Journal of Computing and Information Technology - CIT 15, 2007, 3, 237–255
doi:10.2498/cit.1000877

A Survey of Wireless Security

Radomir Prodanović[1] and Dejan Simić[2]

[1]Air Forces and Aircraft Defense, Serbian Army, Serbia
[2]Faculty of Organizational Sciences, University of Belgrade, Serbia

Constant increase in use of wireless infrastructure networks for business purposes created a need for strong safety mechanisms. This paper describes WEP (Wired Equivalent Privacy) protocol for the protection of wireless networks, its security deficiencies, as well as the various kinds of attacks that can jeopardize security goals of WEP protocol: authentication, confidentiality and integrity. The paper also gives a summary of security improvements of WEP protocol that can lead to a higher level of wireless network infrastructure protection. Comparative analysis shows the advantages of the new 802.11i standard in comparsion to the previous security solutions.

Keywords: authentication, confidentiality, integrity, WEP protocol, deficiencies of WEP, security threats to 802.11, TKIP, 802.1x, WLAN safety improvements, RC4, AES

1. Introduction

Wireless networks are becoming more and more popular today. Big corporations are using them more and more often due to their advantages. Popularity of local wireless networks owes much to their advantages, such as: user mobility, fast and simple installation, flexibility, scalability and relatively low price. WLAN (Wireless Local Area Network) enables users to access resources no matter of the place they occupy. By using mobile computers, users can have the access to the resources no matter of their location within the wireless network. All the above mentioned advantages come from the medium that transfers the data – with the wireless networks, it is the air. Data are transferred via radio waves spreading throughout the space and thus the information reaches anyone with the appropriate radio receiver. Therefore, there is a problem of the protection of information. Traditional mechanisms for the physical protection of wired networks (firewalls and shields) cannot be applied to the protection of wireless networks. It was necessary to create mechanisms for the protection of the wireless networks in order to enable users to use wireless networks and feel sure about the accuracy of information and their privacy. 802.11i standard for wireless local networks introduces WEP protocol to try to solve the problems of protection and to make the level of protection of wireless local networks similar to the protection level of wired local networks.

The remainder of the paper is organized as follows. Section 2 specifies various kinds of attacks that can jeopardize security goals of WEP protocol: authentication, confidentiality and integrity. Section 3 describes WEP protocol for the protection of wireless networks. Section 4 deals with the basic security deficiencies of the WEP protocol. Significant safety improvements of WEP protocol that can lead to a higher level of wireless network infrastructure protection are described in Section 5. This section also gives the comparative analysis of WEP protocol and WPA and WPA2 solutions with clearly identified advantages of the new IEEE 802.11i standard in comparison to previous safety solutions. Section 6 describes two symmetrical cryptographic algorithms, RC4 and AES, used for wireless protocols in order to maintain data confidentiality and integrity. The conclusion is given in Section 7.

2. Security Threats to 802.11 Wireless Networks

Protection of wireless networks means protection from attacks on confidentiality, integrity and availability. There are four attack techniques that can violate confidentiality or privacy

[1]: traffic analysis, passive eavesdropping, active eavesdropping with partially known plaintext and active eavesdropping with known plaintext. One of these techniques can be applied to violate both confidentiality and integrity or only confidentiality and only integrity.

Traffic analysis. It is a very simple technique that enables an attacker to take over a packet during its transmission. This technique enables the attacker to have access to three types of information. The first type of information is related to identification of activities on the network. The second type of information important to the attacker is identification and physical location of AP in its surroundings. The third type of information an attacker can get by traffic analysis is information about the communication protocol. An attacker needs to gather the information about the size and number of the packet over a certain period of time.

Passive eavesdropping. This technique is used to watch over an unlimited wireless session. The only condition to be fulfilled is that the attacker has the access to the area of emission. With a decrypted session the attacker is able to read the data during its transmission and gather them indirectly by surveying the packets. This kind of attack is not based on violation of privacy, but information gathered in this way can be used for more dangerous kinds of attacks.

Active eavesdropping with partially known plaintext. During this type of attack, the attacker watches over a wireless session and actively injects his own messages in order to reveal the content of the messages in the session. Precondition for this type of attack is access to communication area and some knowledge on the part of the message, such as IP address. The attacker is able to modify the content of the packet so that the integrity of the message remains preserved. Usually the attacker changes final IP or TCP address.

Active eavesdropping with known plaintext. In this type of attack, the attacker injects messages known only to him into the traffic in order to create conditions for decryption of the packets that should be received by other wireless users. These conditions are created by creating IV sequence and message for each single message that is sent. After some time, when a packet with the same IV as in the database appears, the attacker is able to decrypt the message. The only way to prevent this kind of attacks is to change WEP key often enough.

There are three techniques that can violate the integrity of the traffic [1]: unauthorized access, highjacking attack and replay attack. In order to successfully implement these techniques, it is necessary to apply attack techniques for privacy.

Unauthorized access. The above mentioned attacks are directed towards the network in general, not towards users. But, once the attacker gets access to the network, he is able to initiate some other types of attacks or use network without being noticed. Some may think that unauthorized use of the network is not a significant threat to the network since the access rights allocated to resources will disable the attackers. However, usually, an unauthorized access is the key to initialization of ARP (Address Resolution Protocol) attack.

VPN (Virtual Private Network) and IPsec solution can protect users from the attacks that directly influence the confidentiality of application data, but it cannot prevent attacks that indirectly ruin confidentiality. Man in the middle, highjacking and replay attacks are the best examples of these kinds of attacks.

Man-in-the-middle-attack. This attack enables data reading from the session or modifications of the packets which violate integrity of the session. There are several ways to implement this type of attack. One is when an attacker disrupts the session and does not allow the station to re-establish communications with the AP. The station tries to establish session with the wireless network through AP, but can do that only through the workstation of the attacker pretending to be AP. At the same time, the attacker establishes connection and authentication with the AP. Now there are two encrypted tunnels instead of one: one is established between the attacker and AP, while the second is established between the attacker and the station. This enables the attacker to get access to the data exchanged between the workstation and the rest of the network.

ARP attacks. This is the sub-type of the man-in-the-middle attack since these attacks are directed towards one component of wired network [2] and towards wireless clients [3]. The attacker escapes authentication or provides false accreditations. By geting the false accreditations, the attacker becomes a valid user and gets the access to the network as authenticated user.

Highjacking attacks. By this type of attack, the attacker deprives the real owner of the authorized and authenticated session. The owner knows that he has no access to the session any more, but is not aware that the attacker has taken over his session and believes that he has lost the session due to ordinary failures in network functioning. Once the attacker takes over a valid session, he can use it for various purposes over a certain period of time. Such attack could be combined with DoS attack [4]. It happens in a real time.

Replay attack. This type of attack is used to access the network through authorization. The session under attack does not change or disrupt in any way. The attack does not happen in a real time. The attacker gets the access to the network after the original session expires. He comes to the authentication of one or more sessions, and then replies to the session after a certain period of time or uses a couple of sessions to compose the authentication and reply to it.

There are several types of DoS (Denial of Service) attacks that can violate availability of the network. Jamming and attack on 4-way handshake are only some of the DoS attacks.

Jamming. Jamming [5,6] is one of DoS attacks on network availability. It is performed by malicious attackers who use other wireless devices to disable the communication between users in a legitimate wireless network.

Attack on 4-way handshake. The last phase in the authentication process, 4-way handshake process, proved to be unsafe for DoS attacks, though some of the attacks start in the first phase of the authentication process, but appear during the 4-way handshake process. In order to prevent the processor and the waste of memory resources, static and dynamic 4-way handshake solutions for protection from DoS attacks [7], as well as solutions for early detection of DoS attacks in the first phase of the authentication [8] have been introduced.

3. WEP Protocol

WEP protocol is the basic part of IEEE 802.11 (IEEE – Institute of Electrical and Electronics Engineers) standard for the protection of WLAN networks. The basic function of WEP protocol is to provide data security in wireless networks in the same way as it is in the wired networks. Lack of physical connection among users and wireless networks enables all users within the network range to receive data if they have appropriate receivers. The only possible way to protect this kind of network was to create a protocol that would work on the second layer of OSI model and, in this way, provide the data protection during the transmission. In order to protect data transmitted among the communicating parties, WEP uses shared secret key of

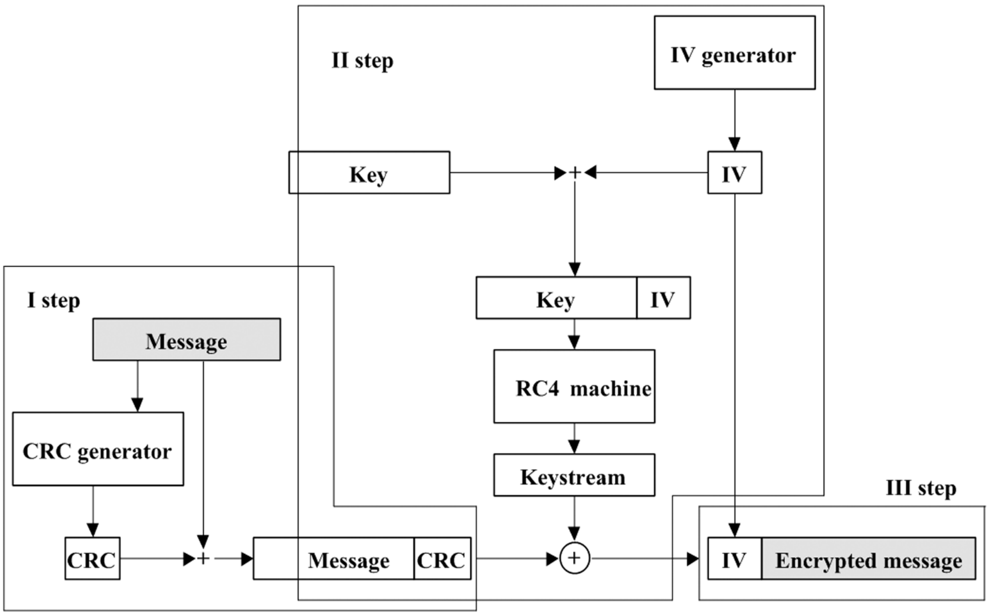

Figure 1. WEP protocol execution.

40 to 140 bits. WEP protocol is applied through the following three steps [9]:

— CRC (Cyclic Redundancy Code) message is calculated and added to the original message.

— The second step in WEP protocol application is encryption (as shown in Figure 1). The message is encrypted by RC4 algorithm. Encryption is d one in three phases. First, pseudo-random data sequence of three bytes is generated (IV – Initialization Vector) to extend the key. Then RC4 algorithm generates keystream based on the new key. Encryption ends with the application of exclusive or function (XOR) between keystream and message thus resulting in encrypted message.

— The last step is to transmit sequence IV and encrypted message.

Once the message has come to its final destination, the reverse procedure is applied. Again, the extended key is generated on the basis of transferred IV and shared key; then RC4 algorithm generates keystream, XOR function is calculated between keystream and message that arrived, and, as a result of XOR function, decrypted message is received. The accuracy of CRC sum for a decrypted message is calculated by CRC of the decrypted message. Then it is compared to the sent CRC. If the decrypted message CRC is the same as the sent CRC, the message received matches the message sent.

WEP protocol should achieve three main safety goals [10]:

Authentication. It is the procedure used to confirm identity of the communication participants. According to IEEE 802.11 specification, there are Open System Authentication and Shared-key Authentication. *Open System Authentication* enables mobile stations to access the access point without confirmation of the station's identity. This is a one-way authentication since mobile stations believe to communicate with the right access point. Open System Authentication is very sensitive to attacks and allows unauthorized access. *Shared-key Authentication* is based on encryption technique and on questions and answers procedure between a station and the access point. The authentication process is ended when the access point decrypts the station's answer by shared key and thus enables the access of the workstation only if decryption result is equal to the question that has been sent.

Confidentiality. In 802.11 standards the confidentiality is realized by encryption technique. WEP protocol for the protection of confidentiality uses RC4 algorithm and symmetrical key together with pseudo sequence. In general, every increase in key length brings the increase in protection. However, recent brute-force attacks on wireless local networks are jeopardizing privacy. This means that WEP protocol is sensitive to attacks no matter of the key length.

Integrity. WEP protocol provides integrity of messages transmitted between stations and access point by using CRC technique. Integrity of message received is violated when the checksum differentiates. In this case, the message received is rejected.

4. Security Deficiencies of WEP Protocol

Although WEP protocol uses RC4 algorithm that is highly reliable, there are several safety deficiencies. This section describes WEP protocol deficiencies.

The risk of keystream reuse. In [11,12] WEP protocol a key is extended by IV stream in order to get different keystreams for encryption of each of the transferred frames. However, there are some deficiencies in using the keystreams. The deficiency is in the result that we get when calculating XOR function with the arguments that represent two messages encrypted by the same keystream – the result is the same as if the XOR was calculated between plaintext encrypted by the same keystream. If the result generated by the XOR function applies to one plaintext we can then decrypt the second encrypted message.

The risk of keystream reuse is security deficiency of WEP protocol. This problem is caused by repeating IV sequence since:

— The key is changed rarely, so when the same IV is generated together with the same key that has not been changed, we get a repeated keystream. Attackers can very easily access the IV since it is not encrypted during the packet transmission.

— Some of the PCMCI cards reset IV to 0 each time they are initiated.

— WEP standard proscribes the length of IV that cannot be changed.

Key management. A standard does not specify in what way the key distribution is done. Globally shared key of 4 streams was in use for some time. Each message contained a field for the identification of a key that is in use. However, this principle was not sustainable, so now we have mainly one key in a wireless network. This means that if one key is used by more than one user, chances for key decryption are increased. Administrators set user workstation configurations alone, in order to solve this problem. The best way is to change the key often enough. This, however, requires reconfiguration of wireless network driver on the each of the workstations each time the key is changed. The problem may occur with the large scale networks since it is time consuming. Wireless networks without key management enable attackers to analyze the data transmitted through the network easily and make IV base for message decryption.

WEP protocol uses checksum generated by CRC-32 algorithm to check if the message is changed during the transmission. Checksum alone cannot prevent attackers from falsifying the message being made to detect accidental errors in the message and not to prevent message modifications. Therefore, the attackers are able to modify the message or inject some other message.

Message modification. Message modification means modification of messages in the process of transmission. The message receiver will not notice that the message was modified. This security deficiency takes origin from the WEP checksum that is linear function of the message. Due to linear characteristics of the checksum, there is a possibility to control modifications in the encrypted message without changing the checksum. This means that it is possible to do any modifications in an encrypted message with no fear that the receiver will notice these modifications.

Message injection. This security deficiency of WEP protocol comes from two WEP protocol characteristics:

— WEP checksum is an unlocked function, and

— It is possible to apply the old IV functions with no detection by receiver.

Due to the first characteristic, anyone knowing the message can calculate the checksum field. This allows escaping access control measures. The second characteristic enables attackers to inject their message in case they know IV sequence and keystream. An attacker encrypts his own message by knowing the keystream and sends it to the receiver. Since the message comes with the IV sequence, the receiver will be able to decrypt the message without noticing that the message was injected.

Message decryption. Possibility of modifying encrypted packets without being noticed can be applied for decryption of the messages sent to users. WEP uses keystream that is presumably safe (RC4), which means that direct attack on encryption will not succeed. Recipients can decrypt the message only if they have the secret key. Access point with IP router role could be used for decryption. Encrypted packet could be modified during transmission by a new Internet address of the attacker's locations. The access point would then decrypt the packet and send it to the new destination where it could be read by the attacker.

5. Safety Improvements of WEP

Safety improvements of WEP protocol are based on the improvements of the mechanisms for preservation of WEP security goals. It has been noticed that it is not RC4 encryption algorithm causing WEP protocol deficiencies, but the repetition of the encryption keystream. The first solution used to overcome this problem was RSA patch for WEP that enabled each package to have a different key. The new improvement appeared as Wi-Fi Protected Access (WPA), a temporary solution that did not require any upgrades or hardware replacements. In order to improve data confidentiality and integrity, WPA2 applies a new encryption algorithm, AES (Advanced Encryption Standard). Introduction of the new algorithm requires new equipment and creates incompatibility with the existing wireless equipment. WPA2 introduces safe "mixed mode" that supports WPA and WEP workstations. IEEE group designs a safety authentication mechanism via 802.1x network port, known as Robust Security Network Association (RSNA) in order to improve the authentication mechanism in wireless networks. Introduction of IEEE 802.1x and specification defines two kinds of safety algorithms: RSNA and pre-RSNA. Pre-RSNA is the connection with the old WEP protocol and the old way of authentication. The development process of WEP safety improvements is shown in Figure 2.

RSNA provides two protocols for data confidentiality, TKIP (Temporal Key Integrity Protocol) and AES-CCMP (Counter-mode/CBC-MAC Protocol). TKIP protocol provides compatibility with WPA and WPA2, while AES-CCMP protocol provides higher confidentiality and compatibility with WEP2 mechanism. RSNA also provides improved 802.1x authentication and protocol for key management.

Improvements are adjusted to the existing network equipment without any significant performance malfunctions. The new 802.11i standard introduces a new mechanism for message encryption, integrity check and authentication.

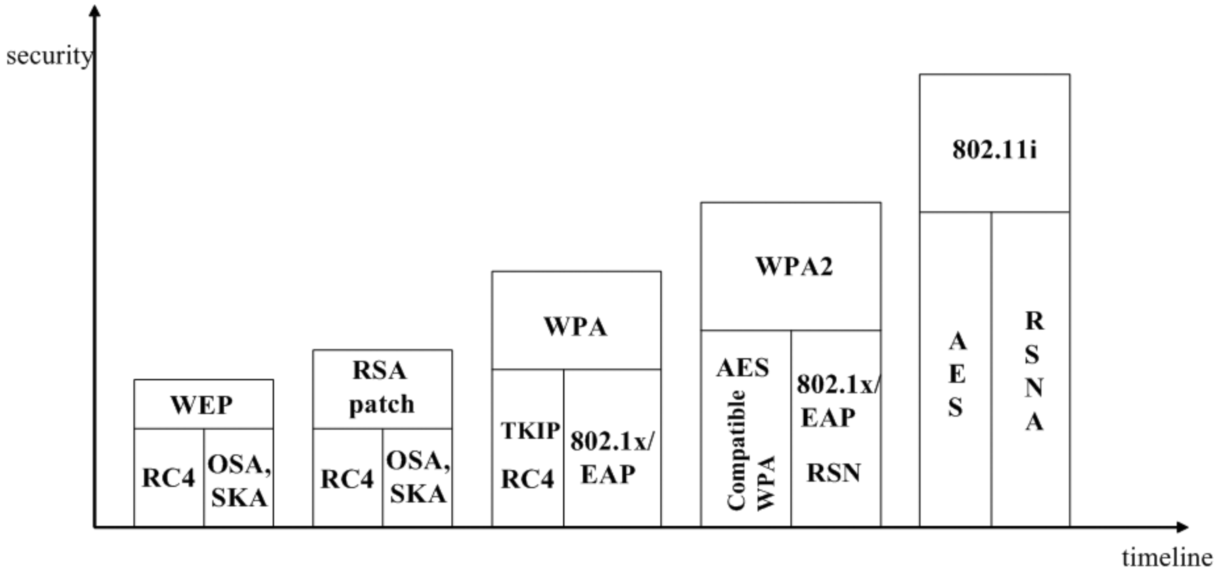

Figure 2. WEP protocol safety improvements.

5.1. RSA Patch for WEP

RSA Security and Hifn have discovered a new way of fast generation of keys unique for each of RC4 algorithm packets. The new solution is named Fast Packet Keying and it uses hash technique of fast generation of a unique keystream for each packet. The solution is based on the following rules [13]:

— A 128 bit RC4 key named temporal key (TK) is used for encryption and decryption,

— A keystream generated by RC4 algorithm is used for encryption and decryption, and

— Initial vector value cannot be used more than once.

RSA uses a special hash function applied in two phases. In the first phase, transmitter address (TA) is injected into the temporal key providing thus a different key for each packet. This means that in the process of data transmission from workstations to access point, a set of keys different from the set of keys used during data transmission from the access point to the workstation will be used. In the second phase, there is a combination of the first phase output with IV, generating thus a unique keystream for each of the packets.

In comparison to WEP protocol, Fast Packet Key solution seems to be more complex since it takes more time for key generation. But the first phase output can be cashed once the second phase has ended. First phase cash and generated 16 bits IV will generate key for the next packets.

Many manufacturers of wireless networks have accepted this patch for their products in order to raise the level of safety. There are four key elements for which this patch is significant in the wireless equipment market:

— Low price,

— Easy implementation for both new and old products,

— Possibility of distribution via e-mail, and

— Increased safety.

5.2. Wi-Fi Protection

IEEE studied all details of WEP security problems and focused on the design of new safety mechanisms for wireless networks. The solutions are offered in 802.11i standard. However, standard issuance and ratification can take a few years and the market makes a pressure on manufacturers so that they are not in a position to wait for standard issuance and ratification to be finished. In order to solve this problem, Wi-Fi defines WPA (Wi-Fi Protected Access) standard to improve the protection of wireless devices. WPA has contributed to the increased protection of wireless communications through the increased level of data protection and access control of current and future solutions to wireless networks. WPA is designed to be the software upgrade to the existing devices and is compatible with the new IEEE 802.11i standard. WPA has several purposes:

- To be a strong protective mechanism for wireless networks,
- To be interoperable,
- To replace WEP,
- To enable the existing Wi-Fi wireless devices to be upgraded with the new software solution,
- To be applicable in small, as well as in large wireless networks, and
- To be applicable immediately.

The first improvement [14] offered by WPA is data encryption by TKIP (Temporal Key Integrity Protocol). This protocol provides a strong encryption mechanism whose characteristics are:

- A unique stream for encryption of each of the packets,
- Message integrity check (MIC, Michael),
- IV extension, and
- Repeated key mechanism.

The second improvement is related to the strong security authentication of the users through 802.1x and EAP (Extensible Authentication Protocol).

In large networks, WPA uses authentication server RADIUS to secure centralized management and control of the access. In small SOHO (Small Office/Home Office) networks, there is no centralized authentication server so that WPA is initiated by a special mode. This mode is also called Pre-Shared Key (PSK) and it enables users to authenticate by a password or a key. Users have to enter a password (or a key) to the access point, otherwise home network reaches each of the workstations included in the Wi-Fi wireless network. Devices with appropriate password can be networked and thus protected from eavesdropping and other unauthorized users.

5.3. TKIP

TKIP is a collection of algorithms created to improve and solve security problems of WEP. Majority of cryptographic functions is realized through hardware in wireless networks adapters, thus it is not possible to improve the hardware. RC4 is an encryption device implemented in hardware of wireless network adapters and is not replaceable. To solve this problem TKIP uses RC4 device in the way that changes the methods of use of the shared key. In WEP, shared key is used directly in encryption, while in TKIP it is used for generation of other keys. TKIP algorithms can be applied in the current wireless equipment without significantly ruining the performance.

TKIP gives WEP four new improvements [15]:

- Encrypted message integrity code to prevent message falsifications,
- Strict IV sequences to prevent replay attacks,
- Key generation, and
- Mechanism to refresh keys in order to prevent attacks related to key repetition.

Encrypted message integrity code (MIC). MIC is an encryption mechanism based on hash function design to work on existing wireless network adapters in order to detect false messages. MIC mechanism consists of three components:

- authentication key (Michael key, both the sender and the receiver have the same key),
- tag function, and
- verification.

Tag function generates the tag based on the authentication key and message. Generated tag is an encryption for integrity check and is sent together with a message. Receiver performs verification and if the result is TRUE, that means that the message is original, if the result is not TRUE, that means that the message is false. MCI strength is in the number of tag bits (n). This means that if the attacker wants to send a false message, 2^n messages have to be sent [16].

MIC has a level of protection of $n = 20$, while the strongest attacks could generate 2^{29} messages. It is obvious that MIC with the above given level of protection is not completely safe. Therefore, TKIP implements mechanisms for detection of false messages and in case there are two false messages in a second, it is considered to be an attack. In that situation keys must be erased, session must be terminated and one minute has to pass before the new session with the new TKIP and Michael keys is established.

Strict IV sequences. False messages appear when the attacker meets the message and sends it as his own. Usually, this problem is solved by linking IV counter with the MIC key. Each time the MIC key is replaced, IV sequence is reinitialized. This strategy requires the transmitter to stop its transmission when the same IV sequence repeats for one MIC key. This happens when communications ceases or MIC key changes. TKIP affects IV sequence. Transmitter and receiver set IV to zero each time TKIP key is changed. Sender increments IV sequence for each packet that is sent. TKIP requires receiver to supervise all sequences of the IV sequence that has just arrived. If the newly arrived IV sequence is smaller or even the same as the previous IV sequence for the same TKIP key, or if IV sequences arrive in no logical order, then it is a reason to dismiss these messages.

Key generation. In WEP protocol a unique key for each packet is based on concatenation of unchanged key and IV sequence. As a result of this key generation there is his often repetition. For each of the packets a new key is generated by hash function based on TKIP key and IV sequence. It is called temporal key since its duration is temporal and it changes when its time elapses.

Key generation in TKIP protocol has two phases (Figure 3):

— In phase 1, hash function is calculated based on the MAC address of the sender, temporal session key and high 32 bits of IV. This phase is calculated only if temporal key of the session is changed.

— In phase 2, hash function is calculated by the phase 1 output and low 16 bits of IV. As an output, we have a key stream of 128 bits. In fact, the first 3 bits of phase 2 are compatible with IV in WEP, while the remaining 13 bits are compatible with WEP. The purpose of phase 2 is to make it difficult for the attacker to find correlation between IV and a key for each of the packets.

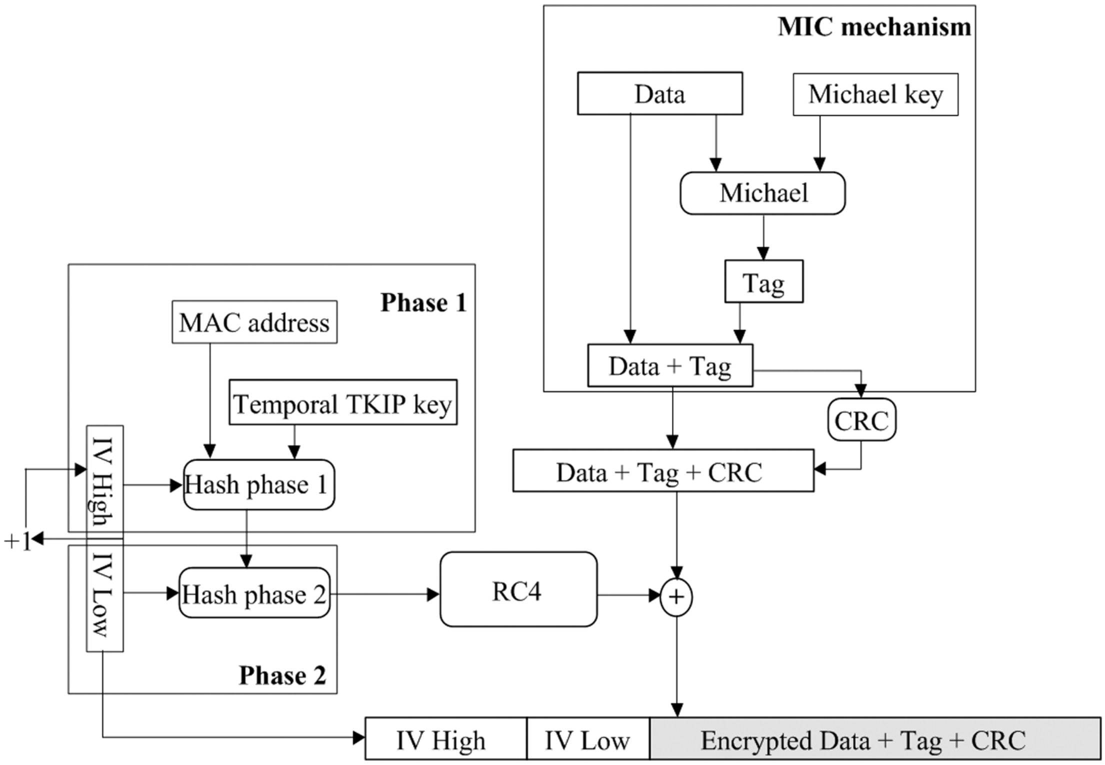

Figure 3. WEP protocol safety improvements.

The analysis of C code that implements both phases shows that some of the cryptographic characteristics of S-box have been applied [17].

Refresh key mechanism. TKIP mechanism has three keys:
— Temporal key,
— Encryption key, and
— Master key.

Temporal keys. Temporal keys are 128 bit encryption key and 64 bit key for encryption of data integrity. TKIP uses separate key sets on both sides of connection, so that there are four temporal keys in total. TKIP identifies these sets of keys by 2 bit identification device named WEP keyid. When first connection is established, the first set of keys is immediately connected to one of the two sets of WEP keyid. When a new set of keys is created, a new keyid is distributed to it. After the connection between a new pair of temporal keys is established TKIP implementation will continue to receive packets on the old keyid and its keys. However, later on, the transfer will be conducted only via new keyid and its keys. New temporal keys are created with the first or repeated establishment of connection.

Encryption key. Encryption key protects temporal keys. There are two of these keys – one is used to encrypt the message to introduce temporal keys, while the other serves to protect the message from being falsified.

Master key. Master key is exchanged among workstations and 802.1x authentication servers. This key is directly related to authentication and is used for secure distribution of key streams. Master key is created after a successful authentication and is related to one session only.

5.4. 802.1x

IEEE 802.1x [18] is standardized way to the network secure access. By using security methods in 802.1x standard it is possible to access the network securely, even when products of different manufacturers are in use. 802.1x is only a part of security technology that disables unauthorized access to the network and does not control traffic of the authorized users. 802.1x does not require a specific authentication protocol, but uses EAP for encapsulation of other authentication protocols (LEAP – Lightweight Authentication Extension Protocol; EAP-TSL – Transport Layer Security; EAP-TTLS – Tunneled TLS; EAP-PEAP – Protected EAP). A successful authentication [19], both of a client and authenticator, has to be completed before any traffic from the client is allowed. Before authentication 802.1x logical component (PAE – Port Access Entry) prohibits any traffic except for the EAP request that is being forwarded to the authentication server. Based on the EAP message, authentication server determines whether a client has or does not have an access to the network. Then it sends a message to the authenticator and, based on the message, the port is either in the position to prohibit or approve the traffic.

Previous researches have showed that primary authentication method [20] (open authentication system and shared key authentication) and access control based on MAC control lists are not secure mechanisms. In order to solve the problem, IEEE group designed new security architecture for wireless local networks – Robust Security Network (RSN). RSN provides a mechanism for connecting to the network only through an authorized 802.1x network port. Network port represents a connection between the station and AP. RSN uses three entities defined by 802.1x standard: station, authenticator and authentication server. The station is an entity that wants to access the network through authenticator's network port (access point). The station is authenticated through authenticator on authentication server from which it receives accreditations.

RSN connection is performed in three phases [21, 22, 23]:

Phase 1: Request, authentication and association. The station looks for the AP with appropriate SSID. All APs in the range answer with the Probe Request framework, as shown in Figure 4. When the station identifies with which AP it is connected and accepts its parameters, authentication is performed as well as connection to the AP. At the end of phase 1 the workstation and the AP establish security rules and 802.1x authentication port is locked. 802.1x network port remains locked as long as the authentication procedure has been completed.

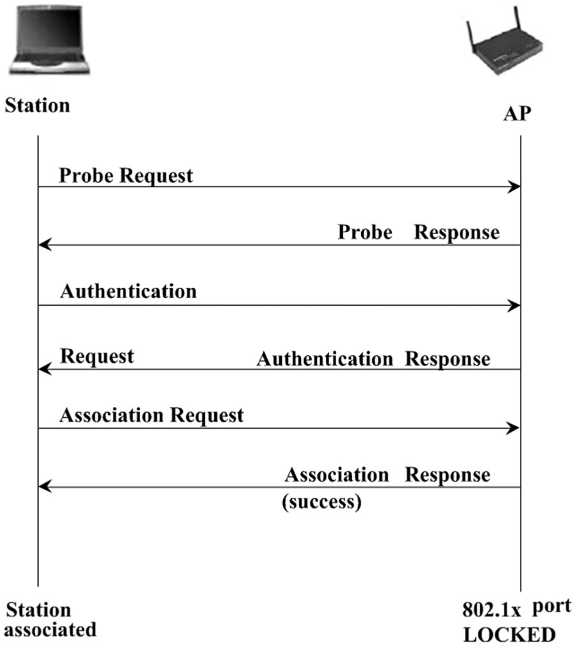

Figure 4. Request, authentication and association.

Phase 2: 802.1x authentication. In this phase the station is authenticated with the authentication server. The station and the AP have to authenticate mutually in order for the station to escape false access points and for the access points to escape false stations. 802.1x standard uses EAP for different authentication mechanisms. In communications between the station and the authenticator, EAP protocol uses four messages: EAP Request, EAP Response, EAP Success and EAP Failure. EAP can route messages to the authentication server (such as RADIUS) through 802.1x port when it is locked. EAP packets between the station and the authenticator encapsulated EAPOL (EAP over LAN) packets, while EAP messages between authenticator and authentication server are encapsulated in RADIUS packets. The station sends EAPOL start message to the authenticator. Based on this message, the authenticator requires station identification. The station then replies with identity parameters that are forwarded to the authentication server by authenticator. Then the mutual authentication between the station and authentication server is done as shown in Figure 5. If the mutual authentication is successful, the authentication server generates Master Session key (MSK) and forwards it to the authenticator and to the station. PMK (Pair-Wise Master Key) is then generated by the station and authenticator based on the MSK.

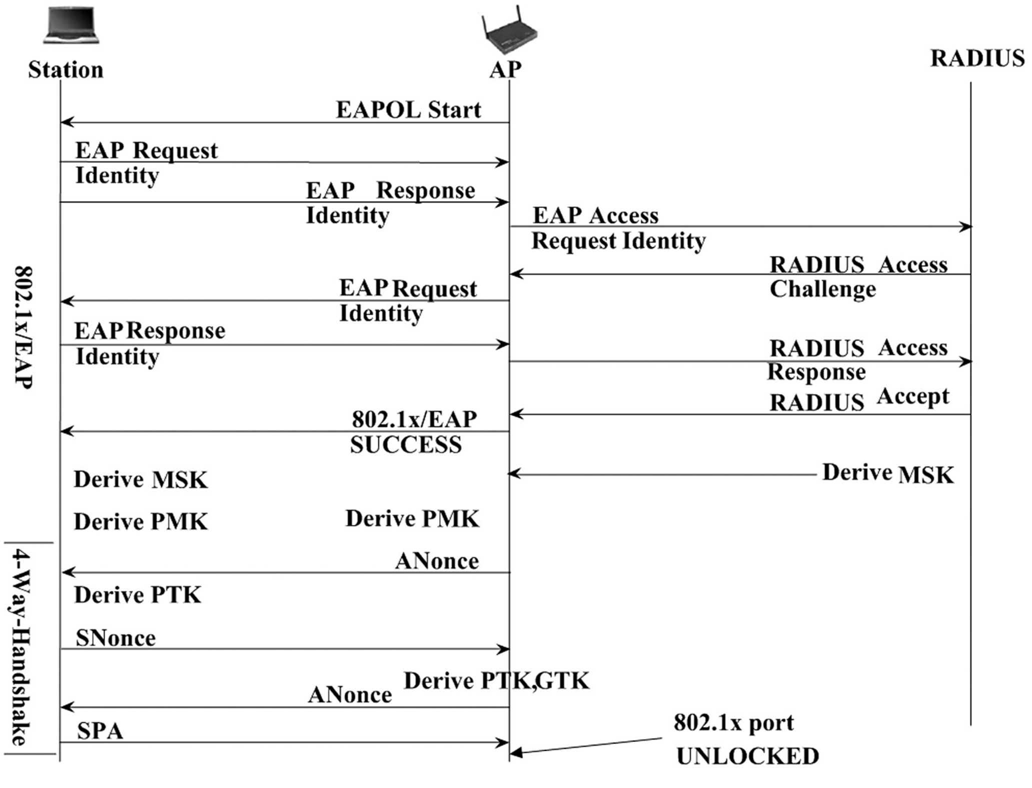

Figure 5. 802.1x/EAP and 4-way handshake.

Phase 3: 4-Way Handshake. The station and the authenticator have to mutually confirm the current PMK in order to complete successfully RSNA (as shown in Figure 5). After successful confirmation a PTK (Pair – Wise Transient Key) is generated to be used for a secure transfer of session data. Now 802.1x port is unlocked.

802.1x authentication has several advantages:

- — Administrators can define users' responsibilities in the network, they do not have to pair manually users' names with MAC addresses, and can easily find mistakes and supervise the network,
- — Administrators allow access to the network according to the manufacturer standards,
- — An authorized port cannot be compromised by a non-802.1x client,
- — The authenticator waits for a certain period of time for a client to re-authenticate before the port is locked,
- — A continuity of authentication procedure is allowed in case the client was temporarily unable to respond to authenticator's request,
- — It is allowed for more devices to access the network by a shared mediator (such as hub), and
- — Protection is imposed to all users of the access point.
- — In addition to the advantages mentioned before, 802.1x authentication has also some deficiencies. These deficiencies result from the mistakes in 802.1x and EAP protocols [24, 25] that the attackers have used for attacks.

5.5. WPA, WPA2 and 802.11i

IEEE 802.11i [16], an IEEE standard ratified on June 24, 2004, is an addition to IEEE 802.11 standard that deals with the protection of small and large wireless networks. IEEE 802.11i is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. WPA2 is a product of Wi-Fi alliance that guarantees that all the equipment with WPA2 installed can support the most important characteristics of 802.11i. Wi-Fi alliance enables AP usage supported only by WPA2 mode and AP supported by mixed WPA2/WPA mode. This means that WPA2 equipment is compatible with WPA. Due to WEP security problems WPA2/WPA mode is not allowed in WPA2 equipment.

WPA and WPA2/802.11i specify new standards for authentication, encryption and message integrity.

Authentication. WPA and WPA2/802.11i use 802.1x/EAP for authentication and key exchange. 802.1x authentication model requires the existence of 802.1x client, authenticator (access point) and authentication server (RADIUS). WPA and WPA2 use 802.1x for the authentication in large networks, while a shared key authentication is used in small networks. 802.11i introduces pre-authentication [26] in order to escape re-authentication and reduce all late arrivals caused by 802.1x. Reduced lateness of 802.1x would enable faster roaming between wireless station and APs. This is very important for the application sensitive to lateness.

Key Management. The process of management and creation of the key is the same for the TKIP and AES-CCMP (Advanced Encryption Standard – Counter Mode with Cipher Block Chaining message Authentication Code Protocol). Both TKIP and AES-CCMP are defined by 802.11i standard, but there is a difference in the number of keys. AES-CCMP uses the same number of keys for message encryption and data integrity while TKIP uses two keys. This difference is the result of the fact that TKIP is based on RC4 encryption technique while AES-CCMP uses advanced encryption standard.

WPA and 802.11i encryption and integrity. TKIP and AES-CCMP solution are introduced to improve bad WEP encryption mechanisms. Wi-Fi alliance integrated TKIP into WPA in order to use it on the WLAN hardware. TKIP protocol contains RC4, but introduces changes in the area of message integrity, IV creation and key management, all that with the purpose of increasing WEP safety.

AES-CCMP [27] is the core of 802.11i standard and is mandatory in 802.11i standard while TKIP is supported by 802.11i standard. Future WLAN equipment will use AES-CCMP for encryption and message integrity. AES algorithm [28] uses encrypted key of 128, 192 and 256 bits for encryption and decryption of data in blocks of 128 bits. 802.11i standard requires the use of 128 bit AES-encrypted key. It means that a message that cannot be divided into 128 bits has

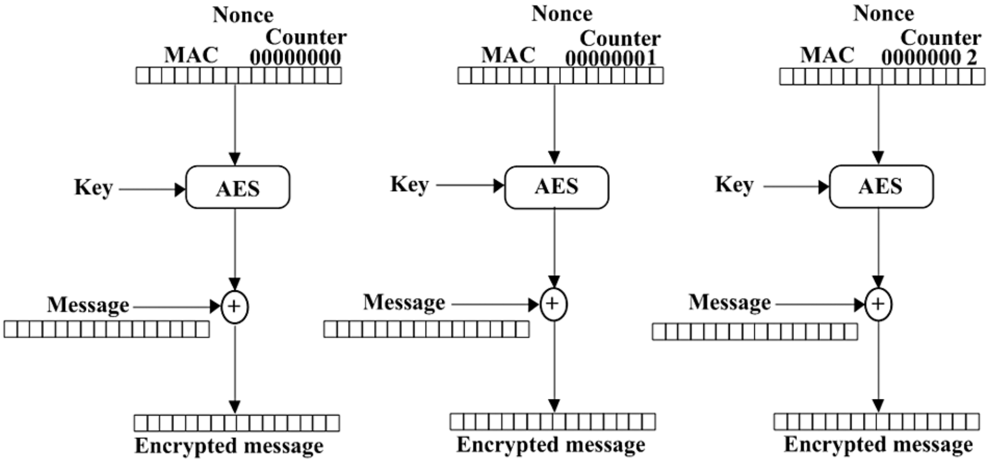

Figure 6. AES encryption by counter.

to be converted in 128 bits blocks before encryption. This is done by CCMP by adding random data in blocks to become 128 bit blocks. When decryption is completed, CCMP removes added data that are not a part of the original message.

CCMP in AES-CCMP is a combination of two AES counter mode encryption and CBC-MAC (Cipher Block Chaining – Message Authentication Code protocol) techniques [29].

The first technique adds nonce and counter on AES temporal key and encrypts a message by XOR. Nonce is MAC address of the sender and frame ordinal number. MAC address is used in order to use the same increment in different communications directions, thus providing different encryption streams. Packet ordinal number has a purpose to detect for the receiver injection of old packets. Receiver remembers the ordinal number of the last packet and accepts all packets with bigger ordinal number. A counter is changed for each of data encrypted blocks, as shown in Figure 6. An attacker can find out a starting value of the counter, but cannot know which block applies to which increment.

For message security it is not enough only to encrypt the message, but to preserve the integrity, too. CBC-MAC mechanism guarantees that the message will not be modified during the transmission between two devices. CBC-MAC is based on CBC algorithm of encryption. This algorithm operates in a way that it calculates XOR between unencrypted and previously encrypted blocks, then it is encrypted by AES key and XOR for that block is calculated by next unencrypted block, as it is shown in Figure 6. The procedure is repeated until the final 128 bit CBC-MAC block is generated. It is obvious that CBC-MAC block value depends on the value of all previous blocks and since all these blocks are encrypted, it is also obvious that CBC-MAC depends on the key. If a receiver finds some irregularities with a CBC-MAC, it means that there was message modification (message integrity is ruined) or that the message was encrypted with a different key.

Figure 7 shows the procedure of calculating CBC-MAC.

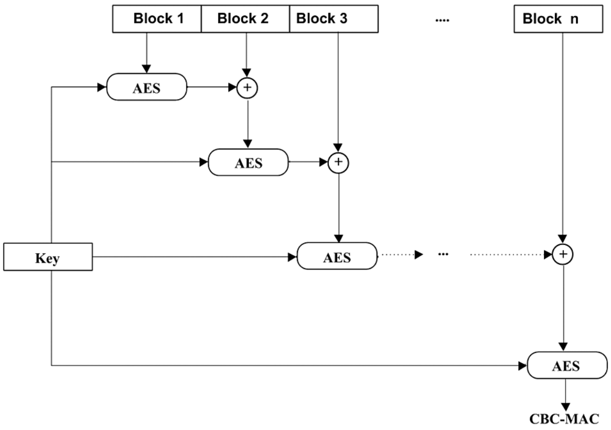

Figure 7. CBC-MAC calculation.

This section describes differences between WPA and WPA2/802.11i safety improvements. Table 1 gives a comparison of these safety improvements in comparison to WEP as a first solution to achieve safety goals in WLAN networks. Table also shows availability of safety solutions in improvements of all three safety goals.

	WEP	WPA	WPA2/ 802.11i
Authentication	Open authentication system and shared key authentication (same key as for encryption) – Pre-RSN	Shared key authentication and strong authentication based on 802.1x and EAP (RADIUS server)	Authentication based on 802.1x and EAP (RADIUS server) and pre-authentication, RSNA
Encryption	Thoroughly researched and documented defficiencies	Removes all WEP deficiencies	Removes WEP and WPA deficiencies
	40 bit key	128 bit key	128, 192, 256 bit keys
	Statical key distribution – all network users use the same key	Dynamic key distribution – new keys for each user, session, packet	
	Manual key distribution – it is necessary to enter the key into each device	Dynamic key distribution	
	Uses IV		Does not use IV
	RC4 algorithm encryption		AES algorithm encryption
Integrity	CRC	MIC (64 bit key)	CBC-MAC (the same key as for encryption)

Table 1. Comparative analysis of WLAN safety improvements.

6. RC4 and AES Cryptographic Algorithms

RC4 and AES cryptographic algorithms belong to the group of symmetrical encrypting algorithms. Symmetrical encrypting algorithms are algorithms that use the identical keys both for the processes of encryption and decryption. These algorithms are completely public, meaning that their safety is not based on the algorithm secrecy but on the secrecy of the key. The model of symmetric encryption system consists of five elements: plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm. The encryption process takes place at the sender's by having encryption algorithm transform plaintext by K key into a non-comprehensible message. The process of decryption is the opposite: at the receiver's, the ciphertext is translated into a comprehensible message by decryption algorithm and the key.

Symmetric cipher algorithms are divided into two categories:

Stream cipher. The main characteristic of the stream cipher is that the keystream is generated from the initial value (secret key) and previously agreed algorithm. This cipher system accepts, at the start, a range of elements (bits or bytes) of the plaintext that has been encrypted immediately. In these systems, the key represents the input value into the pseudorandom number generator that generates keystream. Then, XOR function between each plaintext and keystream bytes is calculated thus providing ciphertext.

One of the deficiencies of this cipher system is caused by the use of pseudorandom stream. Algorithm for generation of pseudorandom stream is determined, meaning that, statistically, it is not random. Thus, the same keystream will appear after some time. In order to improve the design of sequential stream cipher, it is necessary to consider the design issues of the stream cipher given in [30].

Block cipher systems. Block cipher systems process plaintext blocks of fixed length and generate ciphertext in blocks of the same length, usually of 64 bits. Ciphertext is generated from the plaintext by repeating the function F after few rounds. The F function depends on the previous round output and K key. This function is also called round function as it has been applied in each round.

These cipher systems use different cryptographic modes as a technique for improvement of cryptographic algorithm efficiency. A recommendation for block cryptographic modes [31] specifies five cryptographic modes for symmetrical block cipher systems: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) mode. One of the algorithms using cryptographic modes is AES with specification defined in FIPS Pub. 197 [32].

RC4 and AES belong to different groups of symmetrical cipher systems. RC4 belongs to the group of stream symmetrical cipher systems, while AES belong to the group of block symmetrical cipher systems.

6.1. RC4

RC4 is the best known of all sequential cipher systems. It was designed by Ron Rivest for RSA Security in 1987. It uses key of variable value and it is oriented on work with the bytes. This cipher system works very fast due to very small number of necessary operations. Thus, to obtain one output data (encrypted byte), 8 to 16 mechanical operations are needed.

RC4 algorithm is very simple and easy to implement. The key of variable length of 1 to 256 bytes is used for initializing 256 bytes S array. S array contains permutation of all 8-bits numbers from 0 to 255. Encryption and decryption stream, K, is generated from the S array by choosing one of 255 unique stream conditions.

RC4 algorithm execution phases:

Initialization of S array. S array is initialized by values of 0 to 255 in ascending hierarchy, i.e. S[0] = 0, S[1] = 1, ..., S[255] = 255. At the same time, a temporary array, T, is created. T array fields are filled in by K key value depending on the initialization point and key length. If a key length is keylen bytes, then the value of the i-field of the temporary T stream is equal to the K key value on i-filed in the key. The initialization is shown by the following lines of codes:

```
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

Initial permutation of S array. T array is used for initial permutation of the S array by changing the S[i] value with S[j] value, whereas j is calculated by T array as shown in the following lines of codes:

```
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

Cipher Stream Generation. Cipher stream goes through all the elements of S. Value of each of the stream elements, S[i], is replaced by the value of the element S[j], whereas j is calculated by S[i]. After replacement of the S[i] and S[j], t index is calculated, indicating the S stream element whose value will be taken for cipher stream. The scheme of generation of cipher stream is shown by the following code:

```
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
```

6.2. AES

In order to replace the “run out” DES, NIST (National Institute of Standards and Technology) has organized cryptographic competition for a new cryptographic algorithm, according to the requirements defined in [33], to be used by government institutions. There were 15 proposals and 5 of them were selected as best according to the given requirements. In October 2000 NIST chose Rijndael designed by two Belgian researchers: Joan Daemen and Vincent Rijmen. Rijndael was much faster in comparison to its competitors (MARS, RC6, Serpent, Twofish) and required less memory in the process of encryption and decryption. NIST publicly released AES in 2001.

This algorithm belongs to the group of block cipher algorithms. It supports keys and blocks of 128 to 256 bits in sequences of 32 bits. The length of the key and the length of the block could be chosen independently. AES requires blocks of 128 bits and keys of 128, 192 and 256 bits. This actually means that there are two types of AES, one of 128 bits block with 128 bits key, and another one of 128 bits block with 256 bits key.

But before we start with the encryption and decryption process, it is necessary to review in what way the input data and the key are presented.

The plaintext is divided into 128 bit blocks that are the starting point for encryption and decryption algorithm. These blocks appear in the form of square matrix of bytes [28]. The starting block of the plaintext is put into the two dimensional array of 4x4 bytes (state array) whose value is changed after each completed algorithm phase. After the final stage, state array is copied to an output matrix.

The key of 128 bits is described in the same way as starting blocks, with the square matrix of bytes. Then the key is enlarged into the stream of 44 32 bit words whereas each of the words is equal to 4 bytes. Four words make the round key. It is obvious that there are 11 keys, but the work is conducted with 10 rounds. The first key is used for initialization of encryption, while the last key is used for initialization of decryption. The rest of the keys is used in encryption and decryption rounds.

When 192 bit or 256 bit key is used in the AES algorithm, 12 or 14 rounds take place and the key is enlarged to 52 or 60 words accordingly.

The starting matrix of the data block for encryption and decryption is filled in columns, meaning that the first four bytes of 128 bit block occupy the first column of the matrix, the second four bytes occupy the second column, and so on. The same principle applies with the enlarged key, meaning that the first four bytes make a word that occupies the first column of the key matrix.

The processes of encryption and decryption of AES algorithm take place in a certain number of rounds, whereas each of the rounds consists of one permutation and three substitutions:

Substitution of bytes. AES defines matrix of 16x16 bytes containing permutation of all possible 256 8 bit values. This matrix is called S-box. Each of the bytes of the original matrix is mapped into the new byte in the following way: the 4 most important bit bytes are order index of S-box, while 4 less important bit bytes are column index of S-box. According to the two mentioned indexes, the value of the matrix field is replaced by the respective value from the S-box. Inverse substitution is conducted in the same way by using inverse S-box. S-box is designed in a way that is resistant to the crypto-analytical attacks.

ShiftRows Permutation. This permutation is conducted according to the rows of the original matrix. The first row of the original matrix remains the same. There is 1-byte circular left shift in the second row. In the third row, there is 2-byte left shift, while in the fourth row, there is 3-byte left shift. This permutation is shown in the Figure 8.

MixColumn Substitution. This substitution is conducted for each column. Each of the column bytes is mapped into a new value used for all four column bytes. This transformation is shown in Figure 9. Each of the elements in substitute matrix is the product of the element of one of the rows of the transformation matrix and one of the columns of the original matrix.

Coefficients of transformation matrix are linear with maximum distance between bytes of each of the columns. Column substitution combined with the row permutation enables that, after few

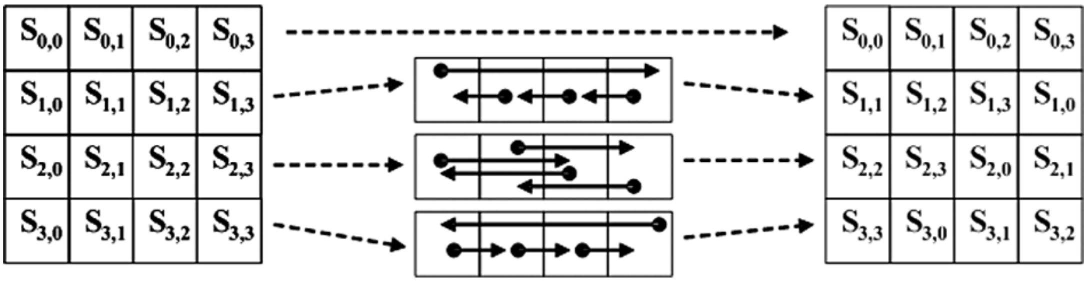
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,1}$ $S_{1,2}$ $S_{1,3}$ $S_{1,0}$
$S_{2,2}$ $S_{2,3}$ $S_{2,0}$ $S_{2,1}$
$S_{3,3}$ $S_{3,0}$ $S_{3,1}$ $S_{3,2}$

Figure 8. ShiftRows permutation.

$$(2*S_{0,0}) \oplus (3*S_{1,0}) \oplus S_{2,0} \oplus S_{3,0}$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}$$

Figure 9. MixColumn substitution.

rounds, the value of the original matrix depends on all input bits at the very beginning [34].

Output value is obtained by multiplication (*) and XOR operation (circled plus symbol). Multiplication of the x value (in this case value 02, i.e. 02*y) is calculated in the following way:

— if the most important bit y is equal to 0, then 1-bit left shifting is conducted. 0 is put in the place of the last bit,

— if the most important bit y is equal to 1, then 1-bit left shifting is conducted. 0 is put in the place of the last bit. The new value is now added to (0001 1011) by XOR operation.

Inverse MixColumn substitution is conducted in the same way by using inverse matrix.

AddRoundKey Substitution. In this type of substitution, the XOR function is applied between the results of previous transformations and 128 bit round key. The transformation is conducted in a way that each of the original matrix fields XORs with the suitable extended key field (the fields of the same index of the original matrix and extended key are summed up exclusively). Inverse transformation is identical as XOR function is inverse in itself. This substitution affects every bit of the original matrix.

The safety of the AES algorithm is secured due to complexity of the key extension (each round key) and the complexity of the above mentioned transformations.

7. Conclusion

WEP is the first protocol for data protection in wireless networks. This mechanism is designed to achieve three safety goals: authentication, confidentiality and message integrity. This mechanism is based on RC4 algorithm (an algorithm that can be trusted) but, still, WEP does not achieve safety goals completely. Basic WEP deficiencies come from unsafe authentication, repeated use and open transfer of IV, key management system and a mechanism for the protection of message integrity that is not applied properly. All these deficiencies can lead to many threats to WEP safety goals.

WPA contributes to the increase of wireless communication protection by Wi-Fi standard through increased level of data protection, access control and integrity. WPA standard is defined by software upgrade of current devices and is completely compatible with a new IEEE 802.11i standard. WPA introduces TKIP group of algorithms created to improve safety mechanisms of WEP and provide strong and safe authentication by 802.1x/EAP standard. 802.11i introduces a new authentications standard, encryption and message integrity. 802.11i defines Robust Security Network Association (RSNA) procedure to provide mutually strong authentication and key management procedure. AES counter encryption contributes significantly to the increase of data protection during communication transmission, while CBC-MAC contributes to integrity preservation by mixing encrypted and non-encrypted data blocks.

802.11i standard provides a high level of protection from the attacks, but cannot solve all the problems caused by some DoS attacks. One of these attacks is jamming, whereas an attacker can disable communications among wireless networks users by using some devices.

References

[1] J. WELCH, S. D. LATHROP, A Survey of 802.11a Wireless Security Threats and Security Mechanisms. *United States Military Academy West Point*, New York, (2003).
`http://www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf`

[2] B. FLECK, J. DIMOV, Wireless access points and ARP poisoning: wireless vulnerabilities that expose the wired network. *White paper by Cigital Inc.*, (2001).
`http://www.cigitallabs.com/resources/papers/download/arppoison.pdf`

[3] I. MARTINOVIC, F. A. ZDARSKY, A. BACHOREK, C. JUNG, J. B. SCHMITT, Phishing in the Wireless: Implementation and Analysis. *Kaiserslauterer Uniweiter Elektronischer Dokumentenserver, Universitatsbibliothek Kaiserslautern*, (2006).
`http://kluedo.ub.uni-kl.de/volltexte/2006/2035/pdf/martinovic.pdf`

[4] G. RUPINDE, S. JASON, C. ANDREW, Specification-Based Intrusion Detection in WLANs. *22nd Annual Computer Security Applications Conference*, Miami Beach, Florida, (2006).

[5] AUSCERTAA-2004.02, Denial of Service Vulnerability in IEEE 802.11 wireless devices. (2004).
`http://www.auscert.org.au/render.html?it=4091`

[6] C. WULLEMS, K. THAM, J. SMITH, M. LOOI, A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANS. *IEEE Press*, (2004), pp. 129–136.

[7] F. RANGO, D. C. LENTINI, S. MARANO, Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack inWi-Fi Protected Access and IEEE 802.11i. *EURASIP Journal on Wireless Communications and Networking*, Hindawi Publishing Corporation, pp. 1–19, (2006).

[8] R. PRODANOVIC, D. SIMIC, Holistic Approach to WEP Protocol in Securing Wireless Network Infrastructure. *Com SIS*, Vol. 3, No. 2, pp. 97–113, (2006).

[9] White paper: Testing for Wi-Fi Protected Access (WPA) in WLAN Access Points. Net-O2 Technologies, (2004).
`http://whitepapers.zdnet.co.uk/0,39025942,60152756p,00.htm`

[10] N. BORISOV, I. GOLDBERG, D. WAGNER, Intercepting Mobile Communications: The Insecurity of 802.11. DRAFT. (2002).
`http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf`

[11] J. R. WALKER, Unsafe at any key size; An analysis of the WEP encapsulation. *IEEE Document 802.11-00/362./*, (2000).

[12] N. BORISOV, I. GOLDBERG, D. WAGNER, Intercepting mobile communications: the insecurity of 802.11. *In Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, Rome, Italy, (2001).

[13] WEP Fix using RC4 Fast Packet Keying. RSA Laboratories, (2002).
`http://www.comms.scitech.susx.ac.uk/fft/crypto/wep.pdf`

[14] Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, (2003).
`http://www.wi-fi.org/opensection/pdf/whitepaper_wi-fi_security4-29-03.pdf`

[15] J. R. WALKER, 802.11 Security Series (Part II: The Temporal Key Integrity Protocol (TKIP)). *Intel Corporation.*
`http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf`

[16] IEEE P802.11i/D10.0. *Medium Access Control (MAC) Security Enhancements*, Amendment 6 to IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, (2004).

[17] W. HAN, D. ZHENG, K. CHEN, Some Remarks on the TKIP Key Mixing Function of IEEE 802.11i. *Cryptology ePrint Archive*, (2006).
`http://eprint.iacr.org/2006/129.pdf`

[18] L. BLUNK, J. VOLLBRECHT, B. ABOBA, J. CARLSON, H. LEVKOWETZ, Extensible Authentication Protocol (EAP). *Internet Draft draft-ietf-eap-rfc2284bis-06.txt*, (2003).

[19] J. ANTHON, Using IEEE 802.1x to Enhance Network Security. *FoundryNetworks*, (2002).
`http://www.foundrynet.com/solutions/appNotes/PDFs/802.1xWhite_Paper.pdf`

[20] M. ARUNESH, A. W. ARBAUGH, An Initial Analysis of the IEEE 802.1X Standard. Maryland, (2002).
`http://www.cs.umd.edu/~waa/1x.pdf`

[21] T. KARYGIANNIS, L. OWENS, Wireless Network Security 802.11. *Bluetooth and Handheld Devices*, NIST, (2002).
`http://csrc.nist.gov/publications/nistpubs/800-48/nist_sp_800-48.pdf`

[22] J. C. CHEN, M. C. JIANG, Y. W. LIU, Wireless LAN security and IEEE 802.11i. *IEEE Wireless Communications*, (2005), vol. 12, no. 1, pp. 27–36.

[23] C. HE, J. C. MITCHELL, Security Analysis and Improvements for IEEE 802.11i. Stanford, USA, (2004).
`http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf`

[24] G. RUPINDE, S. JASON, C. ANDREW, Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks. *Proceedings of the 2006 Australasian workshops on Grid computing and e-research*, Vol. 54, pp. 221–230, (2006).

[25] L. HAN, A Threat Analysis of The Extensible Authentication Protocol. *Honours Project*, School of Computer Science, Carleton University, (2006). http://www.scs.carleton.ca/ barbeau/ Honours/Lei_Han.pdf

[26] L. PHIFER, 802.11i: Robust and ready to go. (2004). http://searchmobilecomputing.techtarget.com/tip/1,289483,sid40_gci992741,00.html

[27] E. PEREZ, 802.11i (How we got here and where are we headed). Orlando, (2004). http://www.giac.org/practical/GSEC/Elio_Perez_GSEC.pdf

[28] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FIPS Pub197: Advanced Encryption Standard (AES), (2001).

[29] D. WHITING, R. HOUSLEY, N. FERGUSON, Counter with CBC-MAC (CCM). RFC 3610, (2003).

[30] I. KUMAR, Cryptology. *Laguna Hills*, CA: Aegean Park Press, (1997).

[31] M. DWORKIN, Recommendation for Block Cipher Modes of Operation – Methods and Techniques. NIST, (2001).

[32] FIPS PUBLICATION 197, Advanced Encryption Standard (AES). U.S. DoC/NIST, November 26, (2001).

[33] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Request for Candidate Algorithm Nominations for the Advanced Encryption Standard. *Federal Register*, September 12, (1997).

[34] J. DAEMEN, V. RIJMEN, AES Proposal: Rijndael, Version 2. *Submission to NIST*, March (1999). http://csrc.nist.gov/ encryption/aes

Received: May, 2006
Revised: March, 2007
Accepted: April, 2007

Contact addresses:

Radomir Prodanović
Serbian Air Forces and Air Defense
Serbian Army
Glavna 1, Zemun, Serbia
e-mail: radisa100@ptt.yu

Dejan Simić
Faculty of Organizational Sciences
POB 52, Belgrade, Serbia
e-mail: dsimic@fon.bg.ac.yu

RADOMIR PRODANOVIĆ is a MSc student at FON – Faculty of Organizational Sciences, University of Belgrade. He is working for Serbia Army, Air Forces and Aircraft Defense, as Designer of Information Systems. He was Chief of Center for Computer Data Processing and worked on the design and implementation of several applications for his Command. He introduced several software applications in operational work, and designed computer network in the Command of Air Forces and Aircraft Defense. His interests are design and security of computer networks, implementation modern security tehnology in e-business, and management of e-documents.

DEJAN SIMIĆ, PhD, is a professor at the Faculty of Organizational Sciences, University of Belgrade. He received the B.S. in electrical engineering and the M.S. and the Ph.D. degrees in Computer Science from the University of Belgrade. His main research interests include: security of computer systems, organization and architecture of computer systems and applied information technologies.

Appendix A: Abbreviation

AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Access Point
ARP	Address Resolution Protocol
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining – Message Authentication Code
CFB	Cipher Feedback
CRC	Cyclic Redundancy Check
CTR	Counter Mode
DES	Data Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ECB	Electronic Codebook
GTK	Group Transient Key
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	IP Security
IV	Initialization Vector
LAEP	Lightweight Authentication Extension Protocol
MAC	Medium Access Control
MIC	Message Integrity Check
MSK	Master Session Key
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OSI	Open Systems Interconnection
PAE	Port Access Entry
PCMCI cards	Personal Computer Memory Card International Association
PEAP	Protected Extensible Authentication Protocol
PMK	Pair-Wise Master Key
PSK	Pre-Shared Key
PTK	Pair -Wise Transient Key
RADIUS	Remote Authentication Dial In User Service
RC4	A Stream Cipher Algorithm
RSA	Rivesi, Shamir, Adleman Algorithm
RSN	Robust Security Network
RSNA	Robust Security Network Association
SOHO	Small Office/Home Office
SSID	Service Set Identify
TA	Transmitter Address
TCP	Transmission ControlProtocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XOR	Exclusive OR