### 

### [**3413ICT Network Security**](file:///D:\Profiles\user\My%20Documents\Teaching\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop – 9A**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Review Questions:**   1. Explain the functions of the following layers of IEEE 802.11 protocol: logical link control layer, MAC layer, and physical layer.   LLC (**Logical Link Control Layer**): In most data-link control protocols, the data-link protocol entity is responsible not only for detecting errors using the CRC, but for recovering from those errors by retransmitting damaged frames. In the LAN protocol architecture, these two functions are split between the MAC and LLC layers. The MAC layer is responsible for detecting errors and discarding any frames that contain errors. The LLC layer optionally keeps track of which frames have been successfully received and retransmits unsuccessful frames.  **MAC Layer: (**MEDIA ACCESS CONTROL***)*** All LANs consist of collections of devices that share the network’s transmission capacity. Some means of controlling access to the transmission medium is needed to provide an orderly and efficient use of that capacity. This is the function of a **media access control (MAC)** layer. The MAC layer receives data from a higher-layer protocol, typically the Logical Link Control (LLC) layer, in the form of a block of data known as the **MAC service data unit (MSDU)**. In general, the MAC layer performs the following functions:  • On transmission, assemble data into a frame, known as a **MAC protocol data unit (MPDU)** with address and error-detection fields.  • On reception, disassemble frame, and perform address recognition and error detection.  • Govern access to the LAN transmission medium.  The exact format of the MPDU differs somewhat for the various MAC proto- cols in use. The fields of this frame are as follows.   * **MACControl:** protocol control information needed for the functioning of the MAC protocol. For example, a priority level could be indicated here. * **Destination MAC Address:** The destination physical address on the LAN for this MPDU. * **Source MAC Address:** The source physical address on the LAN for this MPDU. * **MAC Service Data Unit:** The data from the next higher layer. * **CRC:** The cyclic redundancy check field; also known as the Frame Check Sequence (FCS) field. This is an error-detecting code, such as that which is used in other data-link control protocols. The CRC is calculated based on the bits in the entire MPDU. The sender calculates the CRC and adds it to the frame. The receiver performs the same calculation on the incoming MPDU and compares that calculation to the CRC field in that incoming MPDU. If the two values don’t match, then one or more bits have been altered in transit.  The fields preceding the MSDU field are referred to as the **MAC header**, and the field following the MSDU field is referred to as the **MAC trailer**. The header and trailer contain control information that accompany the data field and that are used by the MAC protocol.     **PHYSICAL LAYER:** The lowest layer of the IEEE 802 reference model is the physical layer, which includes such functions as encoding/decoding of signals and bit transmission/reception. In addition, the physical layer includes a specification of the transmission medium. In the case of IEEE 802.11, the physical layer also defines frequency bands and antenna characteristics.   1. What is IEEE 802.11i? Explain the Robust Security Network (RSN) protocol.   802.11i is the latest wireless specification that implements a set of security mechanisms that eliminate most of the 802.11 security issues. The final form of the 802.11 standard is known as RSN (Robust Security Standard).   1. Explain the security services provided by RSN, and the security algorithms supported by RSN.   **Authentication**: A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.  **Access control**:1 This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.  **Privacy with message integrity**: MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered.   1. Name the five phases of IEEE 802.11i operations. Explain each phase.   **Discovery**: An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.  **Authentication**: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.  **Key generation and distribution**: The AP and the STA perform several opera- tions that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only.  **Protected Data Transfer**: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.  **Connection Termination**: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.   1. What is Temporal Key Integrity Protocol (TKIP)? What security services are provided by TKIP? How?   IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs: the Temporal Key Integrity Protocol (TKIP), and the Counter Mode-CBC MAC Protocol (CCMP).  TKIP is designed to require only software changes to devices that are implemented with the older wireless LAN security approach called Wired Equivalent Privacy (WEP). TKIP provides two services:   * **Message integrity:** TKIP adds a message integrity code (MIC) to the 802.11 MAC frame after the data field. The MIC is generated by an algorithm, called Michael, that computes a 64-bit value using as input the source and destination MAC address values and the Data field, plus key material. * **Data confidentiality:** Data confidentiality is provided by encrypting the MPDU plus MIC value using RC4.  1. What is Counter Mode-CBC MAC Protocol (CCMP)? What security services are provided by CCMP? How?   ***CCMP:*** is intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme. As with TKIP, CCMP provides two services:   * **Message integrity:** CCMP uses the cipher-block-chaining message authentication code (CBC-MAC), described in Chapter 12. * **Data confidentiality:** CCMP uses the CTR block cipher mode of operation with AES for encryption. CTR is described in Chapter 6.  The same 128-bit AES key is used for both integrity and confidentiality. The scheme uses a 48-bit packet number to construct a nonce to prevent replay attacks.  1. The following table shows a couple of encryption algorithms and their key sizes employed by TLS and WTLS:  |  |  |  | | --- | --- | --- | | **Algorithm** | **TLS Key Size** (bits) | **WTLS Key Size** (bits) | | 3DES | 168 | 40 | | IDEA | 128 | 40 or 56 |     Explain why for the same algorithms WTLS uses shorter keys.  WTLS uses shorter keys because the MAC and encryption keys are derived from the master key, using the HMAC algorithm. The master key is a one time 20-byte value generated for the session using secure key exchange.   1. Consider the WTLS Record Protocol operation as shown by the following figure.       Explain why the data compression is operated before the generation of message authentication code and the encryption.  The mac operation occurs after the compression stage because the MAC operation can be performed faster on a smaller amount of data.   1. In WTLS authentication, a X.509 certificate is used to prove the identity of the server or the client (the certificate owner). Why should the certificate also include the public key of the certificate owner?   Authentication is an optional procedure in WTLS between client and server or client only authenticates the server. If the owner of the certificate provides the public key that party can be authenticated.   1. Explain why security becomes challenging with wireless networks? How is it different from wired networks?   The differences between wired and wireless LANs (in that wireless traffic can be monitored by any radio in range, and need not be physically connected) suggest the increased need for robust security services and mechanisms for wireless LANs. |

**Hands-on Exercises:**

Please continue your work on labs. The 3th lab has been released at the course website.