Network Security
Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Week - 07
Lecture - 38
Securing Wireless LANs : Part 4

Hello, in this lecture, we will continue our discussion of 802.11i and WPA. So, we will now discuss the key derivation. Recall that the station and the access point agree upon the Pairwise Master Key (PMK), in one of two different ways. In the case of a corporate or university campus, an authentication server is used. So, in this case, the station and the authentication server may agree on the PMK during their mutual authentication.

The authentication server then conveys the PMK to the access point. So, this is the mode that is used in the case of large organizations, such as a university or a company. So, in those cases, an authentication server is used, and the station and authentication server agree on the PMK during their mutual authentication, and the authentication server then conveys the PMK to the access point. In the case of homes and small offices, the PSK mode is used, or the pre-shared key mode is used. So, in that case, the PMK is a function of the PSK, which is manually installed in the access point and the station.

So, through any one of these ways, the station and the access point agree upon the pairwise master key. What happens subsequently? This 256-bit PMK is then used to derive a 384-bit Pairwise Transient Key (PTK). In particular, the PTK is a pseudo-random function of the PMK and two nonces, one of which is chosen by the access point and the other nonce is chosen by the station. The PTK is also a function of the MAC addresses of the access point and the station.

So, MAC address stands for medium access control address. So, every node in the network has a unique MAC address. So, the PTK is a function of the MAC addresses of the access point and the station. So, this MAC is not to be confused with the message authentication code. So, this is the MAC address.

Now recall that the 256-bit PMK is used to derive a 384-bit Pairwise Transient Key (PTK). Three chunks of 128 bits each are extracted from the 384-bit PTK. These chunks are as follows. One is the temporal key that is used for encryption and message integrity protection of the data exchanged between the access point and the station after the authentication process. So, this is the most important key.

It’s used for the protection of the data packets that are exchanged between the access point and the station. It is used for encryption and message integrity. Then, the second chunk of 128 bits in length is the key confirmation key. It is used to integrity-protect some of the messages in the four-way handshake. The integrity protection is provided by a message authentication code that is computed as a function of the message and the KCK.

So, we’ll discuss the four-way handshake that takes place to derive the keys. So, this KCK is used to integrity-protect some of the messages in this four-way handshake, which we’ll discuss later on. And then the third chunk of 128 bits is the key encryption key. It is used to encrypt the message containing the group key in the four-way handshake. So, the group key is a key that is used to send broadcast messages securely.

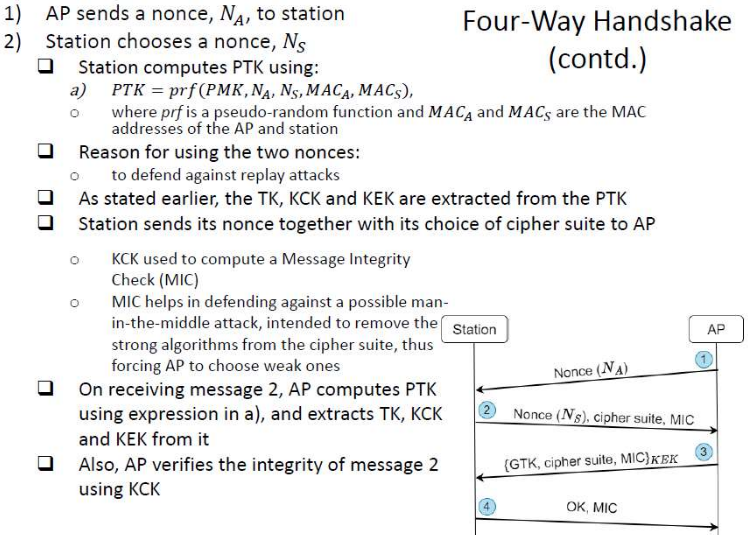
Broadcast messages are those which are sent from the transmitter to all the other nodes in the Wi-Fi network. So, for securing these broadcast messages, the group key is used. And the key encryption key is used to encrypt the message containing the group key in the four-way handshake. We now discuss the four-way handshake. The four-way handshake is performed between the station and the access point after they have agreed upon the PMK through one of the modes that we discussed earlier.

What are the objectives of the four-way handshake? So, the goals are as follows. One is to derive the PTK from the PMK. And another is to verify the cipher suites to be used in the subsequent data communication. Recall that the access point and the station select the cipher suite during the first phase or discovery of their mutual authentication.

So, in particular, the access point transmits a beacon in which the supported authentication and encryption algorithms are included. And then the station selects one authentication algorithm and one encryption algorithm from this list. So, the access point and station select the cipher suite during the first phase or discovery of their mutual authentication, but these have not been securely exchanged. So, there may have been some tampering in these selections. So, one of the goals of the four-way handshake is to verify the cipher suites that are used.

So, in the discovery phase, they exchange the possible algorithms, that is, the cipher suites, but these are later verified as part of the four-way handshake. The reason this is separately done is that initially they agree upon the cipher suite to be used, and later these are verified. The reason is that initially the access point and station have not agreed on any secret that both of them know. So, in particular, they have not agreed on the key to be used for message integrity. So, only after they have agreed upon the key to be used for message integrity can they send message authentication codes to each other and verify the integrity of the cipher suites that were earlier agreed upon as part of the discovery phase.

Another goal of the four-way handshake is to communicate the group key from the access point to the station. As we discussed earlier, the group key is used for securely sending broadcast messages. So, we now discuss the four-way handshake. So, this is illustrated in this figure. This is the station, and this is the access point.



Four-Way Handshake (contd.)

1) AP sends a nonce, N_A, to station
2) Station chooses a nonce, N_S
   - ❑ Station computes PTK using:
     - a) $PTK = prf(PMK, N_A, N_S, MAC_A, MAC_S)$,
       - o where *prf* is a pseudo-random function and MAC_A and MAC_S are the MAC addresses of the AP and station
   - ❑ Reason for using the two nonces:
     - o to defend against replay attacks
   - ❑ As stated earlier, the TK, KCK and KEK are extracted from the PTK
   - ❑ Station sends its nonce together with its choice of cipher suite to AP
     - o KCK used to compute a Message Integrity Check (MIC)
     - o MIC helps in defending against a possible man-in-the-middle attack, intended to remove the strong algorithms from the cipher suite, thus forcing AP to choose weak ones
   - ❑ On receiving message 2, AP computes PTK using expression in a), and extracts TK, KCK and KEK from it
   - ❑ Also, AP verifies the integrity of message 2 using KCK

Station
AP
1
Nonce (N_A)
2
Nonce (N_S), cipher suite, MIC
3
{GTK, cipher suite, MIC}$_{KEK}$
4
OK, MIC

So, in the first step, the access point sends a nonce to the station. We denote this nonce by N_A. Then, in the second step, the station chooses a nonce N_S, and the station sends the nonce N_S along with some other information to the access point. Now, at this point, the station knows the nonce of the access point, that is, the nonce N_A, as well as its own nonce, that is, N_S. Now, the station has obtained enough information to calculate the PTK.

The station computes the PTK using this function. The PTK is a pseudorandom function of PMK, N_A, N_S, MAC_A, and MAC_S, where 'prf' is a pseudorandom function, MAC_A is the MAC address of the access point, and MAC_S is the MAC address of the station. So, the PTK is derived from the PMK, nonces, and the MAC addresses. So, what is the reason for using the two nonces? So, the reason is the same as the reason discussed in the previous protocols that we discussed.

To defend against replay attacks, the nonce N_A defends the access point against replay attacks, and the nonce N_S defends the station against replay attacks. After the PTK is computed by the station, as stated earlier, the temporal key, KCK, and KEK are extracted from the PTK. So, the PTK is a 384-bit key, and TK, KCK, and KEK are 128 bits each. They are extracted from the PTK by the station. Then, as shown in this message, the station sends its nonce together with its choice of the cipher suite to the access point, and a message authentication code is added to it.

So, the KCK is used to compute a message authentication code. This MAC is known as the message integrity check, or MIC in Wi-Fi terminology, and this is to avoid confusion with MAC, or medium access control. So, to prevent confusion between medium access control and message authentication code, we use the term message integrity check or MIC instead of MAC. So, this KCK is used to compute a message integrity check. And that is used to detect any possible tampering in the nonce and the cipher suite.

So, we can see the role of the KCK. It is used to compute a MIC, which is sent from the station to the access point. So, the message integrity check helps in defending against a possible man-in-the-middle attack intended to remove the strong algorithms from the cipher suite and thus forcing the access point to choose weaker ones. So, any tampering in this cipher suite can be detected using the message integrity check in the usual way, that is, if m is the message, then the message integrity check is H(m, s), where s is the secret key KCK, and H is a cryptographic hash function. On receiving this message too, the access point computes PTK using the same expression as the station had used, that is, this expression in A.

So, the access point computes the PTK using this expression and then extracts the TK, KCK, and KEK from it. So, at this point, the access point has also obtained the same keys, TK, KCK, and KEK, which the station had derived earlier. Also, the access point verifies the integrity of message 2 using KCK. So, since the access point knows the KCK, it can compute the same message integrity check which the station had computed and verify whether it matches with the message integrity check that the station had sent. Then message 3 is sent from the access point to the station.

This message 3 contains the current Group Transient Key (GTK). And this GTK is encrypted using the KEK. The GTK is the key used by the access point and all stations to integrity-protect and also to optionally encrypt all broadcast messages. So, these broadcast messages, as we said earlier, are sent by the transmitter to all the other nodes in the network. Message 3 also contains the cipher suite that is chosen by the access point.

Message 3 is encrypted using the KEK and integrity-protected using the KCK. So, now we see the role of the KEK. It is used to securely send the GTK. So, since the GTK is a secret, it needs to be encrypted, and it is encrypted using the KEK. And the MIC is again computed using the KCK.

So, recall that the MIC in step 2 was also computed using the KCK. So, we can see that the KCK is used for MIC computation in steps 2, 3, and 4, as well, as we will see next. Message 4 is an acknowledgment from the station that it has received the previous messages without error. And also, the MIC is added to this message to prevent any tampering. So, this completes the four-way handshake.

After this four-way handshake is completed, all the messages are integrated, protected, and encrypted using the temporal key. After the four-way handshake, the station and the access point have a secret key shared between them, namely the temporal key, which can be used for integrated protection and encryption of the data messages exchanged subsequently between the station and the access point. As we said earlier, MAC is an abbreviation for message authentication code, but in the 802.11 standard, the term MIC is used instead of MAC to avoid confusion with medium access control. So, MIC is another name for message authentication code. It stands for message integrity check.

Now we discuss the pairwise master key and the temporal key. So, recall that the PMK and the exchange of two nonces, one in each direction, are used to create the temporal key, as well as the KCK and the KEK, and then the temporal key is used for encryption and message integrity. So, now a natural question is: why is the PMK itself not used for encryption and message integrity? So, the question is, should we use the PMK itself for encryption and message integrity or use a temporal key derived from the PMK and nonces? So, recall that it is insecure to use long-term keys for authentication for encryption and message integrity within each session.

So, we have discussed this during our discussion of authentication. It is more secure to generate a session key that is different for each session. The temporary key is a session key. Before every data exchange session, a new temporary key is generated, and it is discarded at the end of the session. So, the temporary key changes from session to session.

So, according to this principle, the temporal key is different for different sessions. Recall that the master secret or master key generated after the TLS authentication is a function of two nonces; hence, it is different for different sessions. So, as a result, if EAP-TLS is used for authentication in 802.11i, then the PMK is different for different sessions. So, since the PMK is different for different sessions, why not use the PMK itself as a session key for encryption and message integrity? Why is the temporal key derived from the PMK and two nonces?

So, the reason is that for authentication techniques other than EAP, TLS may be used, under which the PMK is the same for every session. For example, PSK may be used, or EAP with some protocol other than TLS may be used. So, in the case of PSK, we know that the PMK is the same for every session. So, hence, we cannot assume that the PMK is different for different sessions. So, hence, the PMK is combined with two nonces: one sent from the access point to the station and one sent from the station to the access point.

So, the PMK is combined with these nonces, and the temporal key is derived from the PMK and these nonces. This guarantees that the temporal key is different for different sessions. So, that's the reason for using a temporal key in addition to the pairwise master key. So, we discussed that an authentication server is used as part of 802.11i. So, one example of an authentication server is RADIUS, and Diameter is an improvement upon RADIUS.

So, there are different types of authentication servers. RADIUS, which stands for Remote Access Dial-In User Service, is a popular standard specified by the IETF, or Internet Engineering Task Force. The IETF is a standards organization that has standardized many of the protocols that are part of the TCP/IP protocol stack. So, RADIUS is a popular standard specified by the IETF. RADIUS defines the following:

One is a set of functionalities that a RADIUS authentication server should have. So, it specifies which functionalities the AS, or authentication server, should have, and RADIUS also defines a protocol that allows other devices, such as access points, to communicate with the RADIUS authentication server. So, RADIUS specifies not only the functionalities that the authentication server should have but also how other devices, such as access points, can communicate with the authentication server. RADIUS authentication servers can be used not only for Wi-Fi but also in other contexts. So, it can be used in the context of Wi-Fi, in particular 802.11i, and more generally in other contexts where users use some network service via devices called network access servers.

So, examples are dial-up and cloud computing. So, in the case of cloud computing, there is a gateway that is connected to the cloud, and users access the cloud through the gateway, and the gateway acts as a network access server. So, the network access server is the gateway through which some service is provided to users. So, in the case of cloud computing, the cloud computing service is provided to users through the gateway, and in the case of Wi-Fi, the network access server is the access point, and connectivity to the internet is the service provided through the access point. The case of dial-up is similar.

Internet connectivity is provided through a gateway in the case of dial-up as well. In the case of Wi-Fi, users are those who connect wirelessly using a laptop, mobile device, and so on, and access points are the network access servers. So, RADIUS is used in the case of Wi-Fi, but it is more general. It can be used in any context where there is a network access server, including dial-up and cloud computing. Many practical corporate networks use RADIUS servers, and Diameter is another standard for an authentication server, and it is an improved version of RADIUS.

So, Diameter is not an abbreviation, but it is derived from the term radius. So, since diameter is double the radius, it denotes that Diameter is an improved version of RADIUS. So, Diameter is another authentication server that can be used. So, in conclusion, we discussed 802.11i and we discussed different keys that are used, including PMK, PTK, temporal key, and so on. So, we discussed the four-way handshake, which is used to derive the keys that will be subsequently used.

And the four-way handshake is also used to confirm the security algorithms that are used for authentication and encryption. And we discussed the authentication servers and different types of authentication servers, including RADIUS and Diameter. Thank you.