A lightweight solution for wireless LAN: letter-envelope protocol

Extended abstract

IEEE 802.11-based networks have been very successful because they only require inexpensive hardware devices operating on free spectrum with low cost deployment. Due to their popularity, 802.11 networks have been the target for a large number of attacks. Researchers and industrial companies have been trying to fix the vulnerabilities in 802.11 networks by proposing a number of protocols and standards (such as WEP, WPA, EAP, 802.11i, 802.1x). However, some flaws are still not addressed by any of these protocols, one of which is deauthentication/disassociation attack. We investigate a special type of denial of service (DoS) attack on 802.11-based networks, namely deauthentication/disassociation attack or Farewell attack. In the current IEEE 802.11 standards, whenever a wireless station (STA) wants to leave the network, it sends a deauthentication or disassociation frame to the access point (AP). These two frames, however, are sent unencrypted and are not authenticated by the access point. Therefore, an attack can launch a DoS attack by spoofing these message and thus disabling the communication between these wireless devices and their access point.

Farewell attacks. In [1], Aslam et al. describe an association process as a three steps process which four states:

(1) Unauthenticated and unassociated

(2) Authenticated and unassociated

(3) Authenticated and associated

(4) Authenticated, associated and 802.1x authenticated

Initially both STA and AP are in state (1). In order to join a network, a STA scans all channels to find an AP. After identifying the preferred AP, the STA and the AP perform mutual authentication by exchanging several messages. They can use *Open Authentication* or *Shared Key Authentication* [5]. Upon completion of the authentication, both STA and AP move to state (2). In state (2), the STA associates to the AP and both of them transit to state (3). In state (3), the STA can now send data packets to the AP. However, if the 802.1x protocol is supported, then the 802.1x authentication messages will be exchanged between the STA and the AP. On successfully finishing 802.1x authentication, both the STA and the AP move to state (4).

Note that, no receiving a disassociation message the state machine of the STA and the AP move back to state (2) no matter where they were in state (4) or state (3).

Similarly, on receiving a deauthentication message, the state machines transit to state (1). On receiving the disassociation and deauthentication frame, STA and AP clear the relevant states and keys in the memory. The deauthentication and disassociation frames are unauthenticated and unencrypted, thus are sources of persistent flaws in 802.11 networks.

To break the communication between STAs and their AP, an attacker can simply send out a spoofed deauthentication or disassociation frame. There are a number of tool that enable an attacker to spoof the source MAC address of any device, such as: Spoof-MAC, Airsnarf, Mac Changer. Note that attacker spoofs a deauthentication or a disassociation frame of AP with broadcast destination MAC address, the effectively all STAs associated to the AP will be disconnected.

The Farewell attack is simple but can cause serious damage, because the attacker can stop the communication using only limited resources without requiring any special technical skill. If the attacker sends a disassociation frame, the victim STAs must sent up a new association session with the AP. If the attacker sends a deauthentication frame, the victim STAs must perform a new authentication session with the AP in order to resume connectivity. In [2], Bellardo et al. implement the attacks and show that this attack is simple and effective.

There are a number of solution that have been proposed to defend against Farewell attack, as summarized in [1]-[4].

We develop a lightweight scheme for authenticating the management frames. However, instead of using sequence number, we use a one way function, thus our scheme is computationally infeasible to break. That means only the management frames send by legitimate STAs and APs are accepted. Our scheme does not depend on advance cryptographic primitives, thus all 802.11 devices can implement our solution via firmware upgrade.

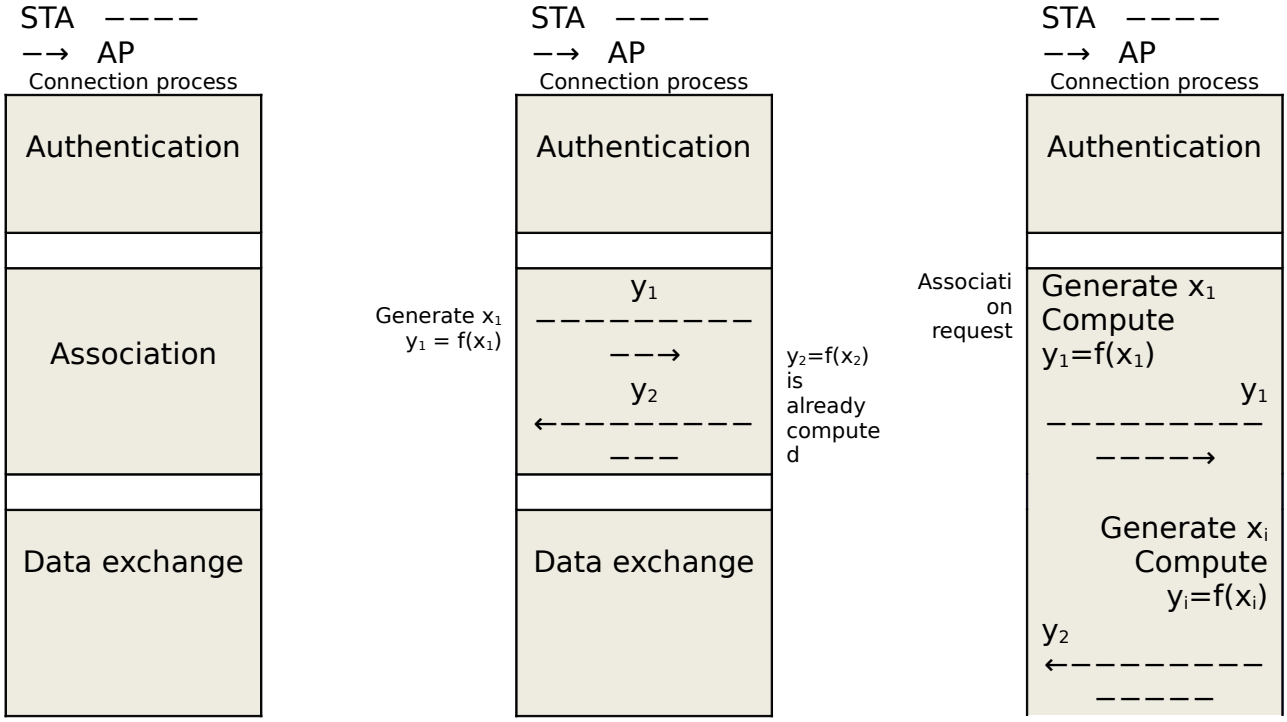
Letter-envelope protocol. We propose a lightweight authentication protocol, which we call “Letter-envelope” protocol that can defend against the Farewell attack. The protocol works based on a one-way function f(.): given $y = f(x)$, it is computationally infeasible to compute x; However, given x, it is easy to compute N. The Letter-envelope protocol is as follows:

- Initially, STA randomly generates x_1, then computes $y_1 = f(x_1)$. Similarly, AP generates x_2 and computes $y_2 = f(x_2)$.
- During the authentication process between STA and AP, STA sends an “envelope” that contains y_1 to the AP, and AP sends an “envelope” containing y_2 to the STA.
- When the STA wants to disconnect from the AP, it sends either the deauthentication or the disassociation frame to the AP, together x_1 to the AP;

we call this value “letter”. If this “letter” corresponds to the “envelope” previously, i.e. $f(x_1) = y_1$ then the frame is authenticated and will be processed accordingly. Otherwise, the frame is rejected.

- Similarly, if the AP wants to disconnect from the STA, it sends the disassociation/deauthentication frame together x_2. The STA disconnects itself from the AP if $f(x_2)=y_2$.

Implementation and experiments. We implement a simple system consisting of one AP, one STA and an attacker. We simulate one legitimate STA associating to the AP and one attacker trying to launch the Farewell attack using Comm View for Wifi (http://www.tamos.com/products/commwifi/) the legitimate STA and the AP both are installed with the modified Association protocol which implements “Letter-envelope” protocol (see Figure 1). We use a PC equipped with a wireless card to simulate the AP. The functionalities of this “AP” are exactly the same as other off-the-shell APs on the market. Our AP is deployed with two different authentication mechanisms: Open Authentication and Shared Key Authentication.



(a) Original Association

(b) Modified Association

(c) Modified Association (special case)

Figure 1: Association protocol

We use Madwifi-0.9.3.3 (http://madwifi.org/) for the STA and the AP. Madwifi-0.9.3.3: this is an open source device driver for wireless cards that use Atheros chipset running on Linux OS. We reprogram the device driver to make it work as a kernel module for the STA and the AP following 802.11 standards with the modified Association protocol.

The configuration of our system is as follows:

- One PC (CPU: Intel Celeron 3GHz, RAM: 1GB, HDD: 80GB) functioning as an AP.
- One PC (CPU: Intel Celeron 1.73GHz, RAM: 512MB, HDD: 80GB) functioning as a legitimate STA. this STA continuously sends ICMP ping packets to the AP to check the connection with the AP.
- One PC (CPU: Intel Core Duo 1.6GHz, RAM: 512MB, HDD: 80GB) running CommView for Wifi to launch the Farewell attack.

We conduct the experiment as follows. We continuously send deauthentication and disassociation frames with spoof MAC address of the STA (to the AP) and of the AP (to the STA) at rate 10 frames/second. If AP can detect the frame to be a spoofed frame, they will ignore the frame and will not disconnect the STA. otherwise it will disconnect the STA and clear information related to that STA in the memory.

The result of the experiments show that our solution is completely effective against the Farewell attack, none of the attacks is successful.

Extracted References

[1] B. Aslam, M. Islam, and S. Khan. 802.11 Disassociation DoS Attack and Its Solution: A Survey. In *Proceedings of the First Mobile Computing and Wireless Communication International Conference*, pages 221-226, Amman, Jordan, September 2006.

[2] J. Bellardo and S. Savage. 802.11 Denial-of-Service attacks: real vulnerabilities and pratical solutions. In *Proceedings of the 12th conference on USENIX Security Symposium*, pages 18-25, Washington, DC, 2003.

[3] E.D. Cardenas. MAC spoofing: An introduction. In *www.giac.org/pratical/GSEC.*

[4] Chibiao Liu. 802.11 Disassociation Denial of Service (DoS) attacks: *www.mnlab.csdepaul.edu/seminar/spr2005*.

[5] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang. Your 802.11 Wireless Network Has No Clothes. *IEEE Wireless Communications*, 9(6):44-51, December 2002.