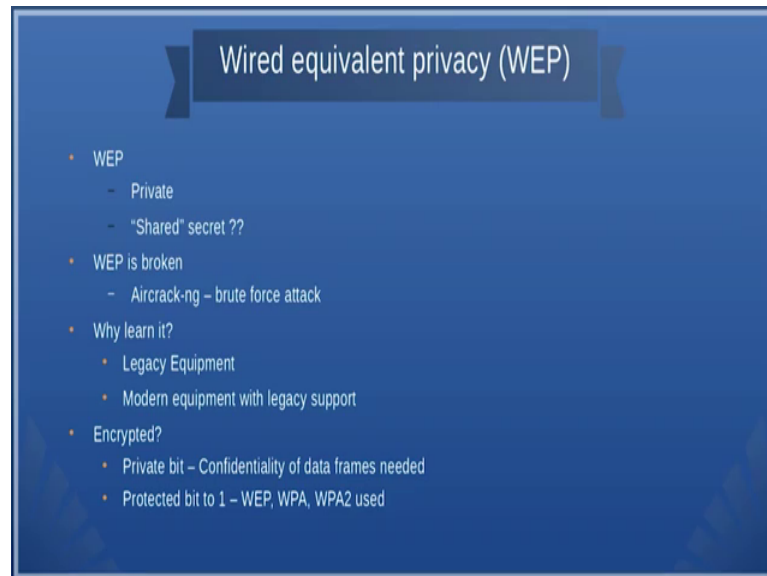


Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 44
Wireless Network Security Framework

(Refer Slide Time: 00:14)



Wired equivalent privacy (WEP)

- WEP
 - Private
 - "Shared" secret ??
- WEP is broken
 - Aircrack-ng – brute force attack
- Why learn it?
 - Legacy Equipment
 - Modern equipment with legacy support
- Encrypted?
 - Private bit – Confidentiality of data frames needed
 - Protected bit to 1 – WEP, WPA, WPA2 used

Any wireless media accesses to provide interconnection equivalent to a wired network. So, which essentially means in wired network, I could form private nets, ok, for example, I can if there are n computers in this room, I will be able to connect them through a LAN network. So, similarly in wireless, we use something known as wired equivalent privacy, most of you will be aware of this because you have to give a shared secret. So, it is called as a shared secret, I mean if a secret I shared, then it is no longer a secret. Therefore, but it is called a shared secret.

Now, the idea behind shared secret is I will be able to identify the access point to which I can connect myself. So, each our access point is grouped together using a certain name and those devices that connect to the access point using a particular name form a sort of private network ok, but the idea is the web; does it provide any security feature ok.

So, if the shared secret is known, then even attacker who knows about the shared secret can actually login to your network, and web is actually broken because you can actually use brute force attack, there is a tool open source tool called air crack ng which actually

store uses stored passwords, ok, commonly used passwords and it also uses brute force mechanism to join into a particular network, but then why should we learn about this because many of the legacy equipments still use wired equivalent privacy and this implies that there is a there is going to be a security loop hole in any organizational network that uses web.

So, current equipments of course, tell you that web is not secure and. So, they ask you to move to other advanced forms like WPA or WPA2, but then you will be having legacy equipment and if the modern equipments that you use have to support legacy, then this loop hole will still remain.

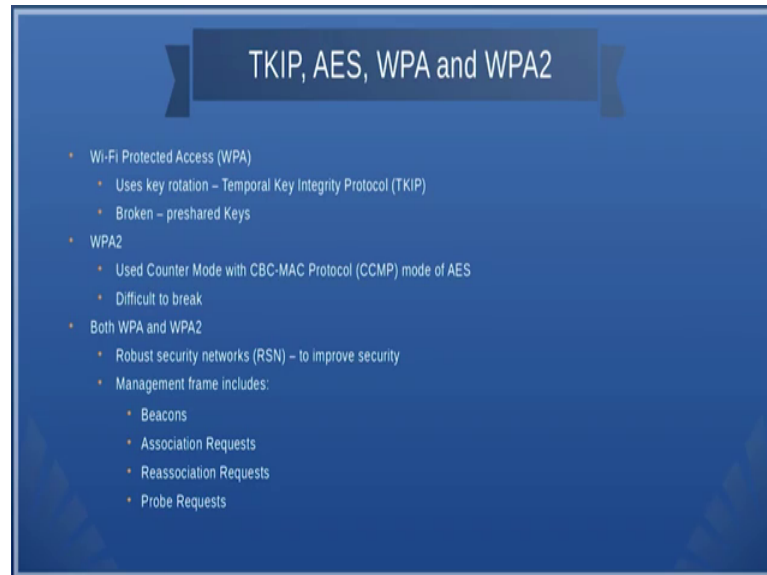
So, how does one identify whether the packets that traverse in a wireless network is encrypted or not, ok. So, there are two bits that you can actually see, one is called the private bit, if it is set to one, then the confidentiality of data frames are needed. So, and there is something known as protected bit ok. So, if you want to see this, just open wire shark and then capture a wireless frame and then take a look at it, it tells you; what type of security is used I mean if its protected bit is used, then it talks about either you can use ae as based WPA2 or WPA, etcetera.

Now, what are these next set of advanced standards that are much better than web, those were configured wires routers will be aware of this the next step that these people took was Wi-Fi protected access or WPA and what it does it uses key rotation, it uses a initialization vector and then because it uses a initialization vector a data can be encrypted much better, but the problem is that the initialization vectors number of bits that is used is limited and because the bits is limited and there are lot of packets that traverse wireless network because of a retransmissions a b, I mean the wireless medium itself is pruned to collisions unlike Ethernet, in wireless, you are pruned to lot of collisions and see it kind of noise that can happen in a wireless network.

So, all these things ensure that there are more packets that traverse the wireless network and if there are more packets that traverse the wireless network, then this initialization vector which is a specific number of bits, I think it is around 24 bits and. So, these have to repeat again and again and again and once something repeats an attacker will be able to identify the patterns and then break the network.

So they used so then they brought in slightly more secure and which is difficult to break kind of a standard like WPA2, ok, it uses something known as counter mode with CBC-MAC protocol; CCMP mode of advanced encryption standard ok.

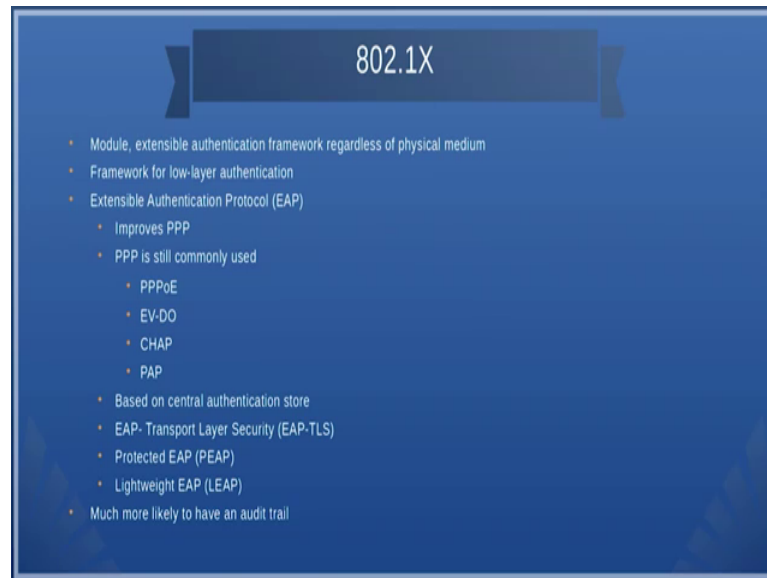
(Refer Slide Time: 04:49)



So, cyber block chaining I mean those are done course on network security know about what is cyber block chaining, ok. So, use of counter mode with CBC and CCMP ensure that your protocol was almost very secure and both WPA and WPA two use something known as robust are called robust security networks it uses a field called RSN and this RSN is part of the management frame and it gives information about the b cons ok, the association request the re association request the prob request, etcetera.

So, in this way if you take WP WEP, it was made more secure by adding WPA2, I mean these are actually you can call it as enhancements based on what people learnt and in this way security was enhanced, but the whole point is that wireless networks still are not secure coming to the next protocol, ok.

(Refer Slide Time: 05:53)



So, what they did was; so, can we enhance this wireless security much more. So, what they actually did was they introduced 802 dot 1 x where if you know about the networking theory you will be aware of protocol called PPP point to point protocol, this is actually a framework of protocols which can be used for authentication authorization, etcetera, ok.

So, what happened is that with 802 dot 1 x ok, they brought in modular and then extensible authentication framework regardless of the physical medium in which you were working. So, even though point to point protocol initially was serial ports or serial point to point communication links, what we can do is that whenever I establish a communication with one other medium ok, it does not matter that medium is shared, I can always go in for a hand shake ok, they use known as something known as a hand shake protocols and I can just once only when a authenticate, I can just get logged into that network.

So, this is a kind of framework that is provided by 802 dot 11 x ok. So, PPP is still commonly used over many of the protocols, I mean PPP is a framework, as I told you and in this framework many protocols like challenge hand shake authentication protocol like chap ok, password authentication like PAP and EVDO and PPPoE, Ethernet and all those things ok, all these things can be done. So, PPP is a kind of a protocol that sits on top of the basic medium and essentially can be used for authentication ok.

Later on, I mean companies like Cisco, they brought in their own kind of authentication protocols like protected EAP, EAP, then EAP-TLS, extensible authentication protocol TLS and then lightweight authentication protocol and so on and the advantage the great advantage of using these kind of 802 dot 1 x kind of protocols is that it can actually take the logs and then it can establish a trail of what has happened because authentication packets have to traverse. So, the network and you can capture those authentication packets and if there is any failure, you will be able to log the failure request. So, that is one of the greatest advantage of using this kind of protocols.

So with that; we actually end the session on the protocol part of it. Now, we will talk something on the device part ok, we will be talking about the access points in general in the next session.

Thank you.