Fragility of the Robust Security Network: 802.11 Denial of Service

Martin Eian

Department of Telematics
Norwegian University of Science and Technology
martin.eian@item.ntnu.no

Abstract. The upcoming 802.11w amendment to the 802.11 standard eliminates the 802.11 deauthentication and disassociation Denial of Service (DoS) vulnerabilities. This paper presents two other DoS vulnerabilities: one vulnerability in draft 802.11w implementations discovered by IEEE 802.11 TGw, and one new vulnerability in 802.11, which is still present in the 802.11w amendment. Attacks exploiting the first vulnerability are significantly more efficient than any known 802.11 DoS attacks, while attacks exploiting the second vulnerability have efficiency and feasability equivalent to a disassociation attack. This paper provides an experimental verification of these attacks, demonstrating their feasability using freely available software and off the shelf hardware. Finally, the root cause of these vulnerabilities is discussed and a backwards compatible solution proposed.

Keywords: Wireless, Security, Denial of Service, 802.11, 802.11i, 802.11w.

1 Introduction

In the original IEEE 802.11 standard[9], ratified in 1997 and accepted as an ISO standard in 1999, the only available security mechanism was Wired Equivalent Privacy (WEP). During the years that followed, WEP was analyzed by the academic community and wireless hackers, and several vulnerabilities were discovered [8] [15] [5]. This motivated the development of a replacement for WEP, IEEE 802.11i. In 2004, the 802.11i amendment was ratified, with two new and improved security mechanisms. The first one, Temporal Key Integrity Protocol (TKIP), was designed as a transitional solution that would support old hardware. The second, counter mode with cipher-block chaining message authentication code protocol (CCMP), was the long term solution to the security vulnerabilities of WEP. The common denominator for WEP, TKIP and CCMP is that they protect 802.11 data frames. No protection is provided for control frames and management frames.

One issue with the lack of management frame protection is that any station on the wireless network can transmit forged management frames. This tactic can be used by an attacker to make a station (STA) deauthenticate or disassociate from the access point (AP). The following association request from the

M. Abdalla et al. (Eds.): ACNS 2009, LNCS 5536, pp. 400–416, 2009.

station gives the attacker the service set identifier (SSID) of the wireless network, thus bypassing SSID cloaking. Furthermore, dictionary attacks against TKIP or CCMP using a password derived preshared key (PSK) require that the attacker observes the initial 4-way handshake, and a successful disassociation attack will result in this 4-way handshake between the wireless station and the AP. Last, but not least, transmitting deauthentication or disassociation frames several times per second is a very efficient Denial of Service attack on the wireless network. Aireplay-ng from the aircrack-ng[1] suite is an example of a freely available tool that implements the deauthentication attack. One countermeasure to these attacks is to provide integrity and replay protection for management frames.

Another issue that has surfaced recently is that several of the new amendments to the 802.11 standard extend the use of management action frames, transmitting potentially sensitive information inside management frames. Examples of such amendments are 802.11k, 802.11r and 802.11v. To avoid the compromise of sensitive information, management frame confidentiality must be provided.

As a response to the above mentioned issues, Task Group w (TGw) was established in 2005 to develop the 802.11w amendment, Protected Management Frames. The original target date for ratification of this amendment was September 2007, but this was later postponed to December 2009. The design goal for 802.11w was to extend the security mechanisms in 802.11i to provide protection for selected 802.11 management frames. 802.11w is currently in draft status. The newest available draft version is 7.0.

The results presented in this paper are based on IEEE 802.11-2007[13], which includes the 802.11i amendment[10], and 802.11w draft version 3.0[12] from September 2007. One additional feature from 802.11w draft version 4.0, protection against SA termination attacks, is also discussed. The analysis of potential DoS vulnerabilities in 802.11 with amendments is based on the observations in [14].

The rest of the paper is divided into eight sections. Section 2 presents the contribution. In Section 3, a short description of related work on 802.11 DoS vulnerabilities is presented. Section 4 contains an analysis of relevant topics from the 802.11 standard with amendments. Section 5 presents theoretical DoS vulnerabilities in 802.11, 802.11i and 802.11w and some general observations on network DoS. Section 6 provides a description of the experiments, analysis and results. The results are discussed in Section 7, and a solution proposed in Section 8. Section 9 contains the conclusion and section 10 contains acknowledgements.

2 Contribution

This paper analyzes medium access control (MAC) layer DoS vulnerabilities in 802.11 with the 802.11i and 802.11w amendments. One apology for MAC layer DoS vulnerabilities is that an attacker can use physical jamming of the radio frequencies to perform a DoS attack anyway, which is extremely difficult to prevent. The motivation for preventing DoS attacks against the MAC layer is that such attacks are far more efficient than jamming, so the attacker has to spend

less effort, and thus will be more difficult to detect and locate. Furthermore, certain attacks against MAC layer vulnerabilities may cause a deadlock such that a station is not able to recover. A jamming attack, on the other hand, will only disrupt network access for as long as the attacker is transmitting.

The configuration used for the experimental analysis is an extended service set (ESS) with a wireless station communicating with an AP. The term station refers to either a non-AP 802.11 device or an AP.

This paper makes three principal contributions. First, a previously unknown DoS vulnerability in 802.11, equivalent to the disassociation vulnerability, and still present in 802.11w, is presented and analyzed. Second, this new vulnerability is tested experimentally together with the deauthentication attack and another vulnerability discovered by J. Epstein in 2007[6]. All experiments were carried out using freely available tools and off the shelf hardware. Third, a robust solution to the MAC layer DoS vulnerabilities in 802.11 is proposed. It is possible to introduce this solution incrementally, preserving backwards compatibility until all APs and stations are upgraded.

3 Related Work

In 2003, Bellardo and Savage demonstrated the feasability and efficiency of the 802.11 deauthentication attack, together with several other DoS attacks against the 802.11 MAC layer[4]. [4] is a useful general reference on DoS attacks against 802.11 networks. In 2007, J. Epstein presented the theoretical SA termination attack[6] and a proposed solution[7] to TGw, which was accepted as part of draft 4.0 of the 802.11w amendment in 2008. The SA termination attack and the proposed solution are analyzed in this paper. The working documents of TGw are available at `https://mentor.ieee.org/802.11/documents`.

4 Analysis of the 802.11 Standard

Only the most relevant parts of the 802.11 standard and the 802.11i and 802.11w amendments are presented as background material. The reader is referred to the IEEE standard and draft documents for a comprehensive review.

4.1 802.11 Authentication and Association

The original 802.11 standard specifies two types of authentication: shared key and open system. The shared key authentication is optional in WEP, and the open system authentication is a two-message null authentication initiated by the station. After authentication, the station performs an association with the AP. Figure 1 shows a successful open system authentication followed by a successful association.

Associations are used to keep track of the stations served by an AP. The 802.11 standard defines two state variables: authentication state and association

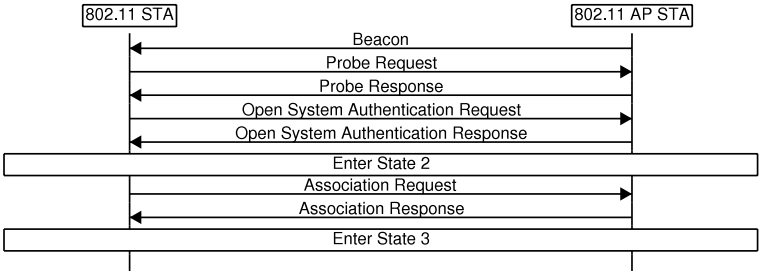

Fig. 1. 802.11 open system authentication and association

Table 1. 802.11 States

State 1	Not authenticated	Not associated
State 2	Authenticated	Not associated
State 3	Authenticated	Associated

state. Three of the four possible combinations of these two variables represent the local 802.11 station states shown in Table 1. Every station maintains a local state for every other station that it communicates with.

802.11 frames are grouped into classes that correspond to the states mentioned above. Frames corresponding to the current state or lower are allowed, thus the allowed frames in State 2 are of Class 1 or 2. If a station receives a Class 2 or 3 frame from a station that is not authenticated, it shall respond with a deauthentication frame. If it receives a Class 3 frame from a station that is authenticated, but not associated, it shall respond with a disassociation frame. Figure 2 shows the valid transitions between the local states in 802.11.

Subsection 11.3.1.2 of the 802.11 standard[13] specifies how the destination STA should handle 802.11 authentication requests:

> Upon receipt of an Authentication frame with authentication transaction sequence number equal to 1, the destination STA shall authenticate with the indicated STA using the following procedure:
>
> a) The STA shall execute the authentication mechanism described in 8.2.2.2.
> b) If the authentication was successful, the state variable for the indicated STA shall be set to State 2.
> c) The STA shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication.

Note that an open system authentication will always be successful, so an AP that receives an open system authentication request will always enter State 2 (authenticated, but not associated).

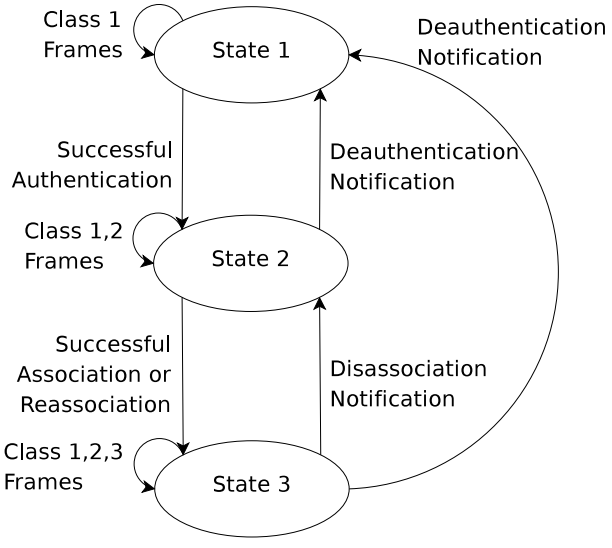

Fig. 2. 802.11 state transitions. The authentication attack triggers a change from State 3 to State 2 in the AP by transmitting a forged open system authentication request. This transition is not shown in the state diagram, the only transition from State 2 to State 3 is a disassociation notification, but it must be allowed to avoid deadlocks when 802.11w is enabled.

4.2 802.11i Security Amendments

802.11i introduces a new security framework: The Robust Security Network (RSN). Authentication and key management in an RSN is carried out after the successful completion of 802.11 authentication and association, as illustrated in figure 1. However, some of the messages are modified. The beacon frames broadcast by the AP and the probe response contain an RSN information element with the supported security parameters. Cryptographic parameters are negotiated during the association phase by including an RSN information element in the association request from the station. If the security parameters are accepted by the AP, it enters State 3, and authentication is carried out using the Extensible Authentication Protocol (EAP)[3]. EAP encapsulation over Local Area Networks (EAPOL), as specified in IEEE 802.1X[11], is used to encapsulate the authentication messages in 802.11 data frames. Figure 3 shows the authentication and key management in an RSN.

802.11i uses security associations (SAs) to store security policies and cryptographic keys. There are two parts of the SA specifications that are relevant to the vulnerabilities discussed in this paper: SA termination and recovery from lost key state synchronization.

SA termination is triggered when an AP receives or transmits certain management frames. If an AP receives a valid association or reassociation frame from a station, it will delete the pairwise transient key SA (PTKSA), which contains

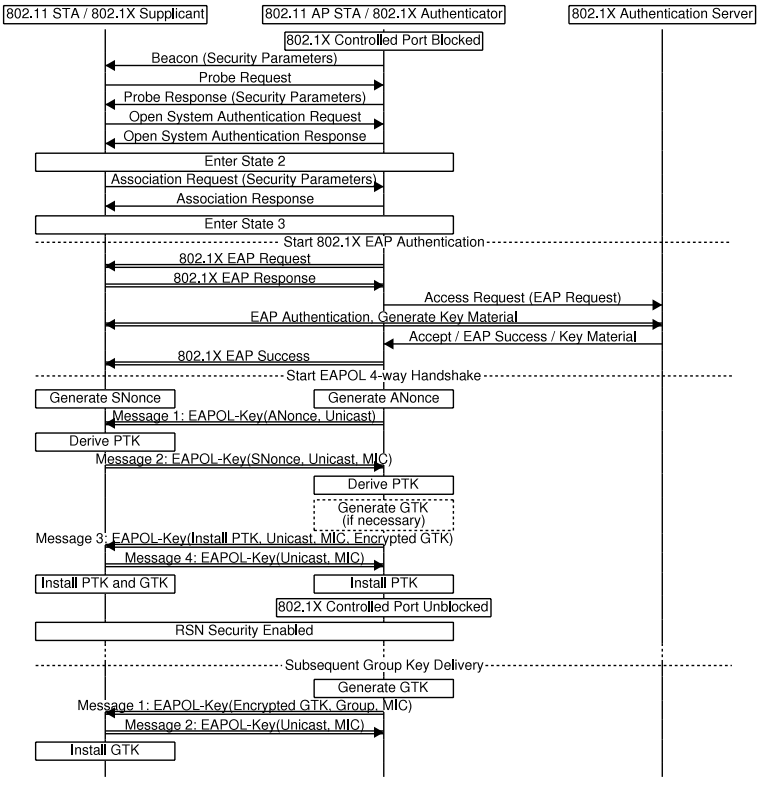

Fig. 3. 802.11i RSN authentication and key management. Single lines represent management frames, double lines represent data frames. Note that a deauthentication attack will force the station to do the whole procedure over again, starting with the authentication request. If pairwise master key security association (PMKSA) caching is enabled, the 802.1X authentication does not have to be repeated.

the station's pairwise transient key. The PTKSA is also deleted if the AP sends or receives a deauthentication or disassociation frame.

Loss of key state synchronization can occur if a station reboots and the temporal keys stored in memory are lost. A station that loses key state synchronization in an ESS shall perform the deauthentication procedure before it sends an authentication request. If the authentication and key management protocol (AKMP) fails between a station and an AP that are associated, both the station and AP shall perform the deauthentication procedure.

4.3 802.11w Protected Management Frames

802.11w uses CCMP from 802.11i to provide integrity, confidentiality and sender authenticity for unicast management frames, and Broadcast Integrity Protocol (BIP) to provide integrity for broadcast management frames. In both cases,

protection is only provided for management frames of subtype action, deauthentication and disassociation. If protection of management frames is enabled and an unprotected management frame of subtype action, deauthentication or disassociation is received, the frame is silently discarded.

5 Vulnerability Analysis

5.1 General Observations

Meadows discusses several important principles for protocol design to minimize the vulnerability to DoS attacks[14]. One of the fundamental principles is the following:

> First of all, such a protocol must provide authentication from the very beginning.

802.11 with the 802.11i and 802.11w amendments does not provide this, since the 802.11 authentication and association procedures are carried out, unprotected, before the 802.11i authentication is initiated. All of the messages exchanged prior to the 802.11i authentication can thus be forged by an attacker. Of particular interest are the messages that result in state transitions for the AP: authentication requests, association requests, deauthentication notifications and disassociation notifications. A successful authentication request will make the AP enter State 2. A successful association request will make the AP enter State 3 if it is currently in State 2. Deauthentication and disassociation notifications will make the AP enter State 1 or State 2, respectively. The 802.11w amendment provides integrity protection for deauthentication and disassociation notifications, and in the latest drafts it also provides a mechanism to avoid forged association requests. Authentication requests, however, are not protected. Exploiting unprotected authentication requests to perform a DoS attack against 802.11 with 802.11i and 802.11w is a principal contribution of this paper.

5.2 The 802.11 Standard

802.11 deauthentication and disassociation DoS attacks are carried out by forging a deauthentication or disassociation frame. The receiving station will change to State 1 for a deauthentication or State 2 for a disassociation. The most efficient of these two is the deauthentication attack. If the station is deauthenticated, it has to authenticate and associate to be able to send and receive traffic again. A slightly more efficient approach is to deauthenticate the AP, which resets the AP to State 1. The next data frame from the station will be dropped, the AP will respond with a deauthentication notification, and the station will then authenticate and associate.

5.3 802.11i Security Amendments

802.11i significantly "improves" the efficiency of the deauthentication DoS attack. Once a station has been deauthenticated, it must first perform 802.11 authentication and association. Then, if enabled, 802.1X authentication must be carried out. 802.1X authentication is not used with TKIP-PSK and CCMP-PSK, or when PMK caching is enabled and a valid PMKSA exists between the AP and station. Finally, an EAPOL 4-way handshake must be completed to derive the temporal keys. Once the 4-way handshake is completed, the station can send and receive traffic.

The SA termination procedures in 802.11i make an even more efficient DoS attack possible. If an attacker sends a forged association or reassociation frame from the station to the AP, the AP will remain in State 3, but the temporal keys will be deleted. The AP will start the EAPOL 4-way handshake, which will eventually time out, then deauthenticate the station, resulting in the procedure described in the previous paragraph.

5.4 802.11w Protected Management Frames

802.11w prevents the deauthentication and disassociation attacks. However, the effect of the SA termination attack is amplified. When the EAPOL 4-way handshake times out, the AP will try to deauthenticate the station. Since the pairwise keys in the AP are deleted, the deauthentication frame will not be protected, and thus discarded by the station. The station will not be able to send or receive any traffic, and is not able to recover, since it discards the deauthentication frames from the AP. An attempt to fix this vulnerability is included in draft version 4.0 and later of 802.11w, where a cryptographically protected SA Query procedure is used to determine whether or not an association or reassociation frame from the station is legitimate. Implementations based on draft 3.0 or earlier, however, are still vulnerable to the SA termination attack.

The SA Query procedure works as follows: if an AP receives an association request from a station with which it has a valid PTKSA, the AP responds that the association request was temporarily rejected. This response tells the station how long it has to wait before it can send another association request. Then, the AP tries to send one or more query messages to the station to check if it has a valid PTKSA. The queries are management action frames protected under the current PTKSA. If a valid response to one of these queries is received, the association request is ignored. If no response is received before the timeout value is reached, the AP will delete the PTKSA. A station that loses key state synchronization will thus have to send an association request, wait until the query procedure times out, then send a new association request. The number of queries and timeout value are configurable parameters.

Another issue with 802.11w is that the recovery procedure for lost key state synchronization in 802.11i is no longer possible, since a station that loses synchronization will not be able to send a protected deauthentication frame to the AP. To recover, a station has to start 802.11 authentication without first performing a deauthentication, and the AP has to allow this to avoid a deadlock.

This can be exploited to enable a new kind of DoS attack against 802.11: The attacker transmits a forged open system authentication frame, which will make the AP enter State 2. The AP still has a valid PTKSA with the station, so once the station transmits a data frame, the AP responds with a protected disassociation frame. The end result is the same as if a disassociation attack had been carried out. This type of attack will from now on be referred to as an "authentication attack".

6 Experiments

The goals of the experiments were to verify the feasability of the authentication and SA termination DoS attacks, and to verify that 802.11w protects against the deauthentication attack. To this end, the authentication, SA termination and deauthentication attacks were performed both with 802.11w enabled and disabled, for a total of six experiments. Each attack was performed 100 times to ensure that the results were consistent.

6.1 Infrastructure Set-Up

The infrastructure under attack consisted of a Cisco 4402 wireless controller (AIR-WLC4402-25-K9) and a Cisco 1030 access point (AIR-AP-1030). Both the wireless controller and access point were running software version 4.2.61.0 with Cisco Management Frame Protection (MFP) based on an earlier 802.11w revision than draft 3.0. 802.11i CCMP-PSK was used for all the experiments. The wireless controller and AP were configured to reject shared key authentication, and CCMP-PSK was required, which means that association requests without an RSN information element were rejected. The station was a laptop computer with a Cisco Aironet 802.11 a/b/g network adapter (AIR-CB21AG-E-K9), running Windows XP SP2. The station was assigned an IPv4 address through DHCP from the wireless controller. Both the AP and station used 802.11g for the experiments. The attacker was a laptop with a wireless network interface card (NIC) with the Atheros AR2413 chipset, running Linux 2.6.22 with the madwifi-ng drivers, and aircrack-ng[1] version 0.9.1 as the attack software. In particular, airmon-ng was used to enable RFMON (monitor) mode, aireplay-ng and airtun-ng were used to inject frames, and airodump-ng to capture traffic. The same wireless network interface was used for frame injection and traffic capture, and the experiments were conducted in a typical office environment, with no shielding from other wireless stations and APs nearby. The only legitimate traffic on the wireless network was an Internet Control Message Protocol (ICMP) ECHO request from the station to a server on the wired LAN every second, and an ICMP ECHO request from the server to the station every second, along with the ICMP ECHO responses. The ping commands in Windows XP and Linux were used to generate traffic from the station and server, respectively.

6.2 Attacks

The attacks were carried out by transmitting a single management frame of subtype authentication request, association request or deauthentication. To ensure that only one frame was transmitted, an attack tool was used to generate the frame, which was captured using airodump-ng. The single frame was then saved to a file and replayed using airtun-ng.

First, the aireplay-ng tool was used to generate an authentication request frame, with the two-byte authentication algorithm field set to "Open System" ($0x0000$). Then, an association request frame containing an RSN information element with CCMP support, which would be accepted by the AP, was obtained by running an authentication attack and recording the subsequent association request transmitted by the station. It is also possible for an attacker to construct a valid association frame from the information contained in the beacon frames broadcast from the AP. The authentication request and association request frames were constructed with the station MAC address as source and the AP MAC address as destination. Last, the aireplay-ng tool was used to construct a deauthentication frame with the AP MAC address as source and the station MAC address as destination.

Once the attack frames were generated, the experiments were performed by transmitting an attack frame once, then waiting for the station to regain connectivity. Once the station was back on-line, a new attack was launched, and this was repeated until a total of 100 attacks of each type had been carried out. All 802.11 frames to and from the AP were recorded for analysis.

6.3 Observations

Several significant results were observed while conducting the experiments.

First, as expected, the deauthentication attack did not work when MFP was enabled, but did work as expected when disabled.

Second, the authentication attack worked, both with and without MFP enabled. The station lost its network connection and had to reconnect.

Third, the valid association attack resulted in a permanent DoS when MFP was enabled. After excessive timeouts, the station interface was automatically assigned a link-local IPv4 address (169.254/16 prefix), and manual intervention was needed to get it back on-line.

6.4 Results

Once the experiments were completed, Wireshark[2] version 0.99.6 was used to analyze the results.

Deauthentication Attack. The deauthentication attack worked as expected. Figure 4 shows the expected and observed results when MFP was disabled. With MFP enabled, the attack had no effect, since the deauthentication notification was ignored by the station.

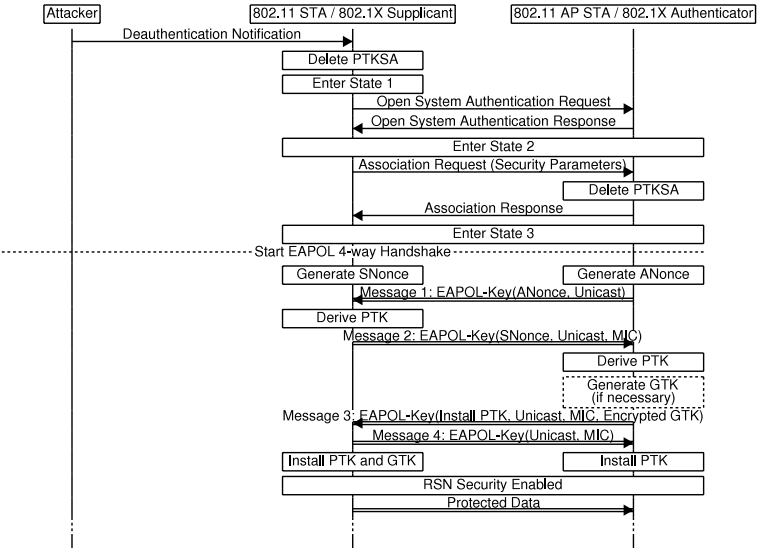

Fig. 4. Expected and observed results for the deauthentication attack with MFP disabled. The attack had no effect when MFP was enabled.

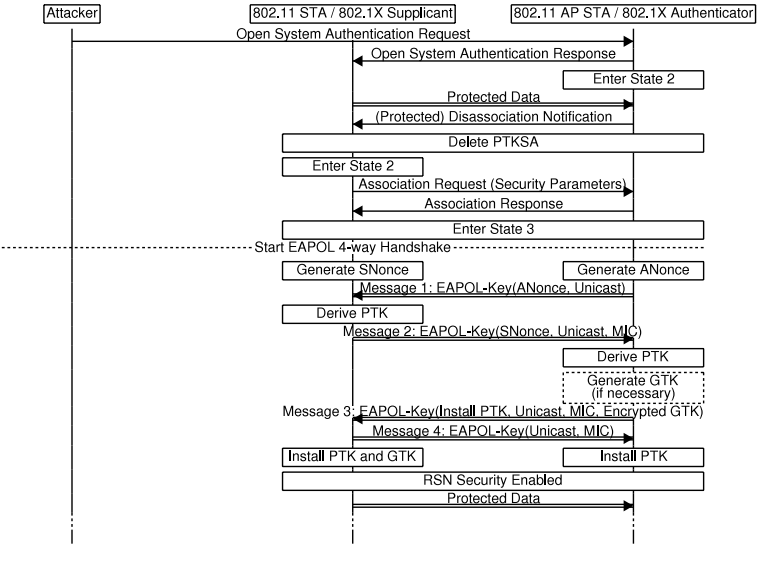

Fig. 5. Expected results for the authentication attack. The only difference between MFP enabled and disabled was that in the former case the disassociation notification was protected.

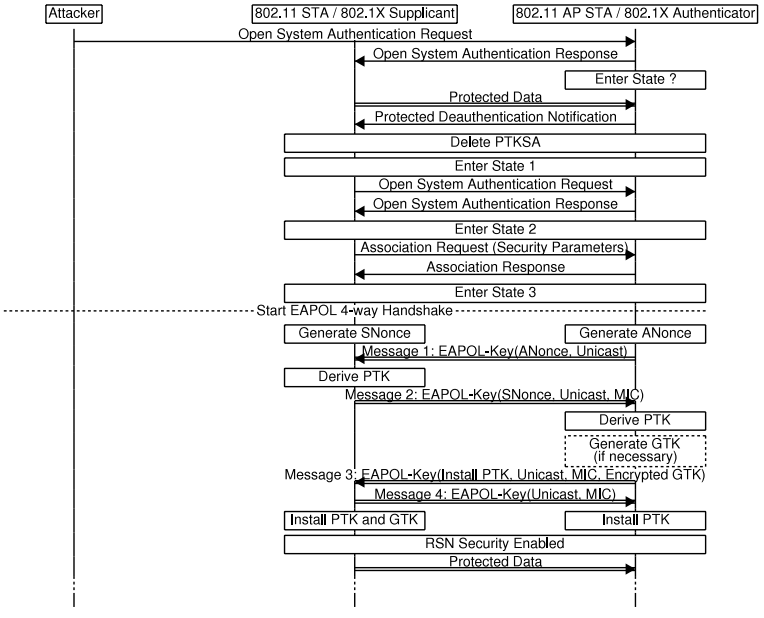

Fig. 6. Observed results for the authentication attack with MFP enabled. The AP responds with a deauthentication notification when it should have used a disassociation notification.

Authentication Attack. The results of the authentication attack were slightly different from the expected results. Figure 5 shows how the attack would work on an implementation that conforms to the standard.

The only difference between the expected and observed results were that the AP responded with a deauthentication notification when it should have used a disassociation notification. Figure 6 shows the observed results with MFP enabled. With MFP disabled, the only difference was that the deauthentication notification was not protected. The reason code in the deauthentication notification frame was "Class 3 frame received from nonassociated station (0x0007)", which confirms that the AP was in State 1 or 2 immediately after the attack.

SA Termination Attack. The results of the SA termination attacks were also as expected. Figure 7 shows the expected and observed results with MFP disabled. One interesting observation is that this attack is more efficient than any other known MAC layer DoS attack against 802.11 when RSN is enabled. In the experiment, the AP sent the first message of the EAPOL 4-way handshake, then waited for one second before retrying. This was repeated three times before the AKMP failed. The SA termination attach thus added three more seconds of downtime compared to the deauthentication attack.

Figure 8 shows the expected and observed results with MFP enabled. The station did not accept unprotected deauthentication notifications from the AP.

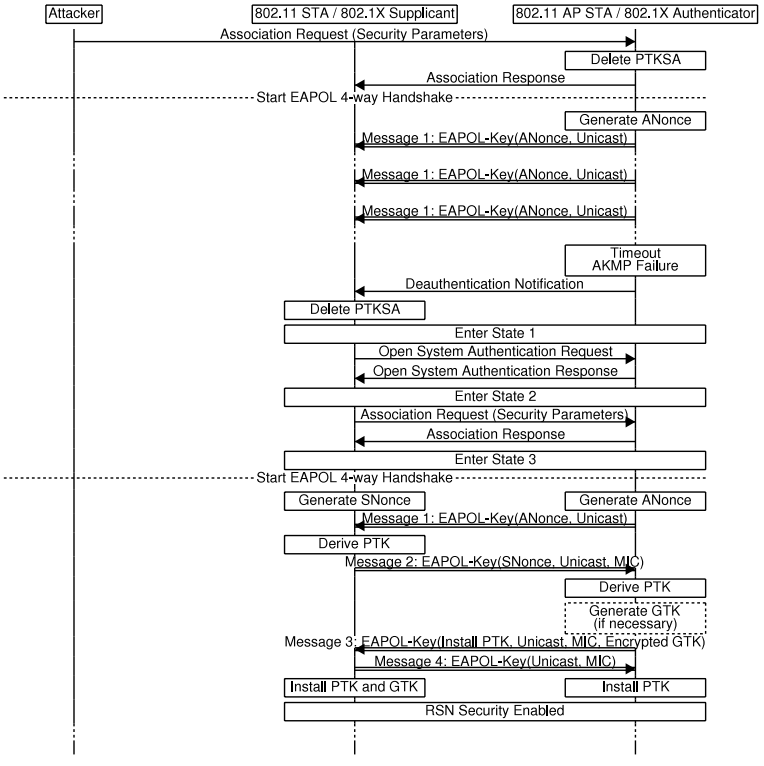

Fig. 7. Expected and observed results for the SA termination attack with MFP disabled. The failed 4-way handshake adds three seconds of downtime compared to a deauthentication attack.

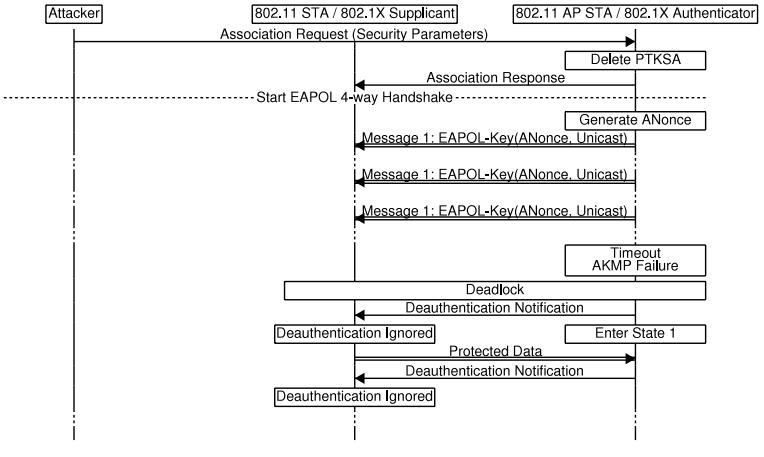

Fig. 8. Expected and observed results for the SA termination attack with MFP enabled. The result is a deadlock.

The end result was a deadlock, with manual intervention required to get the station reconnected.

7 Discussion

The results from the theoretical analysis and the experiments in the previous sections show that a network using 802.11w is vulnerable to the authentication attack. This attack has the same efficiency and feasability as a disassociation attack. 802.11w thus fails to protect against all DoS attacks that are equivalent to the deauthentication and disassociation attacks.

Introducing protected deauthentication and disassociation frames in 802.11w leads to a deadlock vulnerability. If the PTKSA in the AP is deleted while the station still has a valid PTKSA, then the station is not able to recover. This is the result of the SA termination attack. The proposed solution to this vulnerability by TGw is the SA Query procedure. This procedure has a weakness: an attacker who is able to delete messages or perform radio frequency (RF) jamming attacks will still be able to create a deadlock by sending an association request, then deleting the SA queries or perform RF jamming until the SA Query procedure times out. Message deletion in 802.11 networks is possible in the following way: the attacker listens for messages, then switches on the transmitter while the message is in transit to create a collision. Immediately after the collision, the attacker sends a MAC layer acknowledgment (ACK) to the sender. The sender thus assumes that the message was received, and no retransmission occurs. RF jamming attacks are even easier to perform. Since the association response from the AP contains the timeout value, the attacker knows exactly how long the jamming attack must last to result in a deadlock. The 802.11w drafts suggest a timeout value of around one second. An attacker can thus spend one second of RF jamming to permanently disconnect the station.

8 Proposal for a Robust Solution

The root cause of the DoS vulnerabilities in 802.11, both the previously known ones and the new vulnerability presented in this paper, is that 802.11 with amendments does not adhere to the first principle from [14]. The proposed solution adheres to this principle: To provide authentication from the very beginning. The challenge is how to do it, given the existing 802.11 standard with amendments. The creators of WEP did one thing right, their shared key authentication was performed as early as possible. This authentication, as well as the 802.11 open system authentication, is carried out using management frames of subtype authentication. Such frames have an important property, they contain an "Authentication Algorithm Number" field with a length of two bytes. Currently, only the values "0" (open system) and "1" (shared key) are used. This means that it is possible to add identifiers for new authentication methods.

Figure 9 shows the proposed authentication and key management procedure. The new authentication frame specification is the following: Add a new authentication algorithm number, "2", for RSN authentication. Add an RSN information

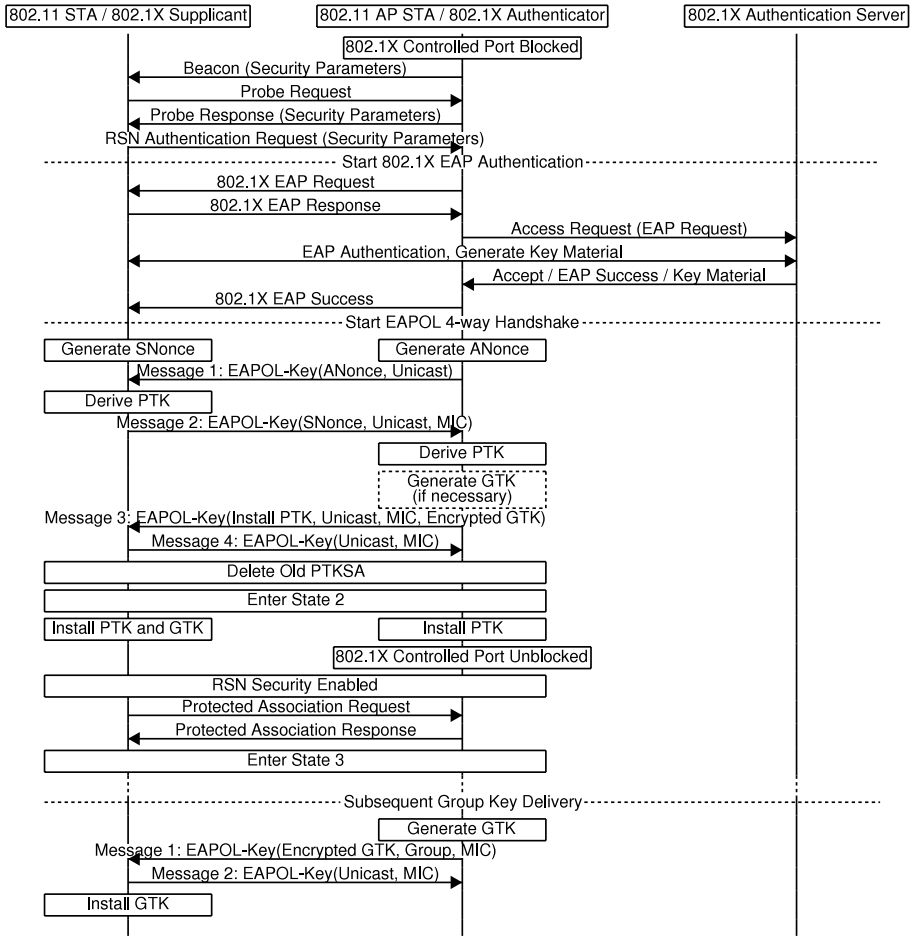

Fig. 9. The proposed solution for RSN authentication and key management. The authentication procedure is initiated when the station transmits an authentication frame with authentication algorithm number equal to 2 and a valid RSN information element. Management frames of subtype "authentication and key management" are used to encapsulate the 802.1X authentication messages, the 4-way handshake and the group key handshake. Note that the association request and response are protected.

element (security parameters) to the authentication frame. This enables the station to specify the authentication method and security parameters to be used in the authentication request.

The remaining issue is how to encapsulate the EAPOL messages used for authentication. This is solved by adding a new management frame subtype of Class 1, "authentication and key management". To remove all of the DoS vulnerabilities described in this paper, the 802.11i EAPOL authentication and key exchange messages are encapsulated in the authentication and key management frames, rather than in data frames. 802.11w should then be amended to also

provide protection for authentication and key management, association request and association response frames. Note that for backwards compatibility, the use of data frames to transport EAPOL messages must still be supported as defined in 802.11i.

Finally, to avoid deadlocks, the PTKSA should not be terminated after a successful association, disassociation or deauthentication, but rather be replaced with a new PTKSA after a successful 4-way handshake. If the protected association procedure fails, both the station and AP should perform the deauthentication procedure.

The construction outlined above can be backwards compatible with 802.11 with amendments, as noted. However, as long as backwards compatibility is preserved, the network will still be vulnerable to the authentication attack described in subsection 5.4. A transitional workaround for this is that the AP maintains a list of stations that have been successfully authenticated using the new authentication method, and that authentication requests for open system or shared key authentication for these stations are ignored. If backwards compatibility is discarded, this is not an issue, since an attacker will not be able to successfully authenticate.

9 Conclusion

All of the attacks presented in this paper were carried out using off the shelf hardware and freely available software. No software or hardware modification was necessary, so any person with access to a laptop computer and an Internet connection should be able to replicate these experiments or carry out actual DoS attacks.

Although the SA termination vulnerability from forged association frames has been addressed in recent draft versions of 802.11w, implementations of early drafts are still vulnerable. Until these have been updated, a network with 802.11w enabled is *more vulnerable* to DoS than a network without. Since the only purpose of 802.11w at the moment is to protect against DoS, a sound recommendation would be to disable it until a solution for this vulnerability is provided.

The SA Query procedure proposed as a solution to the SA termination vulnerability does not protect against an attacker who is able to delete messages or perform RF jamming attacks. Due to the severity of this vulnerability, the author strongly recommends that a more robust solution, such as the one proposed in section 8, is adopted.

The 802.11w drafts do not, as far as the author is aware of, address the authentication attack of subsection 5.4. If protection against all DoS attacks with efficiency and feasability equivalent to the disassociation attack is a goal of TGw, the proposed solution from this paper should be included in the 802.11w amendment.

Acknowledgements

The author would like to thank Stig F. Mjølsnes for valuable help and advice, Jing Xie for suggesting how to design a robust solution, and the anonymous reviewers of this paper for their helpful comments.

References

1. Aircrack-ng, http://www.aircrack-ng.org
2. Wireshark, http://www.wireshark.org
3. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP), IETF RFC 3748 (2004)
4. Bellardo, J., Savage, S.: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In: SSYM 2003: Proceedings of the 12th conference on USENIX Security Symposium (2003)
5. Bittau, A., Handley, M., Lackey, J.: The Final Nail in WEP's Coffin. In: SP 2006: Proceedings of the 2006 IEEE Symposium on Security and Privacy, pp. 386–400 (2006)
6. Epstein, J.: SA Teardown Protection for 802.11w, IEEE TGw DCN 2441, Rev 3 (2007)
7. Epstein, J.: SA Teardown Protection, IEEE TGw DCN 2461, Rev 8 (2007)
8. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. In: Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography, pp. 1–24 (2001)
9. The Institute of Electrical and Electronics Engineers, Inc.: IEEE Std 802.11-1999. IEEE, New York (1999)
10. The Institute of Electrical and Electronics Engineers, Inc.: IEEE Std 802.11i-2004. IEEE, New York (2004)
11. The Institute of Electrical and Electronics Engineers, Inc.: IEEE Std 802.11X-2004. IEEE, New York (2004)
12. The Institute of Electrical and Electronics Engineers, Inc.: IEEE P802.11w/D3.0. IEEE, New York (2007)
13. The Institute of Electrical and Electronics Engineers, Inc.: IEEE Std 802.11-2007. IEEE, New York (2007)
14. Meadows, C.: A Formal Framework and Evaluation Method for Network Denial of Service. In: IEEE Computer Security Foundations Workshop, p. 4 (1999)
15. Tews, E., Weinmann, R.P., Pyshkin, A.: Breaking 104 Bit WEP in Less Than 60 Seconds. In: Cryptology ePrint Archive, Report 2007/120 (2007)