Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 07
Lecture - 37
Securing Wireless LANs : Part 3

Hello, in this lecture, we will continue our discussion of securing wireless local area networks, in particular, Wi-Fi. Recall that in the previous two lectures, we discussed Wired Equivalent Privacy (WEP), which was the security standard included in the original Wi-Fi, introduced in the late 1990s. We discussed that WEP has several security flaws. In this lecture and the next few lectures, we'll discuss an improvement upon WEP, namely 802.11i. We will also discuss WPA or Wi-Fi Protected Access, which is an intermediate measure until the adoption of 802.11i.

So, 802.11i is also known as WPA2 or Wi-Fi Protected Access 2. So, these are the successive standards for Wi-Fi security named WPA, WPA2, and WPA3. WPA3 is the latest one. So, 802.11i is also known as WPA2, which stands for Wi-Fi Protected Access 2. So, Wi-Fi Protected Access, or WPA, became available in 2003, and it was intended as an intermediate or temporary measure in anticipation of the more secure and complex WPA2.

So, it is sometimes referred to as the draft 802.11i standard. So, at the time of adoption of WPA, WEP was widely deployed in many systems, and these hardware systems which implemented WEP could not implement WPA2, so WPA was used as an intermediate measure so that we could use the hardware of WEP to run a more secure set of mechanisms, that is, WPA. So, WPA was this intermediate measure which could operate with WEP. So, it was a temporary measure until the replacement of that hardware and the adoption of 802.11i or WPA2, which is more secure. 802.11i provides better security than WEP in the following respects.

One is that we discussed that WEP's encryption can be easily broken, but 802.11i provides stronger encryption than WEP. So, we discussed that in the case of WEP, the mobile device authenticates to the access point, but the access point does not authenticate to the mobile device. In contrast, in the case of 802.11i, there is mutual authentication; that is, the mobile

device and access point authenticate each other. 802.11i also provides a key distribution mechanism; that is, it provides a mechanism through which the access point and the mobile device can agree upon keys that will be used for encryption and message integrity. So, it uses public key mechanisms for key distribution.

We also saw that the message integrity of WEP can be easily compromised. So, in contrast, 802.11i provides stronger message integrity. So, in the case of 802.11i, in addition to the mobile device and access point, 802.11i defines an additional device known as the 'authentication server'. This authentication server has a secure connection with the access point, and the authentication server stores the secret information that's required for security mechanisms. For example, the authentication server may be a server that contains a username and password database.

So, the scenario is illustrated in this picture. This is the access point, which is communicating wirelessly with a mobile device known as STA or client station. So, this connection between the station and the access point is wireless. And this access point is connected over a wired network to the authentication server. And this connection between the access point and the authentication server is a secure connection.

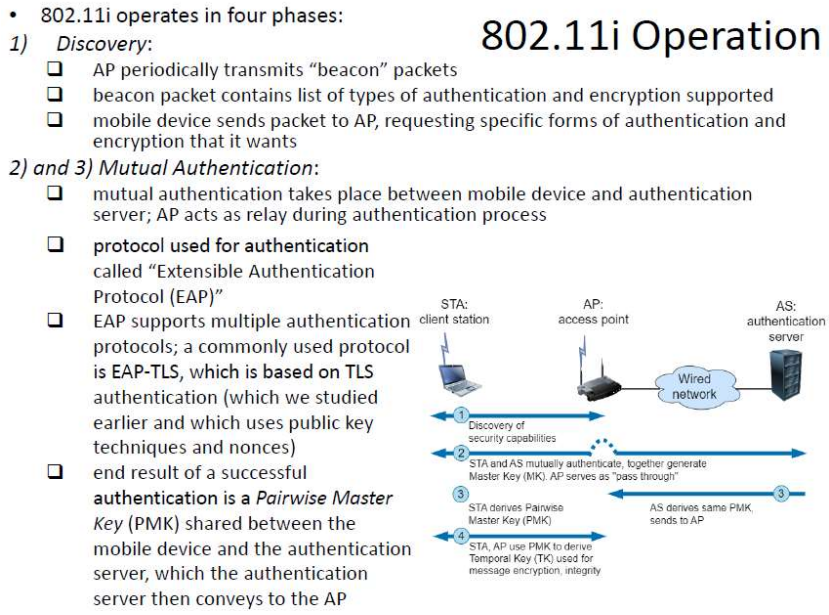
For example, it may be secured using IPsec. A typical way in which an authentication server is used is the following. A corporate or university campus may have an authentication server connected to its local area network, and the authentication server communicates over the LAN with all the access points in the campus. So, there is a single authentication server which is connected over the wired network to many access points in the LAN. So, typically to cover a LAN consisting of several square kilometers in area, we require a large number of access points, maybe several tens of access points or several hundreds of access points.

So, all those access points are connected over the wired network to a single authentication server. So, authentication takes place between the mobile device and the authentication server, and during this authentication process, the access point just acts as a relay. It just forwards messages from the authentication server to the mobile device and vice versa. So, the authentication actually takes place between the mobile device and the authentication server, and the access point just serves as a relay, which forwards packets from the authentication server to the mobile device and vice versa. So, what are the advantages of separating the authentication server from the access point?

Why not store the username and password, that is, all the secret information, in the access point itself? So, the advantages of using an authentication server are as follows. One is that the AP complexity and cost can be kept low. Because security information such as usernames and passwords need not be stored in the access point, which reduces the complexity and cost of the access point. Since there are typically a large number of access points in a LAN, the overall cost can be reduced significantly because each access point's complexity and cost gets reduced.

Another advantage is that the sensitive information and decisions regarding authentication are confined to only one entity, which is the authentication server. If this sensitive information were to be stored in every access point then if any one of those access points were compromised then the security would be compromised. So, this sensitive information is confined to only one entity, which is the authentication server, instead of being replicated at every access point. So, we don't need to defend the security of each and every access point. Instead, we just need to be careful about securing the authentication server, where the sensitive information is stored.

So, it becomes easier to secure the network because all the secure information is only at one location, that is, the authentication server. It is not replicated at each and every access point. So, these are the advantages of having a separate entity, namely the authentication server, which is responsible for security mechanisms. Now, we discuss the operation of 802.11i. 802.11i operates in four phases.



These phases are illustrated in this picture. Again, this is the mobile device, this is the access point, and this is the authentication server. And these phases are as follows. The first phase is the discovery phase, in which the mobile device discovers the security mechanisms that are available with this access point. The access point periodically transmits beacon packets.

So, these beacon packets are periodically sent by every access point, and the main purpose for sending these beacon packets is that mobile devices can scan different channels and discover the access points that are present in the vicinity. These beacon packets contain a lot of information about the network, which protocols the Wi-Fi network uses and so on. So, it contains information about the network. Using this information, mobile devices can connect to the access point. So, apart from some other information which is not related to security, the beacon packet in particular contains a list of the types of authentication and encryption supported.

For example, this access point may support an authentication protocol called EAP-TLS or another protocol called EAP-MD5. So, these are the authentication types supported. Similarly, it may support 3DES and AES as the encryption protocols. So, the beacon packet contains a list of types of authentication and encryption protocols supported. After the mobile device receives a beacon, it sends a packet to the access point requesting specific forms of authentication and encryption that it wants.

So, the mobile device selects the authentication scheme and the encryption scheme from the list of possible authentication and encryption schemes that is included in the beacon. And then the mobile device sends a packet to the AP requesting specific forms of authentication and encryption. Then steps 2 and 3 are for mutual authentication. In steps 2 and 3, the mobile device and the authentication server mutually authenticate each other, and the access point acts as a relay in these steps. So, mutual authentication takes place between the mobile device and the authentication server, and the access point acts as a relay.

The protocol used for authentication is called EAP, or Extensible Authentication Protocol. As we'll see, it is not a single protocol, but it is a framework that supports many possible authentication protocols. So, one of the authentication protocols in this framework can be used for authentication. So, EAP supports multiple authentication protocols. One commonly used protocol is EAP-TLS, which is based on the TLS authentication mechanism that we discussed earlier.

Recall that TLS authentication uses public key techniques and nonces. Similarly, this EAP-TLS also operates similar to the use of TLS. But EAP-TLS is not the only possible protocol. There are multiple authentication protocols supported as part of EAP. So, in steps 2 and 3, the mobile device and the authentication server mutually authenticate each other, and the access point acts as a relay.

So, at the end of this mutual authentication process, the end result is a pairwise master key (PMK) that is shared between the mobile device and the authentication server. And then, we have already mentioned that the access point is connected to the authentication server by a secure connection. The authentication server then conveys this pairwise master key (PMK) to the AP over this secure connection between the authentication server and the access point. So, at this point, the mobile device and the access point share a secret, namely the pairwise master key (PMK), which they can subsequently use to securely exchange data packets with each other. Then, the next step, which is step 4, is key generation.

In this step, the mobile device and the access point independently use the PMK and the exchange of two nonces, one in each direction, to derive the pairwise transient key. So, the role of the nonces is similar to that in the protocols we discussed earlier. These nonces are used to defend against replay attacks. So, the PMK and two nonces, one sent by the access point and one sent by the station, are used to derive a key known as the pairwise transient key (PTK). And from the PTK, the following keys are derived.

One is the Temporal Key (TK), which is used for data encryption and message integrity of the data packets that are exchanged between the access point and the mobile device after this 802.11i authentication process. So, the temporal key is used for encryption and message integrity of the data that is communicated between the mobile device and the access point. Then, two other keys are derived from the PTK. One is the Key Confirmation Key (KCK), which is used for message integrity of certain messages, and the other is the Key Encryption Key (KEK). So, we'll discuss these KCK and KEK later on.

So, we have discussed that in steps 2 and 3, mutual authentication takes place between the mobile device and the authentication server, and the protocol uses EAP. So, EAP is not a single authentication protocol, but rather it's a framework that supports various authentication protocols. So, we'll discuss some examples of the authentication protocols that are part of EAP. Some examples are EAP-MD5, EAP-TLS, and EAP-TTLS. In the case of EAP-MD5, the authentication server challenges the station to transmit the MD5 hash of the user's password.

The station prompts the user for the password and sends its hash to the authentication server. So, if the hash of the password is correct, then the authentication is successful. But this protocol is insecure because an attacker can eavesdrop on this message exchange and obtain the hash of the password. Later on, the attacker can replay the hash password and impersonate the legitimate user. Since the hash is sent in plain text form, an eavesdropper can intercept the hash and later authenticate itself fraudulently.

So, EAP-MD5 is one of the protocols supported in EAP, but it is not secure. Another limitation of EAP-MD5 is that authentication is one way. The authentication of the server to the station is not done as part of EAP-MD5. Then another protocol that's part of the EAP framework is EAP-TLS. It's based on the SSL or TLS protocol, which we discussed earlier.

So, of all the EAP methods, this is the most secure one. It provides mutual authentication and agreement on the master key. It provides agreement on the master key, which is the PMK, pairwise master key. It requires the authentication server as well as the user or the station to have digital certificates. So, we discussed digital certificates earlier.

One feature of EAP-TLS is that, unlike most implementations of TLS used to secure HTTP, which we discussed earlier, in the case of EAP-TLS, client-side certificates are mandatory. So, even the mobile station needs to have a certificate for its public key. So, this requirement makes EAP-TLS highly secure because it's not enough to have a compromised user password to break its security. There is another secret with the user that is the private key, which corresponds to the public key in its certificate. So, because of this requirement, EAP-TLS is highly secure.

There are certificates at the user side as well as at the authentication server side. So, it's relatively straightforward to equip the authentication server with a digital certificate and a corresponding private key. In particular, there is only one authentication server for an entire LAN, so we can easily provide a public key for the authentication server. But assigning a public key and private key pair to each user in the network may not be feasible. There may be hundreds or thousands of users, such as students, employees, and so on, in our network.

So, assigning a public key and private key pair to each user may not be feasible. Hence, users don't have certificates. This makes it difficult to use EAP-TLS in practice. So, a variant of EAP-TLS which overcomes the need to use certificates at the users is EAP-TTLS (EAP Tunnelled TLS). So, in this case, the users don't need to have certificates.

So, EAP-TTLS is similar to EAP-TLS. The difference is that a certificate is only required at the authentication server end. The user doesn't need to have a certificate. The server authenticates itself to the station using its public key-private key pair, and then both sides construct a secure tunnel between themselves. So, this is similar to the operation of TLS, which we discussed in an earlier lecture.

So, in that case, the server authenticates itself to the station, and a secure tunnel is constructed between them. For example, the station may encrypt one secret using the public key of the server and send it to the server. So, using this secret, a secure tunnel is constructed, or alternatively, ephemeral Diffie-Hellman is another way in which the secure tunnel may be constructed. Now, over the secure tunnel, the station authenticates itself to the server by sending its username and password. So, earlier, the server has already authenticated itself to the station.

In this step, once the secure tunnel is created, the station authenticates itself to the server by sending its username and password. Most users, such as students and employees, have usernames and passwords, so they can be used for authentication. These are some examples of the authentication methods that are supported by EAP. Now, there is another mode in which 802.11i can be used, and that is the PSK mode. So, the procedure that we discussed above, using an authentication server, is typically used in large 802.11 networks, such as those deployed in university and corporate campuses.

So, for 802.11i networks deployed in homes and small offices, a different and simpler procedure is often used. That is the PSK mode. It stands for pre-shared key mode. In the case where PSK mode is used, there is no use of an authentication server. Instead, shared keys, that is passwords, are manually installed in access points and provided to the users of mobile devices.

So, this is how 802.11i is used in a typical home, for example. The access point is manually configured with a password, and the people who reside in the home know the password. In case a guest visits them, they share the same password with the guest. So, these passwords are manually configured in the mobile devices, and these passwords are also manually installed in the access points. The pairwise master key (PMK) is a function of the PSK, and it is computed independently by the mobile device and the access point. So, when using the PSK mode, after computation of the PMK, the following steps are used.

The mobile device and the access point use the PMK and the exchange of two nonces, one in each direction, to derive the pairwise transient key. And after this, the process is similar

to that with an authentication server. That is, the temporal key, KEK, and KCK are derived from the pairwise transient key. So, after computation of the PMK, the mobile device sends a nonce to the access point, and the access point sends a nonce to the mobile device. So, these are again used to defend against replay attacks.

And then, using the PMK and the nonces, a pairwise transient key is derived, and then the temporal key, KEK, and KCK are derived from the pairwise transient key. So, this is as in the authentication server mode. And subsequent to the derivation of these three keys—temporal key, KEK, and KCK—the process used is identical to that used in the case of an authentication server. So, the difference only lies in the fact that the PMK is derived differently in the case of the PSK mode. It is derived from a pre-configured PMK and the exchange of nonces.

That's the difference between the PSK mode and the use of an authentication server. In summary, we introduced 802.11i as well as WPA, which was an intermediate measure. So, we discussed the use of an authentication server, and we discussed the operation of the authentication process in 802.11i, which consists of four steps. And we discussed an alternative technique, which is an alternative to the use of an authentication server, namely the PSK mode, or pre-shared key mode. We'll continue our discussion of 802.11i in the next lecture.

Thank you.