Institute of Public Administration
Communication and Network Security
Group 1
Homework (3) Solution

Question (1)

Discuss how to deal with media access in wireless network and wired network.

Solution:

Media access in wireless networks is fundamentally different from the media access mechanisms in wired networks, where one has to hook up a computing device to a network cable for transmitting and receiving data, and the cables are physically protected by walls, ceilings doors, pipes, and other forms of physical structures.

Thus, how to provide wired equivalent media access in wireless networks becomes a unique security issue.

Question (2)

Discuss the evolution and the purpose of WEP security protocol.

Solution:

The WEP protocol, published in 1999, is the security component at the data-link layer of 802.11b.

WEP requires that all STAs and APs in the same WLAN share the same preset secret key K, referred to as the WEP key, and a WEP key may be 40-bit or 104-bit long.

Some WEP products may even support 232-bitWEP keys.

WEP allows each WLAN device to share more than one WEP key, and WEP keys are identified using a 1-byte key ID, denoted by key ID.

WEP does not specify how to generate or distribute secret keys. Thus, secret keys are often selected by the system administrator and distributed using land-line communications or other methods. In general, WEP keys are not changed once they are installed.

Question (3)

What are the major objectives of WPA protocol?

Solution:

The first objective is to correct all the security problems found in WEP.

The second objective is to make the existing hardware that supports WEP also support WPA.

The third objective is to ensure that WPA is compatible with the 802.11i standard to be announced.

Question (4)

What is the IEEE 802.11i standard?

Solution:

802.11i defines a counter mode-CBC MAC protocol (CCMP) using AES-128 to encrypt data and compute the MIC of the data. 802.11i also uses 802.1X to authenticate STAs.

Question (5)

Discuss the definition of Bluetooth technology.

Solution:

Bluetooth is a communication technology for building ad hoc WPANs. It allows wireless devices with low power, for example, cellular phones, PDAs, and embedded systems, to communicate with each other within a short range.

The IEEE 802.15 standard for WPANs is based on the Bluetooth technology.

Question (6)

Define the Zigbee protocol?

Solution:

The ZigBee protocol is a standard for low-power wireless personal area networks similar to Bluetooth.

The protocol is built on top of the IEEE 802.15.4 communications standard. Devices powered by the ZigBee protocol are widely used in health monitoring devices, home security systems, and home automation systems, to name just a few.

Question (7)

What is the difference between WLANs and WMNS networks?

Solution:

WLANs are star networks and WMNs are multihop networks.