIDS Deployment Models:*

WIDS deployment models can classify by three WIDS model categories: overlay deployment, integrated deployment, and hybrid deployment.

WIDS overlay deployment model (*Fig. 4*) has next advantages and disadvantages.

Advantages:

1. Ability to deploy a monitoring solution that is separate from the wireless transport provider.
2. The organization can leverage the overlay WIDS product to monitor for the vulnerability, if a vulnerability is discovered in the transport network implementation equipment.
3. Allowing organizations to monitor for the presence of unauthorized wireless devices.

Disadvantages:

1. Cost.
2. Organizations must deploy wireless sensor devices in all areas that require WIDS monitoring.
3. The lack of integration with the transport network can constrain the analysis capabilities of the overlay model.

The sensors passively listen to the events on the wireless network and use various analysis techniques to identify attacks.

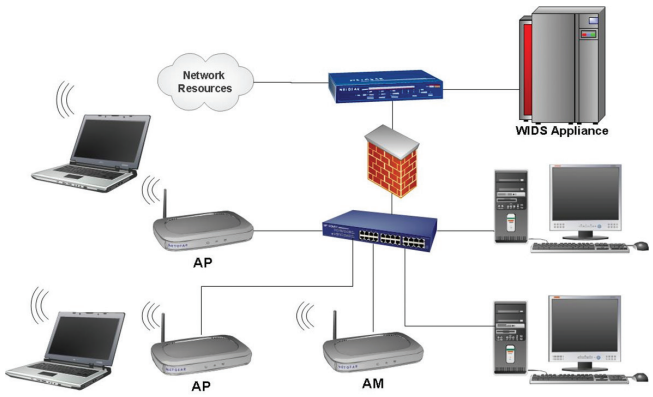

Fig. 4. Overlay WIDS Example, where AM — Air Monitors, AP — Access Point

2. *WIDS integrated deployment model:*

By using WIDS integrated deployment model the access point operates as both a transport provider, and a WIDS sensor, identifying and reporting attacks.

WIDS integrated deployment model characterizes the following advantages and disadvantages.

Advantages:

1. More cost-effective solution for organizations.
2. Has knowledge of dynamic encryption keys.

Disadvantages:

1. The lack of resources.
2. Must provide service and analysis capabilities, restricting the AP's ability to devote available CPU and memory resources to monitoring tasks.
3. Constrain to monitoring the frequency for which it is servicing users.

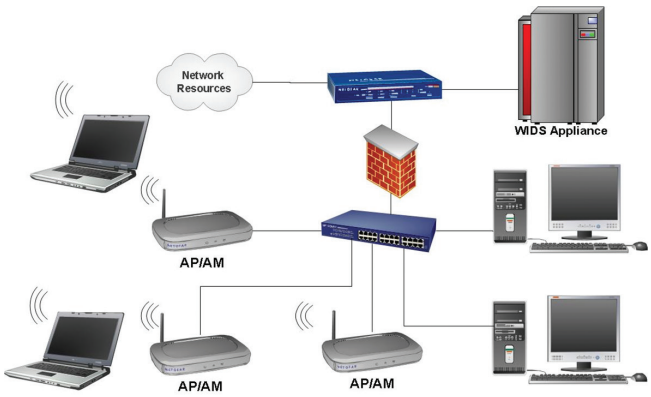

Fig. 5. Integrated WIDS Example, where Dual-purpose AP/ AM devices

3. *WIDS Hybrid Deployment Model:*

WIDS Hybrid Deployment Model uses both dual-purpose APs and dedicated AMs for intrusion detection and protection. Analysis is performed by a centralized controller similar to what is used with an overlay model, rather than the approach used in an integrated WIDS deployment, where processing is handled by distributed access points.

Advantages:

1. Increased flexibility in deployment.
2. Focused analysis mechanisms.
3. More comprehensive attack detection.
4. Powerful response mechanisms.
5. Using a centralized access controller that integrates an identity-based ICSA-certified firewall.

Disadvantages:

1. Cost.
2. The lack of resources.

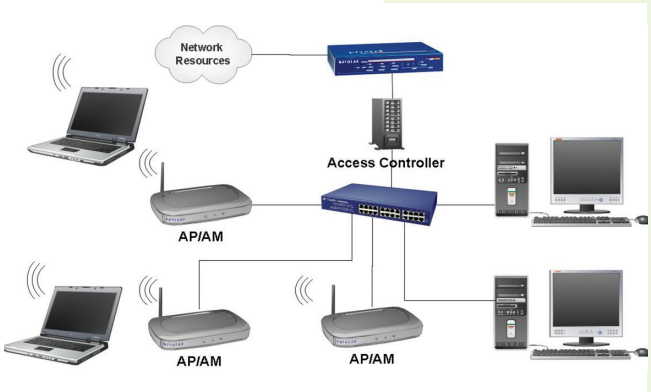

Fig. 6. Integrated WIDS example, where Dual-purpose AP/ AM devices

Methods for detection of attacks in modern Intrusion Detection Systems (IDS) not sufficiently elaborated in terms of the formal model of attacks, and for them it is quite difficult to strictly evaluate properties such as computational complexity, accuracy, etc. Intrusion detection methods are divided into methods for anomaly detection and misuse detection methods. The second type of methods are most of today's commercial systems (Cisco IPS, ISS RealSecure, NFR) — they use a signature (expert) detection methods. There are a lot of academic researches in the field of anomaly detection, but in industrial applications, they are used sparingly and with great caution, as these systems generate a large number of false positives. For expert systems the main problem is the low efficiency of detecting unknown attacks (adaptability). Low adaptability still remains a problem, although such advantages as a low computational complexity and low cost deployment of such systems determine dominance in this area.

4. *Methods of Intrusion Detection:*

In this section of the course the following criteria were selected for the comparative analysis of intrusion detection methods:

The level of system monitoring. This criterion determines the level of abstraction of the analyzed events in

the protected system, and determines the limits of applicability of the method for the detection of attacks on networks. The following levels are considered in this review:

- HIDS — Host-based IDS.
- NIDS — Network-based IDS.
- AIDS — Application-based IDS.
- Hybrid — A combination of different levels of observer.

Verifiability of the method. This criterion allows to evaluate whether a person can (for example, a skilled operator of IDS or expert) to reproduce the sequence of steps for the adoption of a decision on the presence of an attack by comparing the input and output of IDS. For example, signature-based methods will be considered verifi a ble, and clustered — not. Verifi a bility allows the correctness of the method and its implementation at any given time for peer review. The property of this method is important to the operation of the intrusion detection system in real environment as a means of gathering evidence about the attacks.

Adaptive methods. Assessment of the stability of the method to small changes in the implementation of the attacks, which do not change the result of the attack. Adaptability is the only signifi c ant a dvantage o f "alternative" methods of detection of attacks before "signaturebased". Lack of adaptability does not allow protection system to respond quickly to unknown attacks and requires the organization of the system some regular up-dating databases of known attacks, similar to antivirus systems.

Stability. Output method does not depend on the protected system. The stability problem is acute for statistical methods that analyze the absolute values of the parameters of performance and utilization of network resources and components. Trained in the same network recognizer can be sustained in this network, and unstable in all other networks. This stability will be called local. Since learning is usually an "expensive" procedure because it requires the use of large amounts of resources and time, the number of training procedures should be minimized. Methods for detection of attacks, analyzing the input semantics, are more stable than statistics.

Computational complexity. The complexity of this method of analysis is considered in the acquisition mode, without taking into account the possible preliminary stages of setup and training. This criterion is a key problem for intrusion detection in telecommunication networks. Complexity Estimation is sublinear, linear, quadratic, etc.

Based on the comparative analysis it can be concluded that none of the above open IDS does fully conform to the criteria of the "ideal" IDS. The main disadvantage is the lack of adaptability to unknown attacks and the inability to analyze the behavior of objects in a telecommunications network at the same time, at all levels.

Based on the analysis and identified disadvantage the requirements have been developed for modern IDS [6–9] that can be put into the development of a hybrid adaptive intrusion detection method based on signature analysis and state transition. It requires to:

- Cover all classes of attacks.
- Allow to analyze the behavior of the telecommunications network to be protected at all levels: network, nodes, and the level of individual applications.
- Be adaptable to unknown attacks (using an adaptive method of intrusion detection).
- Scale to telecommunications networks of different classes (from small local networks of class "home office" to large multi-segment and switched enterprise networks, providing centralized management of all IDS components).
- Have integrated mechanisms to respond to an attack.
- Be protected against attacks on IDS components, including interception control or attacks "denial of service".
- Be open.

So, the role of intrusion detection systems for information security has increased steadily. The cost of systems and the cost of exploitation for commercial IDS is very high. Given the growing popularity of open source software and its significantly lower cost, it appears that the role of free IDS will grow even faster.

Organizations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity. For most environments, a combination of network-based and host-based IDPSs is needed for an effective IDS solution. Wireless IDPSs may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities.

The course identifies deploying a secure wireless infrastructure, configuring and securing wireless clients:

- Recommendations for managing an authentication architecture, leveraging the RADIUS protocol for authentication validation, RADIUS data encoding rules, EAP transmitted over RADIUS.

- Understanding the impact of a compromised CA, "evil twin" attack.
- Recommendations and preferences for selecting an EAP type, understanding the advantages and disadvantages of EAP/TLS, PEAP, PEAPv1, PEAPv2, TTLS, EAP-FAST, PEAP-EAP-TLS.
- Four techniques for deploying a new root certificate authority: manual, web-server delivery, scripted web-server delivery, automatic trust with GPO.
- Managing client configuration settings with Windows, cached authentication credentials with PEAP on Windows WZC, deploying GPO settings for preferred wireless network, specifying the configuration and settings of preferred WZC networks, editing and implementing wireless-specific GPO policies, recommendations for securing PEAP through GPO.
- Managing third-part wireless manager tools with the Funk Odyssey supplicant, creating a custom installer with Odyssey manager.

Besides security in Wi-Fi network, Protection methods in Bluetooth, DECT, and ZigBee and Mobile technologies are also reviewed in the course.

E. Practical Skills in the Course in "Wireless and Mobile Security"

During the course, students acquire the skills to work with software NetStumbler, Kismet, AirSnort, aircrack and other wireless network monitoring tools. Particular attention is paid to the use of the most common tools of audit wireless networks, both commercial and open source.

The main topics for practice are listed below:

1. ***Wireless Network Mapping:***

The purpose of this practice is to obtain data on wireless networks and visualize the relationships between the elements.

After the study, the students must know and be able to:

- Collect data about wireless devices and their geolocation.
- Write a small Python scripts for data conversion.
- Make a wireless network mapping.
- Build a "client to access point" and "client to probe" relationship graphs.
- Use GPS module in wireless network scanning.
- Parse airodump-ng results and to export its as JSON.
- Make a GPS track on Google maps (for independent work).

2. ***Monitor Network Traffic:***

The purpose of this practice is to collect wireless network data using sniffer and analyze this data on vulnerabilities.

After the study, the students must know and be able to:

- Choose a sniffer for the monitoring of network traffic.
- Restrict on packet processing.
- Collect data from network sniffer.
- Write their own sniffer based on external tools.

3. ***WEP and WPS Hacking Technologies:***

The purpose of this practice is to consider the common methods of hacking Wi-Fi networks.

After the study, the students must know and be able to:

- Conduct attacks on Wi-Fi.
- Set up wireless access point based on known vulnerabilities.
- Test an AP on WEP and WPS vulnerabilities.
- Disable insecure services.

4. ***Research of Radio Frequency Wi-Fi Resources in 2.4–2.5 GHz Range:***

The purpose of this practice is to consider different ways to obtain information about the radiation levels in wireless networks without the use of special spectrum analyzers.

After the study, the students must know and be able to:

- Know ways to obtain information about the energy utilization of channels.
- Know how to get workload of the frequency range.
- Use a mobile phone to receive a list of available wireless networks.
- Determine the workload channel.
- In this practice there are two types of spectrum analyzers used:
- Fourier analyzer (FFT analyzer).
- Analyzers operating in accordance with the heterodyne principle.

In the course a lot of spectrum analyzers for the 2.4–2.5 GHz ISM band will be implemented to connect via USB-interface (FFT analyzer). For example, Ubiquiti AirView2, MetaGeek Wi-Spy, Wi-Detector, as well as on the basis of different sets of debugging (such as TI eZ430-RF2500) or network interface cards (e.g., Atheros AR92xx and AR93xx with Spectral Scan mode [3]). These devices have a number of drawbacks: the price; the difficulty of obtaining data that are usually tied to a particular program; the inability to change the firmware of devices. In addition, there are of course many homemade projects, usually based on TI CC2500 chip and Cypress 693x, as well as modules on their basis.

5. *Wi-Fi Fuzzing:*

The purpose of this practice is to make fuzz testing of wireless access point and to conduct security analysis of the part of PCI DSS standard that is responsible for the wireless network.

After the study, the students must know and be able to:

- Know different ways of Wi-Fi fuzzing.
- Know wireless part of PCI DSS standard.
- Make a fuzz testing of an AP.
- Security analysis of AP in accordance with PCI DSS standard.

Fuzz testing or fuzzing is a black box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion.

A fuzzer is a program which injects automatically semi-random data into a program/stack and detects bugs. The data-generation part is made of generators, and vulnerability identification relies on debugging tools. Generators usually use combinations of static fuzzing vectors (known-to-be-dangerous values), or totally random data. New generation fuzzers use genetic algorithms to link injected data and observed impact. Such tools are not public yet.

6. *Wi-Fi Network DoS Attacks:*

The purpose of this practice is to consider DoS ways to attack the Wi-Fi network.

After the study, the students must know and be able to:

- Know types of DoS attacks on the Wi-Fi network.
- Know typical signs of DoS attack.
- Test an AP by DoS attacking.
- Get an answer on the status of running AP.

A denial of service (DoS) occurs when a system is not providing services to authorized clients because of resource exhaustion by unauthorized clients. In wireless networks, DoS attacks are difficult to prevent, difficult to stop an on-going attack; the victim and its clients may not even detect the attacks. The duration of such DoS may range from milliseconds to hours. A DoS attack against an individual station enables session hijacking.

Jamming the air waves. A number of consumer appliances such as microwave ovens, baby monitors, and cordless phones operate on the unregulated 2.4 GHz radio frequency. An attacker can unleash large amounts of noise using these devices and jam the airwaves so that the signal to noise drops so low, that the wireless LAN ceases to function. The only solution to this is RF proofing the surrounding environment.

Flooding with associations. The AP inserts the data supplied by the station in the Association Request into a table called the association table that the AP maintains in its memory. The IEEE 802.11 specifies a maximum value of 2007 concurrent associations to an AP. The actual size of this table varies among different models of APs. When this table overflows, the AP would refuse further clients. Having cracked WEP, an attacker authenticates several non-existing stations using legitimate-looking but randomly generated MAC addresses. The attacker then sends a flood of spoofed associate requests so that the association table overflows. Enabling MAC filtering in the AP will prevent this attack.

Forged dissociation. The attacker sends a spoofed Disassociation frame where the source MAC address is set to that of the AP. The station is still authenticated but needs only to reassociate and sends Reassociation Requests to the AP. The AP may send a Reassociation Response accepting the station and the station can then resume sending data. To prevent Reassociation the attacker continues to send Disassociation frames for a desired period.

Forged deauthentication. The attacker monitors all raw frames collecting the source and destination MAC addresses to verify that they are among the targeted victims. When a data or Association Response frame is observed, the attacker sends a spoofed Deauthentication frame where the source MAC address is spoofed to that

of the AP. The station is now unassociated and unauthenticated, and needs to reconnect. To prevent a reconnection, the attacker continues to send Deauthentication frames for a desired period. The attacker may even rate the limit of the Deauthentication frames to avoid overloading the already congested network. The mischievous packets of Disassociation and Deauthentication are sent directly to the client, so these will not be logged by the AP or IDS, and neither MAC filtering nor WEP protection will prevent it.

Obviously, the primary thing they can do is to force stations (clients) off of a given network, causing a DoS attack. It can also use death attacks to reveal otherwise hidden SSIDs (not included in beacon frames) by disconnecting the clients, and then monitoring for Probe Requests which always contain the SSID.

7. *Over the Air (OTA)*

The purpose of this practice is to check the firmware updates over the network; to analyze the data transmitted over the network during the upgrade; to investigate the possibility of substitution of transferred firmware.

After the study, the students must know and be able to:

- Know principles of OTA.
- Know weak spots of OTA.
- Create the firmware.
- Provide online firmware.

OTA update is the process of loading the firmware to ESP module using Wi-Fi connection rather that a serial port. Such functionality became extremely useful in case of limited or no physical access to the module.

OTA may be done using:

- Arduino IDE.
- Web Browser.
- HTTP Server.

Arduino IDE option is intended primarily for software development phase. The two other options would be more useful after deployment, to provide module with application updates manually with a web browser or automatically using a http server.

In any case first firmware upload has to be done over a serial port. If OTA routines are correctly implemented in a sketch, then all subsequent uploads may be done over the air.

There is no imposed security on OTA process from being hacked. It is up to developer to ensure that updates are allowed only from legitimate / trusted sources. Once update is complete, module restarts and new code is executed. Developer should ensure that application running on module is shut down and restarted in a safe manner. Chapters below provide additional information regarding security and safety of OTA process.

8. *Research of Stress Loading of Wireless Network:*

The purpose of this practice is to assemble a sample of the test access point based on single-board computer; to explore one of the security aspects of wireless infrastructure — availability.

After the study, the students must know and be able to:

- Restrict imposed on the wireless infrastructure.
- Know methods of collecting system information in OS Linux.
- Establish basic network services for wireless access points in OS Linux.
- Work with the indicator displays (OLED).

Availability is ensuring that authorized users can access and work with information assets, resources, and systems they need, while providing the required performance. Ensuring availability includes measures to support access to information, despite the possibility of interference, including system failure and deliberate attempts to violate availability. The protection of access to and the capacity of mail service would be an example.

Ensuring availability is to identify possible points of failure and liquidation of these points. Strategies for reducing the negative consequences of failure can be management and technology.

The first step is to identify potential points of failure in the network infrastructure. These mission-critical devices, such as switches and routers, as well as the basic terms of the functioning of servers, such as DNSs, need to be analyzed in terms of a possible failure and its impact on the functioning of the IT capabilities. This is related to risk management — identify and minimize risk.

From the standpoint of availability, the following definitions can be given.

Reliability — the ability of a system or an individual component to perform its required function under certain conditions in the specified time period.

Redundancy — the creation of one or more copies (backup) systems, which are available in the event of primary system failure or the presence of the additional capabilities of the system for the organization of its resiliency.

Resiliency — method of operation, in which the functions of the system component (such as CPU, server, network or database) run redundant components in case of failure or a planned shutdown major component. The ability of a system or component to continue to function normally in case of failure of equipment or software.

It is necessary to analyze the possible points of failure in the following components: data, system components, network topology, routers and switches, some critical services.

9. *125 kHz RFID Sniffing*

The purpose of this practice is to consider the work of EM-Marin (EM4100 or EM4102) protocol for 125 kHz RFID and sniff it.

After the study, the students must know and be able to:

- Know EM-Marin protocol.
- Receive data from RFID.
- Sniff and analyze data from RFID.

EM4100 (EM4102, EM-Marin) is a format of contactless radio frequency ID cards by the company EM Microelectronic-Marin (one of the most popular in Ukraine).

They belong to a class of passive RFID cards, because they do not have a built-in power supply. They operate in the frequency range 125 kHz and have a unique number of 40-bit.

They are available in a variety of forms (the most common Clamshell cards, ISO 7810 cards, key rings). ISO-card can be issued in addition to the magnetic stripe identification number, made by stamping, a field for the signature of the cardholder. Personalization ISO-cards is made by thermal printing, screen printing, offset printing. Personalization Clamshell-cards are made using labels that are applied to all the necessary information.

The reader generates a magnetic field frequency of 125 kHz. Once in the magnetic field of the reader, the card receives power and begins to cyclically modulate the magnetic field of the reader signal in which its identification code is encrypted. The range of labels is ranging from 5–10 to 60–70 centimeters, depending on the structural elements tags and readers.

Modulation method of the carrier is amplitude. Data encryption — Manchester. 64 bits, including 40 bits of proper unique number, the special synchronization sequence and parity check bits are cyclically transmitted.

The main use is the control of access to the premises and a car park. A distinctive feature of identity cards Em-marine is lower cost compared to other proximity-card standard (e.g., HID or Mifare).

F. Equipment and Software Components for the Workplace.

Many manufacturers of wireless equipment insert algorithms, but the spectrum is scanned only in the location area of AP, thus, they do not consider particularly customer location. AP starts at the clear channel at the place of its location, which to some extent improves the performance of the entire network, but does not make it the optimal.

Usually existing wireless cards are used for collecting the information, but their range of visibility is often limited only by the IEEE 802.11 standard networks (and some maps do not even see "hidden" networks). Because universal method should consider the use of additional independent devices (spectrum analyzers).

For conducting good practice our course offers a spectrum analyzer for separate scheme. The control unit implemented on Arduino Nano v3.0 (with 3.3V supply) and the receiver — on TI CC2500+PA+LNA module with external antenna. Scheme is equipped with OLEDs 0.96" 128×64 I2C and SPI SSD1306 for visualizing the measurement results. The program is written in Arduino IDE and compiled with GCC.

The *Fig. 7* shows a diagram of the connection module and power to the device. This device can be operated with a controller that receives data via a USB interface (the virtual COM port). On two screens displayed range of 2400.01–2503.40 MHz with spacing in 405.5 kHz. And *Fig. 8* shows an example of display device assembly in a transparent case.

It was found that the control unit memory is not enough (only 2 KB of RAM) to analyze the available channels. Also, this device does not fulfill one of the requirements — must be non-directional antenna, and the half-wave dipole has a distinct polarization.

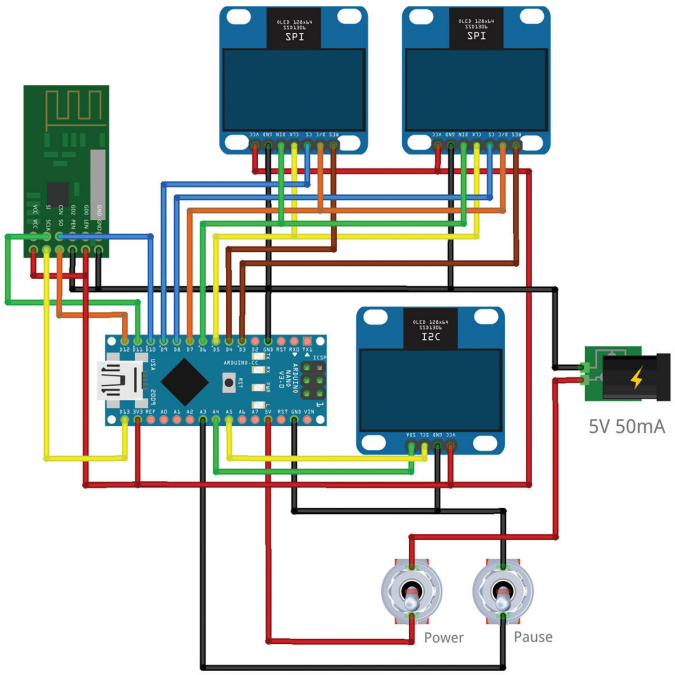

Fig. 7. Schematic diagram of separated receiver and control unit

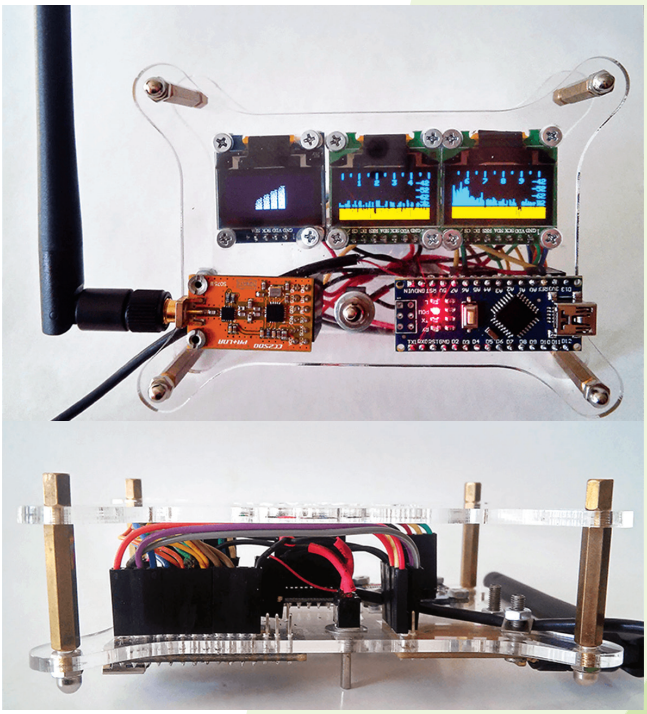

Fig. 8. Separated receiver with external antenna and control unit

To implement the analyzer on a single chip Pololu Wixel has been selected, whose RAM size is 4 KB, the non-directional antenna, five times lower power consumption, almost one and a half times better resolution and SDK with detailed documentation.

Spectrum analyzer on PololuWixel (CC2511F32) with SPI and/or I2C OLED's SSD1306. The spectral width is 2403.47–2476.50 MHz with spacing in 286.4 kHz on two SPI displays. Displays available channels on I2C display. This scheme takes less than 10mA (on 5V).

Prototype can be assembled in a clear acrylic case for Raspberry Pi, but can be built more compactly. Button with a red cap — switch on, and the second one — pause. The left screen displays ZigBee and Wi-Fi channels (not all channels fall within the available range).

So, for practice in the course "Wireless and Mobile Security" the following equipment will be used:

1. Arduino Nano v3.0.
2. TI CC2500+PA+LNA module with external antenna.
3. PololuWixel.
4. OLED's SSD1306 SPI or I2C.
5. Raspberry Pi 3.
6. GPS module (e.g., NEO-6M).
7. UART to TTL adapter with 3.3 V levels (optionally).
8. NodeMCU (ESP-12E).

In the process of learning the course, students will acquire skills to work with different software components: Kismet, AirSnort, Ettercap, Wixel SDK, Arduino IDE, WiFiBeaconJam, WIDS, WIPS, Aircrack and other wireless network monitoring tools.

SUMMARY

The world of wireless and mobile devices is evolving day-to-day, with many individuals relying solely on their wireless devices at workplace and at home. The growing use of mobile devices demands that organizations become more educated in securing this growing technology and determining how to protect their assets best. Using case studies and real-world events, it goes on to discuss risk assessments, threats, and vulnerabilities of wireless networks, as well as the security measures that should be put in place to mitigate breaches.

The wireless networks consist of four basic components: the transmission of data using radio frequencies; access points that provide a connection to the organizational network and/or the client devices (laptops, PDAs, etc.); and users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

Due to the intensive development of wireless networks course in "Wireless and Mobile Security" is very important. The course covers a comprehensive wireless and mobile security overview including the design, planning, installation, and maintenance of wireless network security infrastructures.

The course in "Wireless and Mobile Security" provides knowledge in security architecture of wireless and mobile communication systems, information threats models, vulnerabilities and protection abilities in wireless networks. The students will obtain practical skills in penetration testing of wireless networks by using various protection methods.

REFERENCES

[1] Wireless Geographic Logging Engine database *https://wigle.net/graph-large.html.*

[2] **Astapenya V. M., Sokolov V. Yu.** "Modified accelerating lens as a means of increasing the throughput, range and noise immunity of IEEE 802.11 systems," ICATT'2015 Proceedings of the X Anniversary International Conference on Antenna Theory and Techniques, Kharkiv, Apr. 2015, pp. 267–269.

[3] "CC2500 Low-Cost Low-Power 2.4 GHz RF Transceiver," Texas Instruments, 2016, 97 p.

[4] "Pololu Wixel User's Guide," Pololu Corporation, 2015, 67 p.

[5] **V. Buryachok, G. Gulak, V. Sokolov.** "Miniaturization of Wireless Monitoring Systems 2.4–2.5 GHz Band," Proceedings of the II International Scientific-Technical Conference on Actual Problems of Science and Technology, Kiev, Dec. 2015, p. 41.

[6] "nRF24L01 Single Chip 2.4GHz Transceiver Product Specification," Nordic Semiconductor ASA, Version 2.0, July 2007, 74 p.

[7] **Graham E., Steinbart P. J.** Wireless Security. 2006.

[8] Cisco. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, 19 July 2004.

[9] CSI. CSI/FBI Computer Crime and Security Survey. 2004.

[10] **Hopper D. I.** (2002). Secret Service agents probe wireless networks in Washington.

[11] IEEE 802.11-2007, New York, NY, USA. 2007.

[12] IEEE 802.11i-2004, New York, NY, USA. 2004.

[13] **Bellardo J., Savage, S.** 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proceedings of the 12th USENIX Security Symposium, Berkeley, CA, USA, USENIX Association, 2003.

[14] **Aime M. D., Calandriello G., Lioy A.** Dependability in wireless networks: Can we rely on Wi-Fi IEEE Security and Privacy 5, p. 23–29, 2004.

[15] **Devine C., d'Otreppe T., Beck M.** Aircrack-ng. 2009. *http://www.aircrack-ng.org.*

[16] **Smith J.** Denial of service: Prevention, modelling and detection. 2007.

[17] **Glass S., Muthukkumarasamy, V.** A study of the TKIP cryptographic DoS attack. In: ICON 2007: Proceedings of the 15th IEEE International Conference on Networks, New York, NY, USA, IEEE, p. 59–65. 2007.

[18] **Tews E., Beck M.** Practical attacks against WEP and WPA. In: WiSec '09: Proceedings of the second ACM conference on Wireless network security, New York, NY, USA, ACM, p. 79–86. 2009.

[19] IEEE: IEEE 802.11e-2005, New York, NY, USA. 2005.

[20] **Halvorsen F. M., Haugen O., Eian M., Mjølsnes S. F.** An improved attack on TKIP. In: NordSec '09: Proceedings of the 14th Nordic Conference on Secure IT Systems, Berlin, Heidelberg, Springer-Verlag, p. 120–132. 2009.

[21] IEEE: IEEE 802.11h-2003, New York, NY, USA. 2003.

[22] **Harkins D.** Attacks against Michael and Their Countermeasures. IEEE 802.11 Working Group Document 03/211r0, New York, NY, USA. 2003.

[23] The OpenWrt Project: OpenWrt. 2009. *http://www.openwrt.org.*

[24] **Malinen J.** Hostapd: IEEE 802.11 AP, IEEE 802.1X / WPA / WPA2 / EAP / RADIUS Authenticator. 2009. *http://hostap.epitest.fi/hostapd.*

[25] **Zarate J.** Tomato Firmware (2009) *http://www.polarcloud.com/tomato.*

[26] Cisco Systems Inc.: Enterprise Mobility 4.1 Design Guide, San Jose, CA, USA. 2009.

[27] **M. Beck.** Enhanced TKIP michael attacks. Retrieved 4 February, 2013, from *http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf.*

[28] **J. Bellardo** and **S. Savage.** 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In Proceedings of the USENIX Security Symposium, 2003.

[29] **K. Bicakci** and **B. Tavli.** Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks, 2009.
[30] **A. Stubblefield, J. Ioannidis, A. D. Rubin.** A key recovery attack on the 802.11b wired equivalent privacy protocol (wep). ACM Trans. Inf. Syst. Secur., 7(2), 2004.
[31] **E. Tews, M. Beck.** Practical attacks against WEP and WPA. In Proceedings of the second ACM conference on Wireless network security, WiSec '09, 2009.
[32] **Y. Todo, Y. Ozawa, T. Ohigashi, M. Morii.** Falsification attacks against WPA-TKIP in a realistic environment. IEICE Transactions, 95-D (2), 2012.
[33] **F. M. Halvorsen, O. Haugen, M. Eian** and **S. F. Mjølsnes.** An improved attack on TKIP. In 14th Nordic Conference on Secure IT Systems, NordSec '09, 2009.
[34] **B. Harris, R. Hunt.** Review: TCP/IP security threats and attack methods. Computer Communications, 22(10):885–897, 1999.
[35] **J. Huang, J. Seberry, W. Susilo, M. W. Bunder.** Security analysis of michael: The IEEE 802.11i message integrity code. In EUC Workshops, pp. 423–432, 2005.