UDC 004.492

Holistic Approach to Wep Protocol in Securing Wireless Network Infrastructure

Radomir Prodanović[1], Dejan Simić[2]

[1] Serbia and Montenegro Army
Air Forces and Aircraft Defense
11000 Belgrade, Serbia and Montenegro
[2] Faculty of Organizational Sciences, POB 52,
11000 Belgrade, Serbia and Montenegro
radisa100@ptt.yu, dsimic@fon.bg.ac.yu

Abstract. 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 the higher level of wireless network infrastructure protection. Comparative analysis shows the advantages of the new 802.11i standard in comparison to the previous security solutions. A proposal of possible security improvements of RSNA (Robust Security Network Association) is presented.

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 post 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 data – with the wireless networks that medium is the air. Data are transferred via radio waves spreading throughout the space and thus, the information reaches anyone with the appropriate radio receiver. But 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 describes WEP protocol for the protection of wireless networks. Section 3 gives various kinds of attacks that can jeopardize security goals of WEP protocol: authentication, confidentiality and integrity. Significant safety improvements of WEP protocol that can lead to the higher level of wireless network infrastructure protection are described in Section 4. 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 5 also offers solutions for the improvements of the RSNA. The conclusion is given in Section 6.

2. 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 make 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 in case that they have appropriate receivers. The only possible way to protect this kind of network was to create a protocol that would work on second layer of OSI model and in this way provide the data protection during the data transmission. In order to protect data transmitted among the communicating parties, WEP uses shared secret key of 40 to 140 bits.

WEP protocol should achieve three main safety goals [5]:

- *Authentication*. It is the procedure to confirm the 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 questions and answers procedure between a station and 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 working station 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 to 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 checksum differentiates and in this case the message received is rejected.

3. Security threats to 802.11 wireless networks

Protection of wireless networks means protection from attacks on confidentiality, integrity and availability. Possible threats come from security deficiencies of WEP protocol [16, 6]. There are four attack techniques that can violate confidentiality or privacy [17]: 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 package during its transmission. This technique enables the attacker to have the 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 package 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 data indirectly by surveying the packages. 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 an 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 package 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 packages that should be received by other wireless users. These conditions are created by creation of IV sequence and message for each single message that is sent. After some time, when a package with the same IV as in 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.

There are three techniques that can violate the integrity of the traffic [17]: unauthorized access, high jacking 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 the access to the network, he is able to initiate some other types of attacks or use network without being noticed. Some can be of an opinion 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 the 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 cannot prevent attacks that indirectly ruin confidentiality. Man in the middle, high-jacking 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 packages with violate integrity of the session. There are several ways to implement this type of attack. One way is when attacker disrupts the session and does not allow for the station to establish communications again with the AP. 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 one is established between the attacker and the station. This enables attacker to have the access to the data exchanged between the working station 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 [8] and not towards wireless clients. The attacker escapes authentication or provides false accreditations by this kind of attack. The attacker becomes valid user and gets the access to the network as authenticated user by getting the false accreditations.

High-jacking 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 lost the session due to ordinary lacks in network functioning. Once the attacker takes over a valid session he

can use it for various purposes over a certain period of time. This attack happens in a real time.

Replay attack. This type of attack is used to access the network through authorization. The session that is under an attack does not change nor 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. The attacker comes to the authentication of one or more sessions, and then replies to the session after a certain period of time or uses couple of sessions to compose the authentication and reply to it.

There are several types of DoS (Denial of Service) attacks that can violate the availability of the network. There are several DoS attacks that make use of unprotected control and management frameworks of WLAN and unprotected EAP messages in 802.1X authentication. DoS attacks on AP that generates the abundance of Association Request messages are also known. The attacker could direct DoS attack to Michael algorithm, RSN IE element and 4-Way Handshake. All these DoS attacks and counter measures are described in [9]. Chapter 5.5 gives recommendations for the early detection of RSN IE Poisoning attack.

Jamming. Jamming [3, 22] is one of DoS attacks on network availability. It is performed by malicious attackers who use other wireless devices to disable the communications of users in a legitimate wireless network.

4. Security improvements of WEP

Safety improvements of WEP protocol are based on the improvements of the mechanisms for preservation of WEP security goals. Improvements are adjusted to the existing network equipment without some significant performance malfunctions. The new 802.11i standard introduces a new mechanism for message encryption and integrity check.

4.1. RSA patch for WEP and Wi-Fi protection

RSA Security and Hifn have discovered a new way of fast generation of keys unique for each of RC4 algorithm packages. The new solution is named Fast Packet Keying and uses hash technique of fast generation of a unique keystream for each package. The solution is based on the following rules [18]:

- 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 package. This means that in the process of data

transmission from working stations to access point a set of keys different from the set of keys used during data transmission from the access point to the working station will be used. In the second phase there is a combination of the first phase exit with IV generating thus a unique key stream for each of the packages.

IEEE studied all details of WEP security problems and focused on 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 brought 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.

The first improvement [21] offered by WPA is data encryption by TKIP (Temporal Key Integrity Protocol).

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

4.2. TKIP i 802.1x

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 ruining the performance significantly.

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.

IEEE 802.1x [4]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 [1], 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.

4.3. RSNA

Previous researches showed that primary authentication method [2] (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 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 [19, 7]:

Phase 1: Request, authentication and association. Station looks for the AP with appropriate SSID. All APs in the range answer with the Probe Request framework, as shown in Figure 1. 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 the phase 1 the workstation and AP establish security rules and 802.1x authentication port is locked. 802.1x network port remains locked as long as the authentication procedure has not been completed.

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. EAP can route messages to the authentication server (such as RADUIS) through 802.1x port when it is locked. EAP packages between the station and the authenticator encapsulated EAPOL (EAP over LAN) packages, while EAP messages between authenticator and authentication server are encapsulated in RADUIS packages. If the mutual authentication is successful, the authentication server generates Master Session key (MSK) and forwards it to the authenticator and

the station. PMK (Pair-Wise Master Key) is then generated by the station and authenticator based on the MSK.

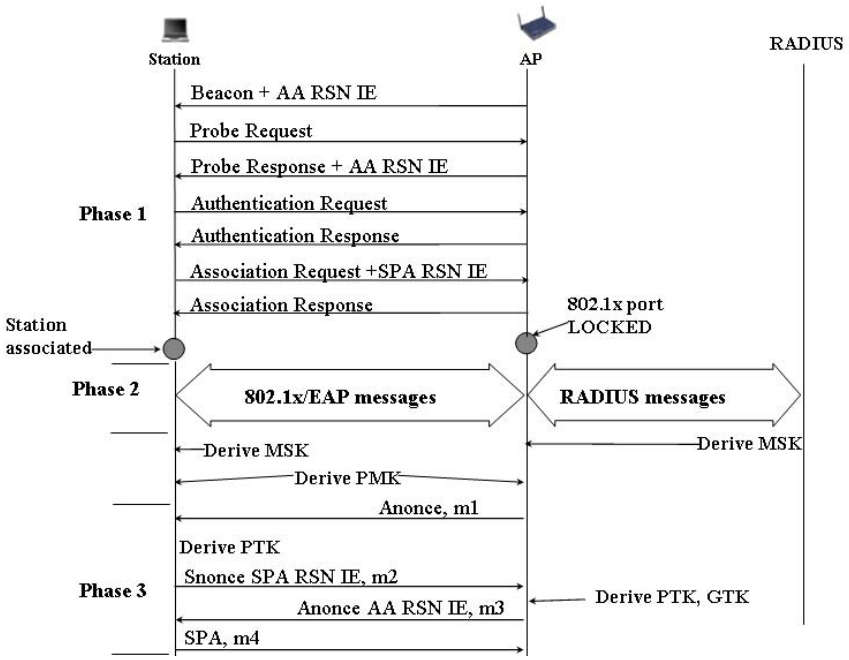

Fig. 1. RSNA Procedures

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 1). 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.

4.4. WPA, WPA2 and 802.11i

IEEE 802.11i [10], an IEEE standard ratified 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. WPA2/WPA mode is not allowed in WPA2 equipment due to WEP security problems.

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 [14] 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 and all that in order to increase WEP safety.

AES-CCMP [13] 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 [12] 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 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 [20].

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.

Table 1. Comparative analysis of WLAN safety improvements

<table>
<tr><th></th><th>WEP</th><th>WPA</th><th>WPA2/
802.11i</th></tr>
<tr><td>Authentication</td><td>Open authentication system and shared key authentication (same key as for encryption) – Pre-RSN</td><td>Shared key authentication and strong authentication based on 802.1x and EAP (RADIUS server)</td><td>Authentication based on 802.1x and EAP (RADIUS server) and pre-authentication</td></tr>
<tr><td rowspan="6">Encryption</td><td>Thoroughly researched and documented defficiencies</td><td>Removes all WEP deficiencies</td><td>Removes WEP and WPA deficiencies</td></tr>
<tr><td>40 bit key</td><td>128 bit key</td><td>128, 192, 256 bit key</td></tr>
<tr><td>Statical key distribution – all network users use the same key</td><td colspan="2">Dynamic key distribution – new keys for each user, session, package</td></tr>
<tr><td>Manual key distribution – it is necessary to enter the key into each device</td><td colspan="2">Dynamic key distribution</td></tr>
<tr><td colspan="2">Uses IV</td><td>Does not use IV</td></tr>
<tr><td colspan="2">RC4 algorithm encryption</td><td>AES algorithm encryption</td></tr>
<tr><td>Integrity</td><td>CRC</td><td>MIC (64 bit key)</td><td>CBC-MAC (the same key as for encryption)</td></tr>
</table>

4.5. The proposals of possible security improvements of RSNA

One of the viable DoS attacks is the attack on the RSN IE authentication. This kind of attack starts during the Phase 1 of RNSA procedure, and becomes visible during the implementation of the 4-Way Handshake procedure.

RSN IE authentication procedure starts in Phase 1 when the authenticator produces Beacon signal. The authenticator inserts RSN IE in the Beacon frame. IEEE 802.11i introduces RSN IE (RSN Information Element) as an information carrier for authentication and key selection. During the Pahse 1 the authenticator introduces RSN IE once again into the message he sends to the user – this time it is the Probe Response message. When authentication messages are exchanged, the user inserts his RSN IE in Association Request message. During the implementation of the 4-Way Handshake procedure, the user and the authenticator both check RSN IE they exchanged in Phase 1 of the RSNA procedure (as shown in Figure 1). In the second message (m2), 4-Way Handshake user sends his RSN IE he received from the authenticator in Phase 1. Now the authenticator compares his RSN IE (RSN IE sent to the user with the Beacon and Probe Response messages) to the RSN IE he received from the user. If there is no match between these two, the authenticator generates an error of safety parameters, rejects the keys (Master Session Key, Pairwise Master Key) he exhanged with the user before the 4-Way Handshake procedure and generates a message to disrupt further communication. If RSN IE of the authenticator remains unchanged, then the authenticator in his third message sends to the 4-Way Handshake user RSN IE he received with the Association Request message. The user compares the RSN IE he sent to the authenticator in the Phase 1 to the RSN IE from the third message (m3). If there is a mismatch, the user rejects the keys and generates a message to stop communication.

RSN IE authentication attack is undertaken when the attcaker modifies the “insignificant“ RSN IE bites in the authenticator's Beacon frame or Probe Response message. The second possible way to conduct the attack is to modify “insignificant“ RSN IE bites in Association Request message. In both cases modified bites will not influence the correctness of the frames and the authentication will continue. But, during the 4-Way Handshake procedure, verification of RSN IE station and authenticator is being done. As previously described, the user sends RSN IE received from the authenticator in his second 4-Way Handshake message. The authenticator compares the RSN IE he received in the second message to the RSN IE he sent to the user by Beacon and Probe Response messages. In case of a mismatch between the two RSN IE, the authenticator disrupts the session. The user checks the RSN IE in the same way, only after the third message that contains the RSN IE authenticator received with Association Request message. This attack is known as RSN IE Poisoning.

RSN IE Poisoning is detected before 802.1x port is being unblocked and safe communication started. The attack is initiated during the dissemination of the Beacon frame, and becomes visible during the 4-Way Handshake procedure. In this period of time, resources of the station, authenticator and

authentication server are being used. Frequent RSN IE Poisoning attacks make it impossible for the station to authenticate and thus realize communication.

This kind of attack could be prevented by providing a mechanism for earlier attack detection. The authors of this paper discuss in theory three mechanisms for early detection of RSN IE element modification during connection establishment. The purpose of these mechanisms is to detect the false RSN IE in early stages of RSNA procedure before the 802.1x port is blocked.

In the Phase 1 of RSNA procedure, the workstation receives Beacon and Probe Response messages from RSN IE authenticator. The workstation does not know if the RSN IE has been changed by the attacker in the process of communication. As user always replys to authenticator's messages by its own messgaes, the authors recommend to send the RSN IE of the authenticator with the messages sent as a reply to the above mentioned messages (as shown in Figure 2). Now the authenticator could compare the RSN IE he received from the workstation to the RSN IE he sent with the Beacon and Probe Response messages. In case of the mismatch of the two RSN IE the authenticator disrputs the communication. In this way it would be possible to prevent the change of authenticator's RSN IE.

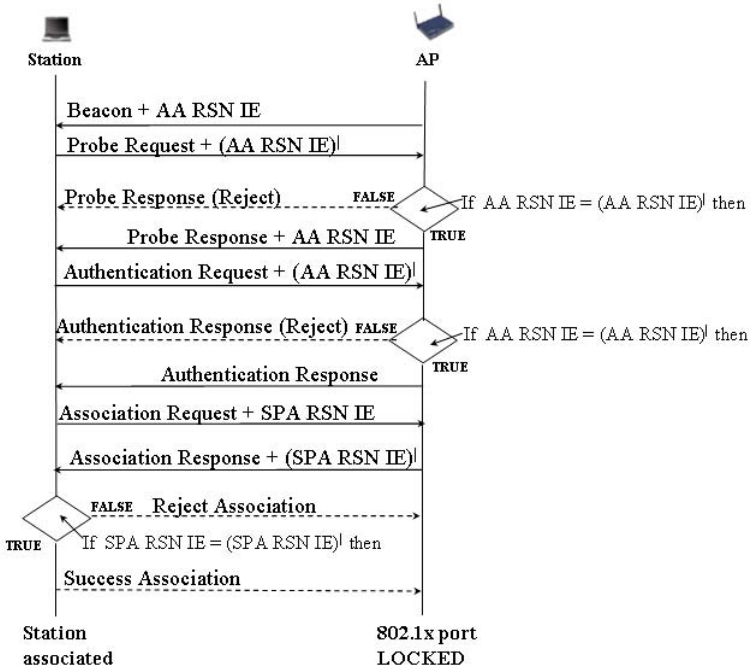

Fig. 2. The First Mechanism for early detection of RSN IE Poisoning

The attacker could change the user's RSN IE in the same way during the transmission of the Association Request message. The authors recommend the same approach as in detection of authenticator's RSN IE changes. This time the authenticator will send user's RSN IE by the Association Response message. User will compare RSN IE sent and received and will generate a message to disrupt the communication before ports are blocked in case that there is incompatibility of RSN IEs.

The core of this mechanism is to answer to every RSN IE sent by RSN IE received, to compare them and depending on the result to continue or disrupt further authentiaction and association.

One deficiency of this mechanism is a need for modification of three standard messages. It is necessary to modify the Probe Request, Authentication Request and Association Response messages by inserting RSN IE into them. The next deficiency comes from a frequent comparison of RSN IE and RSN IE'. The user performs comparison once, while the authenticator performs this comparison twice (upon the receipt of the Probe Request and Authentication Request messages). Each time comparison is performed, the processor's time is spent resulting in speed reduction. This is more noticeable at the authenticator' side then at the user's since at the same time the authenticator conducts multiple comparisons for several users who try to establish communication. One more deficiency of this mechanism is not sufficient protection of RSN IE in RSNA messages exchange procedures.

The good side of the mechanism is its capability to reduce RSN IE Poisoning attack. In order to conduct RSN IE Poisoning attack, now the attacker must follow and change not only the authenticator's messages with the RSN IE but the user's messages with authenticator's RSN IE also. This complicates the procedure for RSN IE attacking, so the attacker is no longer efficient as before when he was only to change RSN IE once. Attacker's effectiveness is reduced and thus cost effectiveness of this kind of attack is brought to question. The mechanism enables detection of the attack before 802.1x port is blocked to the contrary of the existing mechanism that is being applied during 4-Way Handshake procedure, thus preventing the user, authenticator and RADIUS server resources to be spent.

The second mechanism is the modification of the first one. The difference is in the fact that in the second mechanism the user sends authenticator's RSN IE together with his RSN IE in the Association Request message, as in Figure 3. Now the authenticator performs only one check of RSN IE. In this way the deficiencies of the first mechanism related to the spending of the authenticator's resources are reduced. This mechanism requires introduction of the following messages by the user: Reject Association (with this message the user rejects establishing connection with the authenticator due to the incompatibilities of RSN IEs sent and received) and Success Association (with this message the user accepts the establishment of connection with the authenticator).

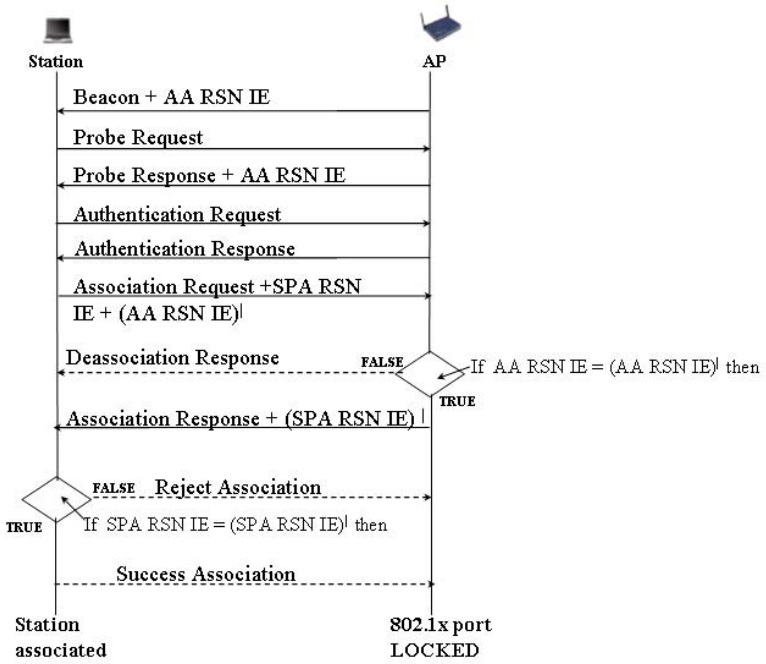

Fig. 3. The Second Mechanism for early detection of RSN IE Poisoning

Both above mentioned mechanisms work with unprotected RSN IE. A skilled attacker could track RSN IE all the time and change it before the user and the authenticator perform the comparison. Neither the user nor the authenticator has the mechanisms to detect the RSN IE changes and its source. In order to escape this deficiency of RSN IE change detection and source, the authors consider introduction of Public Key Infrastructure (PKI). Now the mechanism for early detection of RSN IE Poisoning attack would be based on the verification of integrity of RSN IE received either by the user or the authenticator.

Each user has a pair of keys (a public and a secret key). The authenticator has not only his public and secret keys but public keys of all the users. Also, all users have the public key of the authenticator. Before the authenticator sends his Probe Response message, he uses his secret key for digital signature of RSN IE. Digital Sign IE (DS IE) adds RSN IE and then encrypts RSN IE and DS IE by the public key of the user trying to establish connection. When the user receives RSN IE of the authenticator, he first decrypts by his secret key the RSN IE he received, and then verifies DS IE by the public key of the authenticator. If DS IE verification is successfully completed, RSN IE procedure is continued. If DS IE verification is not successfully completed that means that there has been a modification of authenticator's RSN IE. In this case RSN IE procedure is disrupted and starts from the beginning.

Verification of the user's RSN IE is done in the same way. The user digitally signs his RSN IE by his secret key. Digital Sign DS IE joins RSN IE to be encrypted by the authenticator's public key. RSN IE encrypted in this way is then sent via Association Request message to the authenticator. The authenticator then decrypts RSN IE by his secret key and verification is done by the public key of the user.

PKI mechanism is more efficient in prevention of RSN IE Poisoning attack than the two previous mechanisms. Now any RSN IE modifications created by the attacker could be detected immediately upon the receipt of the RSN IE message, while in the previous two mechanisms these modifications could be detected only by the party that generated the RSN IE. This mechanism does not require any changes in other messages but only expanding of RSN IE format, meaning that it is only necessary to add a field for digital signature. Also, this mechanism does not require introduction of new messages such as Reject Association and Success Association in the first and the second mechanisms.

The deficiency of this mechanism is key distribution to the users and authenticator as well as compatibility with the users that do not use this mechanism. These users cannot establish connection with the authenticator since they cannot decrypt RSN IE.

5. 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 in a good way. 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. Some DoS attacks cannot be eliminated completely, but could be detected sooner via appropriate mechanisms. The authors considered in theory three mechanisms for early detection of RSN IE Poisoning attack. Application of these mechanisms could significantly reduce the efficiency of RSN IE Poisoning attacks and would bring its cost effectiveness in question. If DoS attacks cannot be completely eliminated, than it is necessary to apply appropriate mechanisms in order to prevent them and reduce the damage they can cause.

6. References

1. Anthon,J.: Using IEEE 802.1x to Enhance Network Security. FoundryNetworks. (2002). [Online]. Available at: http://www.foundrynet.com/solutions/appNotes/PDFs/802.1xWhite_Paper.pdf
2. Arunesh, M., Arbaugh, A.W.: An Initial Analysis of the IEEE 802.1X Standard. Maryland. (2002). [Online]. Available at: http://www.cs.umd.edu/%ewaa/1x.pdf
3. AusCERTAA-2004.02. Denial of Service vulnerability in IEEE 802.11 wireless devices. (2004). [Online]. Available at: http://www.auscert.org.au/render.html?it=4091.
4. Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J., Levkowetz,H.: Extensible Authentication Protocol (EAP).Internet Draft draft-ietf-eap-rfc2284bis-06.txt. (2003).
5. Borisov, N., Goldberg, I., Wagner, D.: Intercepting Mobile Communications: The Insecurity of 802.11, DRAFT. (2002). [Online]. Available at: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
6. Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications: the insecurity of 802.11. InProceedings of the 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy. (2001).
7. Chen, J.C.,. Jiang, M.C., Liu, Y.W.: Wireless LAN security and IEEE 802.11i. IEEE Wireless Communications, vol. 12, no. 1, pp. 27-36, (2005).
8. Fleck, B., Dimov, J.: Wireless access points and ARP poisoning: wireless vulnerabilities that expose the wired network. White paper by Cigital Inc. (2001). [Online].Available at: http://www.cigitallabs.com/resources/papers/download/arppoison.pdf
9. He, C., Mitchell, J. C.: Security Analysis and Improvements for IEEE 802.11i. Stanford, USA. (2004). [Online]. Available at: http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf
10. 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).
11. Karygiannis, T., Owens, L.: Wireless Network Security 802.11, Bluetooth and Handheld Devices. NIST, (2002). [Online]. Available at: http://csrc.nist.gov/publications/nistpubs/800-48/nist_sp_ 800-48.pdf

12. National Institute of Standards and Technology. FIPS Pub197: Advanced Encryption Standard (AES). (2001).
13. Perez, E.,: 802.11i (How we got here and where are we headed). Orlando. (2004). [Online]. Available at: http://www.giac.org/practical/GSEC/Elio_Perez_GSEC.pdf
14. Phifer, L.: 802.11i: Robust and ready to go. (2004). [Online]. Available at: http://searchmobilecomputing.techtarget.com/tip/1,289483,sid40_gci992741,00.html
15. Walker, J.R: 802.11 Security Series (Part II: The Temporal Key Integrity Protocol (TKIP)). Intel Corporation. [Online]. Available at: http://cache-www.intel.com/cd/00/00/01/77/17769_ 80211 _part2.pdf
16. Walker, J.R.: Unsafe at any key size; An analysis of the WEP encapsulation. IEEE Document 802.11-00/362. (2000).
17. Welch, J., Lathrop, S.D.: A Survey of 802.11a Wireless Security Threats and Security Mechanisms., United States Military Academy West Point, New York. (2003). [Online]. Available at: http://www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf
18. WEP Fix using RC4 Fast Packet Keying. RSA Laboratories. (2002). [Online]. Available at: http://www.comms.scitech.susx.ac.uk/fft/crypto/wep.pdf
19. White paper: Testing for Wi-Fi Protected Access (WPA) in WLAN Access Points. Net-O_2 Technologies. (2003). [Online] Available at: http://www.net-o2.com
20. Whiting, D., Housley, R., Ferguson, N.: Counter with CBC-MAC (CCM). RFC 3610. (2003).
21. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. Wi-Fi Alliance. (2003). [Online]. Available at: http://www.wi-fi.org/opensection/pdf/whitepaper_wi-fi_ security4-29-03.pdf
22. Wullems C., Tham, K., Smith, J., Looi, M.: Technical Summary of Denial of Service Attack against IEEE 802.11 DSSS based Wireless LAN's. [Online]. Available at: http://www.isrc.qut.edu.au/wireless/

Radomir Prodanovic is a MSc student at FON - Faculty of Organizational Sciences, University of Belgrade. He is working at Serbia and Montenegro Army, Air Forces and Aircraft Defense as Designer of Information Systems. Radomir Prodanovic was Chief of Center for Computer Data Processing and worked on design an implementation more applications for his Command. He introduced more software applications in operational work, and designed computer network in 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 Simic, 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.