A Practical Message Falsification Attack on WPA

Toshihiro Ohigashi[1] and Masakatu Morii[2]

[1] Hiroshima University, 1–4–2 Kagamiyama, Higashi-Hiroshima, 739–8511 Japan
ohigashi@hiroshima-u.ac.jp
[2] Kobe University, 1–1 Rokkodai, Kobe-ku, Kobe-shi, 657–8501 Japan
mmorii@kobe-u.ac.jp

Abstract. In 2008, Beck and Tews have proposed a practical attack on WPA. Their attack (called the Beck-Tews attack) can recover plaintext from an encrypted short packet, and can falsify it. The execution time of the Beck-Tews attack is about 12-15 minutes. However, the attack has the limitation, namely, the targets are only WPA implementations those support IEEE802.11e QoS features. In this paper, we propose a practical message falsification attack on any WPA implementation. In order to ease targets of limitation of wireless LAN products, we apply the Beck-Tews attack to the man-in-the-middle attack. In the man-in-the-middle attack, the user's communication is intercepted by an attacker until the attack ends. It means that the users may detect our attack when the execution time of the attack is large. Therefore, we give methods for reducing the execution time of the attack. As a result, the execution time of our attack becomes about one minute in the best case.

Keywords WPA, TKIP, falsification attack, man-in-the-middle attack

1 Introduction

Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) [1] is a security protocol for wireless LAN communication, and it provides confidentiality and integrity. WPA has been designed in order to fix weaknesses [2–5] of Wired Equivalent Privacy (WEP) [6], which is a past security protocol used in many wireless LAN products. WPA uses two kinds of keys, which are a 64-bit message integrity check (MIC) key and a 128-bit encryption key. The former is used to detect the message forgery/falsification, and the latter is used to encrypt/decrypt packets. These keys are generated from a shared master key.

The security of WPA has been analyzed by many researchers [7–9]. Moskowitz has shown a weakness on WPA against a dictionary attack [7]. He/she can avoid the weakness to generate the master key from a random and long passphrase. Most other analyses [8, 9] have evaluated components of WPA, and these are not effective attacks for threatening WPA.

In 2008, Beck and Tews have proposed a practical attack [10] on WPA implementations those support IEEE802.11e Quality of Service (QoS) features [11].

Their attack (called the Beck-Tews attack) can recover a MIC key and a plaintext from an encrypted short packet (e.g., ARP packet and DNS packet), and falsifies its encrypted packet using a recovered MIC key. The execution time of the attack is about 12-15 minutes. Since the Beck-Tews attack is a method based on the reply attack, the targets are required to support IEEE802.11e QoS features. Hence, their result is limited one.

In this paper, we propose a practical message falsification attack on any WPA implementation. Firstly, in order to ease targets of limitation of wireless LAN products, we apply the Beck-Tews attack to the man-in-the-middle (MITM) attack[3]. The Beck-Tews attack on the MITM attack is not required to support IEEE802.11e QoS features, it means that our attack can apply any WPA implementation. Secondly, we discuss an effective implementation of the MITM attack for the wireless LAN network. In the MITM attack, the user's communication is intercepted by an attacker until the attack ends. It means that the users may detect our attack when the execution time of the attack is large. Therefore, thirdly, we give methods for reducing the execution time of the attack. As a result, the execution time of our attack becomes about one minute in the best case.

2 Wi-Fi Protected Access

In WPA, a master key is shared between an access point and a client. The master key generate two kinds of keys, which are a 64-bit MIC key K^* and a 128-bit encryption key K. A 64-bit MIC is generated from a MIC key and a data, and it is used to detect the message forgery/falsification. An encryption key is used to encrypt/decrypt packets.

2.1 Processes of Sender

A sender calculates a MIC from a MIC key and a MAC Service Data Unit (MSDU) by using Micheal[1]. The MIC is added to the MSDU, as follows:

$$MSDU||micheal(K^*, MSDU), \tag{1}$$

where $micheal(K^*, MSDU)$ is a 64-bit MIC and $||$ is concatenation. The MSDU with the trailing MIC is fragmented into MAC Protocol Data Units (MPDUs). A 32-bit checksum is calculated from each MPDU by using CRC32, and it is added to the MPDU, as follows:

$$MPDU||CRC32(MPDU), \tag{2}$$

where $CRC32(MPDU)$ is a 32-bit checksum.

Encryption of WPA is executed for each MPDU with the trailing checksum. A packet key PK is generated from a 48-bit initialization vector (IV), an encryption

[3] Beck and Tews also have written about the summary of the Beck-Tews attack on the MITM attack in [10], however, it has not discussed the strategy, the implementation, and the evaluation of the attack yet.

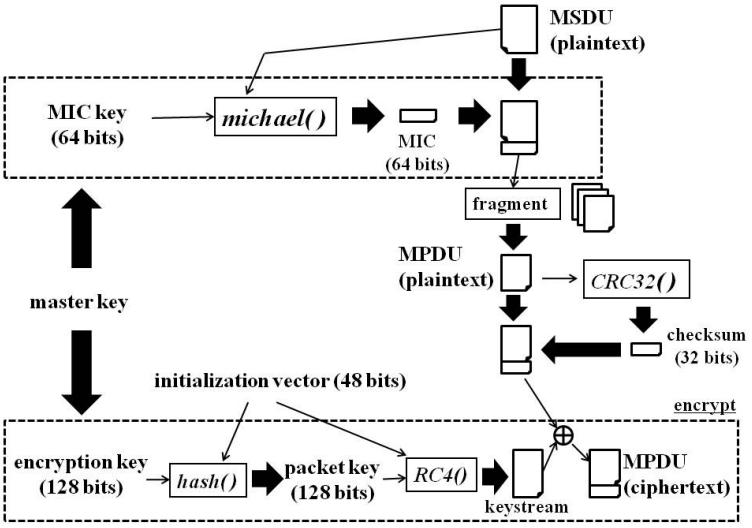

Fig. 1. Processes of sender on WPA

key K, and a MAC address by using a specific hash function for WPA $hash()$. IVs for each MPDU are different, and the value of the IV is incremented by one when the IV is generated newly. In WPA, the IV is called TKIP sequence counter (TSC). A stream cipher RC4 [12] is used as an encryption algorithm for WPA. RC4 generates a pseudo-random sequence (called a keystream) $Z = (Z_1, Z_2, \ldots, Z_L)$ from a packet key and an IV, where Z_i is a byte variable and L is the length of a plaintext. The keystream is XOR-ed with a plaintext $P = (P_1, P_2, \ldots, P_L)$ to obtain a ciphertext $C = (C_1, C_2, \ldots, C_L)$ as follows:

$$C_i = P_i \oplus Z_i \quad (i = 1, 2, \ldots, L), \tag{3}$$

where C_i and P_i are a byte variable, respectively. Then, the encryption of WPA is written as follows:

$$C = (MPDU||CRC32(MPDU)) \oplus RC4(PK, IV). \tag{4}$$

An encrypted MPDU and the IV are sent to the receiver. We show processes of sender on WPA in Fig. 1.

2.2 Processes of Receiver

The receiver receives an encrypted MPDU and an IV. The IV is compared with *the TSC counter*, which is a value of the IV corresponding to an encrypted MPDU accepted most recently. If the received IV is less than or equal to the

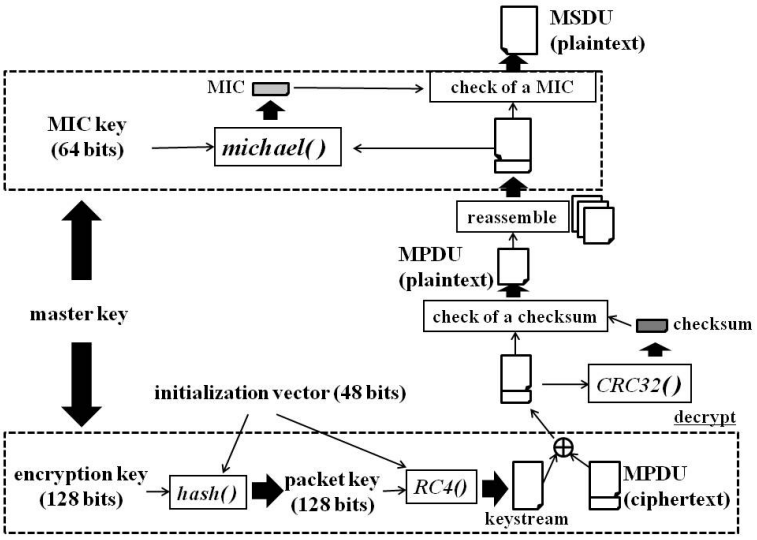

Fig. 2. Processes of receiver on WPA

TSC counter, the received encrypted MPDU is discarded. In the decryption of WPA, the receiver generates a keystream $\hat{Z}$ from a received IV and a packet key PK. The keystream $\hat{Z}$ is same as that of the sender Z. A plaintext P is obtained by using $\hat{Z} = Z$ as follows:

$$P_i = P_i \oplus Z_i \oplus Z_i = C_i \oplus Z_i \quad (i = 1, 2, \ldots, L). \tag{5}$$

Then, the decryption of WPA is written as follows:

$$(MPDU||CRC32(MPDU)) = C \oplus RC4(PK, IV). \tag{6}$$

The receiver calculates a checksum from the received MPDU, and the checksum is compared with the received checksum. If these checksums differ, the received MPDU is discarded. Note that the receiver does not send the error message of checksum to the sender.

When all MPDUs are obtained, these are reassembled to the MSDU. The receiver calculates a MIC from the received MSDU and the MIC key by using Micheal, and the MIC is compared with the received MIC. If these MICs differ, all the received MPDUs corresponding to the MSDU are discarded and the receiver sends the error message of MIC (a MIC failure report frame) to the sender. In WPA, the MIC key is changed if more than two error messages of MIC are sent to the sender in less than a minute. When the MSDU is accepted, the TSC counter is updated to the most larger value in the IVs corresponding to all the MPDUs. We show processes of receiver on WPA in Fig. 2.

3 The Beck-Tews Attack

The Beck-Tews attack [10] is a method that applies the chopchop attack [2] on WEP to the attack on WPA. This attack recovers a MIC key and a plaintext from an encrypted short packet, and falsifies its packet, practically.

3.1 The Chopchop Attack on WEP

The purpose of the chopchop attack on WEP is to obtain the information of a plaintext from a given ciphertext. Note that this attack cannot obtain an encryption key of WEP.

Processes of WEP are different from WPA as follows:

1. The value of IV is not checked.
2. There is not a process of adding a MIC.
3. The receiver sends the error message of checksum to the sender.

An falsified encrypted packet that is made from an encrypted packet accepted in the past is not discarded since the value of IV is not checked. Integrity check of a message is executed by only the checksum, and the receiver sends the error message of checksum to the sender if the checksum is incorrect.

The chopchop attack focuses on a property of CRC32. Let P be a MPDU with the trailing checksum, and R be the least significant byte (LSB) of P, namely R is the LSB of the checksum. Additionally, let P' be P truncated by one byte, namely it satisfies $P'||R = P$. P' will most probably have an incorrect checksum. In CRC32, we can modify the checksum of P' to a correct one by XORing the checksum of P' with $f(R)$, where $f()$ is an 1-to-1 byte permutation[4]. If the checksum of P' is XOR-ed with $f(R^*)$, the modified checksum is incorrect one, where R^* is a byte variable except the correct R. It means that a correct R can be identified from all 256 candidates of R by checking the error message of checksum of the modified P'. Assume that the attacker wants to know R. Then, the attacker make the modified P' for each candidate of R, and sends to the access point or client. If the guessed R is correct, the error message of checksum of the modified P' is not sent to the attacker. After at most 256 guesses and in average 128 guesses, the attacker has guessed the correct value of R. Above operation can also be done on the encrypted packet since the modification of a plaintext by XOR operation is executed easily in the encryption of the stream cipher.

When the chopchop attack is executed, the attacker can obtain the LSB of P, which is R, from ciphertext. Then, we can also obtain C', which is C truncated by one byte and has a correct checksum. When the attacker executes the chopchop attack for C', the 2-nd byte from the lower of P is obtained. In a manner similar to that, the low-order x bytes of P is obtained by executing the chopchop attack x times. Additionally, the attacker can obtain the keystream bytes corresponding to obtained information of P.

[4] The concrete equation of the permutation has been written in [10].

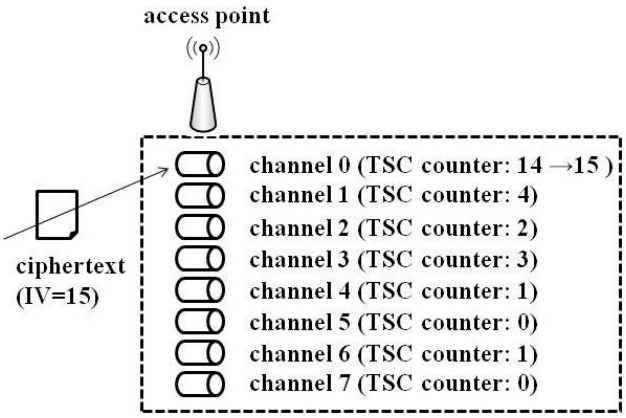

Fig. 3. A WPA implementation that supports IEEE802.11e QoS features

3.2 The Chopchop Attack on WPA

In WPA, a falsified encrypted packet that is made from an encrypted packet accepted in the past is discarded since the value of IV is checked. Beck and Tews have shown that the chopchop attack can be executed on WPA implementations those support IEEE802.11e QoS features in [10]. The IEEE802.11e QoS features allow 8 different channels for different data flows, and each channel has the TSC counter independently (Fig. 3). Suppose that an attacker has captured an encrypted packet with $IV = 15$ for channel 0. Then, the attacker cannot execute the chopchop attack on channel 0 since the TSC counter of channel 0 has been updated to 15. However, the attacker can execute the chopchop attack on the other channel if a TSC counter of the channel is less than 15.

When the error message of MIC is sent, all checksums of MPDUs are correct. Thus, the chopchop attack on WPA checks the guessed R is correct by using the error message of MIC. However, to execute the attack is difficult when the number of MPDUs is large. Then, Beck and Tews focus on the short packet (e.g., ARP packet and DNS packet). These packets do not cause the fragmentation, and the MPDU is concatenation of packet header/data, the MIC, and the checksum. When the attacker executes the chopchop attack x times, the execution time of the attack is required at least $x - 1$ minutes since the MIC key is changed if more than two error messages of MIC are sent to the sender in less than a minute. We call the time *the wait time for MIC error*.

3.3 Attack Scenario and Execution Time

We describe the Beck-Tews attack. The purpose of the Beck-Tews attack is not only to obtain the plaintext but also to recover a MIC key and to falsify its packet. Beck and Tews focus on ARP request/response packet as targets of the

attack. In [10], they discuss the attack under an assumption that bytes of an ARP packet are fixed or known values except the last byte of the source and destination IP addresses. That is, the number of unknown bytes of an ARP packet is 2. We also adopt same assumption in this paper.

Firstly, the Beck-Tews attack recovers a plaintext from an encrypted ARP packet. The number of unknown bytes of the plaintext is 14 bytes, namely that are 2 bytes of the ARP packet, 8 bytes of the MIC, and 4 bytes of the checksum. The attacker recovers the MIC and the checksum by executing the chopchop attack 12 times. This process requires at least 11 minutes for the wait time for MIC error. The unknown bytes of an ARP packet are recovered without the chopchop attack. The number of candidates for the unknown bytes of an ARP packet is 2^{16}, and the attacker can make 2^{16} candidates of the ARP packet. For each candidate of the ARP packet, the checksum is calculated using the MIC. The attacker compares the calculated checksum with the checksum recovered by the chopchop attack. If these checksums are not identical, the candidate of the ARP packet is removed. By the process, the candidates of the ARP packet reduce to one, and all the information of the plaintext is recovered from the encrypted ARP packet. Additionally, the keystream corresponding to the plaintext can be recovered.

Secondly, the Beck-Tews attack falsifies the encrypted ARP packet. To falsify the packet, the attacker obtains the MIC key. Since Micheal is an invertible function, the MIC key is recovered from the ARP packet and MIC easily. The attacker makes a falsified ARP packet, and calculates the MIC using the recovered MIC key and the falsified ARP packet. Then, the checksum is calculated from the falsified ARP packet and MIC. Finally, the attacker can make the encrypted falsified ARP packet using the keystram recovered by the Beck-Tews attack. According to [10], the execution time of the Beck-Tews attack is about 12-15 minutes. Most of the execution time of the Beck-Tews attack is the time for the wait time for MIC error.

In [10], Beck and Tews have shown an attack under a condition that a MIC key is obtained. Then, a MIC can be calculated from an ARP packet using the MIC key. The attacker recovers the checksum only by executing the chopchop attack 4 times. This process requires at least 3 minutes for the wait time for MIC error. The attacker makes 2^{16} candidates of the ARP packet, and can calculate the MIC using the MIC key in each candidate. For each candidate of the ARP packet, the checksum is calculated using the MIC. The attacker compares the calculated checksum with the checksum recovered by the chopchop attack. In a manner similar to the Beck-Tews attack without the MIC key, all the information of the plaintext is recovered from the encrypted ARP packet and can make the encrypted falsified ARP packet. According to [10], the execution time of the attack is about 4 minutes.

4 Our Attack

The Beck-Tews attack does not work WPA implementations those do not support IEEE802.11e QoS features. Then, we discuss a practical message falsification attack that works any WPA implementation. Firstly, we apply the Beck-Tews attack to the MITM attack in order to work any WPA implementation. Secondly, we give a strategy for attack and methods for reducing the execution time of the attack.

4.1 Man-In-the-Middle Attack

A condition for executing the chopchop attack on WPA is to obtain an encryption packet that the IV larger than the TSC counter has used. An solution for satisfying the condition is IEEE802.11e QoS features, but it reduces the range of the targets wireless LAN products. Thus, we present the approach based on the MITM attack as the other solution.

In the MITM attack, the attacker interrupts encrypted packets of the access point/client. In addition, the attacker falsifies the encrypted packet, and sends to the receiver, namely the client/access point. This attack can obtain an encryption packet that the IV larger than the TSC counter has used since the captured packet has not reached to the receiver. Thus, the chopchop attack can be executed on the MITM attack.

Figure 4 is a method for achieving the MITM attack in the wireless LAN network. An access point and a client cannot be communicated directly since the interval between these is large. The attacker behaves like a repeater, namely all packets that include SSID beacon are relaid to the receiver with no modification, and the packet of the access point/client delivers to the client/access point. If the attacker want to falsify an encrypted packet, the attacker relays the falsified packets. This method is not detected the user easily. We give a more effective model of the MITM attack in Fig. 5. In the model, the attacker sends the packet using directional antennas. Since the packet of the attacker does not reach the sender, the attack is not detected by the sender easily.

4.2 Strategy

In the MITM attack, the user's communication is intercepted by an attacker until the chopchop attack ends. Suppose that the attacker executes the chopchop attack using an encrypted packet with $IV = x$. If an encrypted packet with $IV = x+1$ is relaid to the receiver, then the chopchop attack using an encrypted packet with $IV = x$ cannot work since the TSC counter is updated to $x + 1$.

In order to reduce the influence of communication blackout, we introduce three modes for our attack as follows:

Repeater mode: The attacker relays to the receiver all packets that include SSID beacon with no modification, and the packet of the access point/client delivers to the client/access point.

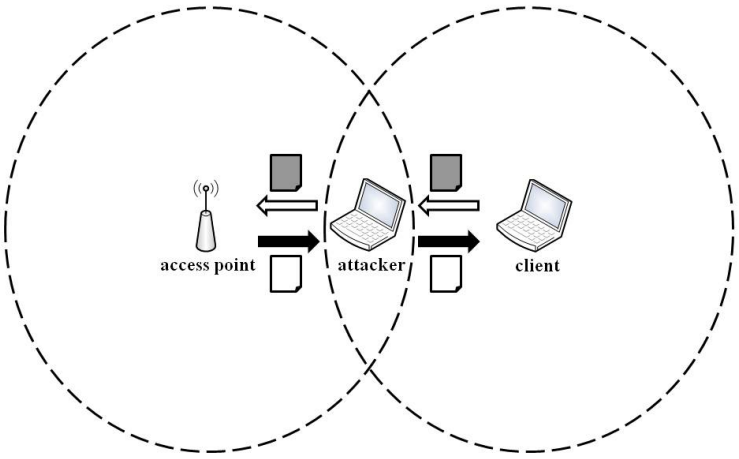

Fig. 4. A model of the man-in-the-middle attack

MIC key recovery mode: The purpose of this mode is to obtain a MIC key. A MIC and a checksum are recovered by the chopchop attack based on the MIM attack, and the MIC key is recovered. The execution time is about 12-15 minutes.

Message falsification mode: The purpose of this mode is to falsify an encrypted packet using a MIC key. When a target is an ARP packet, the execution time of the method in Sect. 3.3 is about 4 minutes. We discuss that the method for reducing the execution time of this mode in Sect. 4.3.

When the attacker does not execute the chopchop attack, the attacker executes the repeater mode. In this mode, the interruption of communication does not occur. The MIC key recovery mode is executed when the influence of communication blackout is small, for example most packets on the wireless LAN network are ARP packets. When an important packet, for example a packet of interactive application, has been sent on the way of the MIC key recovery mode, the mode is interrupted and the attacker executes the repeater mode. After a MIC key is recovered by the MIC key recovery mode, the message falsification mode is executed for falsifying an encrypted packet in a short time.

4.3 Reducing the Execution Time of the Attack

For the strategy of using three modes of our attack, the time of communication blackout by the attack reduces to about 4 minutes in the best case. In this

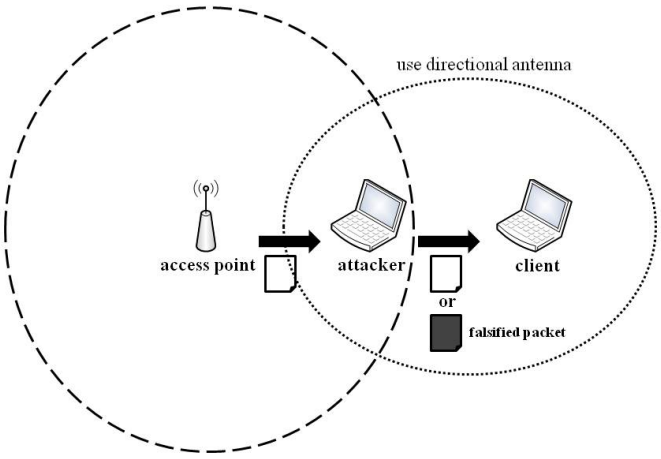

Fig. 5. A model of the man-in-the-middle attack with directional antennas

section, we give the method for reducing the time of communication blackout of the message falsification mode more.

Firstly, we focus on the information obtained from the MIC key recovery mode. When the attack of the MIC key recovery mode succeeds, the attacker can know the IP address of access point. In general, thus IP address of access point is fixed, then the unknown bytes of an ARP packet reduce to 1 byte.

Secondly, we give the method for reducing the execution time for the wait time for MIC error. The Beck-Tews attack recovers all the 4 bytes of the checksum, and the checksum is compared with the checksum calculated from candidates of the ARP packet. To compare 4 bytes of these checksum is effective to improve the success probability of the attack, but it requires at least 3 minutes for the wait time for MIC error. Thus, we adopt the method of comparing only parts of checksum in order to reduce the time of the wait time for MIC error. In our attack, we recover only the last byte of the checksum by the chopchop attack. This process does not require the time for the wait time for MIC error. Thus, the execution time of the message falsification mode of our attack is fewer than that of the Beck-Tews attack for three minutes, namely the execution time of our attack is about one minute.

We evaluate the success rate of our attack. In our attack of the message falsification mode, the number of candidates for the unknown bytes of an ARP packet is 2^8, and the attacker can make 2^8 candidates of the ARP packet. For each candidate of the ARP packet, the checksum is calculated using the MIC. The attacker compares the last byte of the calculated checksum with the last

byte of the checksum recovered by the chopchop attack. Suppose that the 8-byte MIC calculated by the candidate of the ARP packet and the MIC key is a uniformly distributed variable, then the probability that the last bytes of these checksums are not identical is $(2^8 - 1)/2^8$. When all the $2^8 - 1$ incorrect candidates are distinguished, our attack succeed. The probability that all the checksums of $2^8 - 1$ incorrect candidates of the ARP packet are not identical is given as follows:

$$\left(\frac{2^8 - 1}{2^8}\right)^{2^8 - 1} \sim 0.369. \tag{7}$$

Therefore, about 37% of the encrypted ARP packets are recovered by our attack with about one minute. Note that the encrypted ARP packet that recovered by our attack can be distinguished.

5 Conclusion

This paper has proposed a practical message falsification attack on any WPA implementation. Our attack is a method that applies the Beck-Tews attack to the MITM attack, and can falsify an encrypted short packet (e.g. ARP packet). We have given a strategy for the MITM attack and the method for reducing the execution time of the attack. As a result, the execution time of our attack becomes about one minute in the best case. Therefore, our attack can execute on any WPA implementation, practically.

The future works are the demonstration experiment for our attack and the evaluation of the detailed execution time of our attack.

Acknowledgements

This work was supported by MEXT KAKENHI (21700018). We want to thank Mr. Hajime Masaoka for his useful comments.

References

1. IEEE Std 802.11i-2004, "Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE, July 2004.
2. KoreK, "chopchop (Experimental WEP attacks)," 2004, available at `http://www.netstumbler.org/showthread.php?t=12489`
3. S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," Proc. SAC2001, Lecture Notes in Computer Science, vol.2259, pp.1–24, Springer-Verlag, 2001.
4. E. Tews, R. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," Cryptology ePrint, 2007, available at `http://eprint.iacr.org/2007/120.pdf`

5. R. Teramura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, "Breaking WEP with Any 104-bit Keys –All WEP Keys Can Be Recovered Using IP Packets Only–," Proc. of SCIS2009, CDROM, 1A2-6, Jan. 2009.
6. IEEE Computer Society, "Wireless lan medium access control (MAC) and physical layer (PHY) specifications," IEEE Std 802.11, 1999.
7. R. Moskowitz, "Weakness in Passphrase Choice in WPA Interface," 2003, available at `http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html`
8. V. Moen, H. Raddum, and K.J. Hole, " Weaknesses in the temporal key hash of WPA," ACM SIGMOBILE Mobile Computing and Communications Review, vol.8, pp.76–83, 2004.
9. "Re: DOS attack on WPA 802.11?," available at `http://www.mail-archive.com/cryptography@wasabisystems.com/msg03107.html`
10. M. Beck and E. Tews, "Practical attacks against WEP and WPA," 2008, available at `http://dl.aircrack-ng.org/breakingwepandwpa.pdf`
11. IEEE-SA Standards Board, "Wireless lan medium access control (MAC) and physical layer (PHY) specifications," Communications Magazine, IEEE, 2007.
12. B. Schneier, Applied Cryptography, Wiley, New York, 1996.