Csci388 Wireless and Mobile Security
– Access Control: 802.1X, EAP, and RADIUS

Xiuzhen Cheng
cheng@gwu.edu

WEP Weakness
1. IV is too short and not protected from reuse
2. The per packet key is constructed from the IV, making it susceptible to weak key attacks
3. No effective detection of message tampering (message integrity)
4. Master key is used directly and no built-in provision to update the keys
5. There is no protection against message replay

Wi-Fi and IEEE 802.11
- Wi-Fi refers to the wireless LAN network
- IEEE 802.11 is a standard, specifying the physical characteristics of the 802.11 LAN
- Wi-Fi Alliance: formed by a group of major manufactures
  - Solve the interoperability problem
  - Ambiguous/undefined areas in 802.11 standard
  - Options of 802.11: some are avoid, some are required in Wi-Fi
  - To obtain the Wi-Fi certification, a manufacturer must submit its product for testing against a set of "gold standard" Wi-Fi products.

IEEE 802.11i and WPA
- IEEE 802.11i is the addendum to the 802.11 standard. 802.11i specifies the new generation of security.
  - 802.11i defines a new type of network called a robust security network (RSN). RSN-enables device is not compatible with Wi-Fi equipment
  - 802.11i task group developed a security solution based on the current capabilities of the Wi-Fi products: TKIP
- Wi-Fi Protected Access (WPA): a subset of RSN specifying TKIP
  - RSN and WPA share a single security architecture that covers procedures such as upper-level authentication, key distribution and renewal.
  - More complex and scalable compared to WEP

802.11i – Three pieces, Two Layers
- Lower layer: TKIP and CCMP
  - Temporal Key Integrity Protocol
  - Counter Mode with CBC-MAC protocol
  - Both provides enhanced data integrity over WEP
  - TKIP being targeted at legacy equipment and CCMP being targeted at future WLAN equipment
- Upper Layer: 802.1x
  - 802.1x is a standard for port based access control developed by a different body within the IEEE 802 organization
  - 802.1x provides a framework for robust user authentication and encryption key distribution
    - Original 802.11 has neither of these features.
  - The three pieces discussed above work together to form an overall security system

Importance of Access Control
- Separate the world with “good guys” and “bad guys”
- How to do it in WPA and RSN?
  - IEEE 802.1X: Originally designed for authenticating ports on wired LANs
  - EAP: Extensible Authentication Protocol
  - RADIUS: Remote Authentication Dial-In User Service
  - IEEE 802.1X with EAP are mandatory for WPA and RSN
  - RADIUS is the method of choice by WPA, and is optional in RSN
  - EAP and RADIUS were both developed for dial-in access
    - Dial-in access control is organized in a very similar way to IEEE 802.1X
A standard for port based network access control. It can be applied to both wired and wireless networks and provides a framework for user authentication and encryption key distribution.

- It can be used to restrict access to a network until the user has been authenticated by the network.
- In addition, 802.1x is used in conjunction with one of a number of upper layer authentication protocols to perform verification of credentials and generation of encryption keys.

Entities in 802.1X

- Three Components
  - Supplicant (client): An entity that wants to have access
  - Authenticator (switch, AP, other NAS, preferably RADIUS capable): An entity that controls the access gate
  - Authentication Server (sometimes part of Authenticator, otherwise RADIUS server, the most common type of authentication server): An entity that decides whether the supplicant is to be admitted — authorizer

802.1X Architecture

- Authenticator acts as a bridge
- 802.1X is a framework, not a complete specification in and of itself. The actual authentication mechanism is implemented by the authentication server

Authentication for Dial-In Users

PPP protocol defines two weak authentication methods:
- PAP: UNAME and PWD are transmitted in clear text
- CHAP: a challenge-response scheme is exploited
- EAP is proposed for stronger authentication in PPP

Authentication for Wireless LAN Users

Database server is centralized

- Similar to the dial-in network organization
- IEEE 802.1X utilizes EAP for access control
- 802.1X implements access control at the point at which a user joins the network.
- In Wireless LAN, an AP needs to create a logical port in software with an authenticator for each wireless user — no physical port is available!
- The number of 802.1X entities in operation is the same as the number of associated mobile devices
- Port traffic, except for 802.1X, blocked until successful authentication

More on 802.1X

- 802.1X authenticates users, rather than machines
  - WEP relies on the shared key, stored each machine
- 802.1X is a framework based on EAP; it is an IEEE adaptation of the IETF’s EAP
  - EAP is originally specified in RFC 2284 and updated by RFC 3748
- EAP is a framework protocol too.
  - Rather than specifying how to authenticate users, EAP allows protocol designers to build their own EAP methods, subprotocols, that perform the authentication transaction
  - EAP methods can have different goals, and therefore, often use many different methods for authenticating users depending on the requirements of a particular situation
**Motivation of EAP**
- When PPP is first introduced in the early 1990s, there were two protocols available for user authentication: PAP and CHAP
- Both PAP and CHAP require the use of a PPP protocol number
- Assigning a PPP protocol number to each authentication method that might be obsolete soon is not favorable
- EAP uses a single PPP protocol number while supporting a wide variety of authentication mechanisms
- EAP is a single encapsulation that can run over link layer such as PPP, 802.3, 802.11
- It is most widely deployed on PPP links

**Generic EAP packet format (EAP over PPP & EAP over LAN)**

<table>
<thead>
<tr>
<th>PPP Header</th>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>Variable length</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAN Header</th>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>Variable length</td>
<td></td>
</tr>
</tbody>
</table>

**EAP Packet Format (Four Types)**

- Code = 1 for request and 2 for response
- Extra field called Type-Code in EAP Request/Response message before the Data field
- Notification: for notification message (eg.Pwd is going to expire…), rarely used for 802.1X
- Type-Code >3 specifying authentication method
- Type-code = 4: MD5 Challenge
- Type-code = 13: EAP-TLS
- Identifier: a number incremented for each message send, data field may contain a prompt (Req/Res) message; used for pairing the request/response – same number for the pair

**EAP Success and Failure**
- Code = 3 for success, =4 for failure
- Short data package containing no data

---

**A Simple EAP Message Exchange**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>End User</td>
<td>Authenticator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Request/Identity: starting the exchange, telling the end users That the network is likely to drop data traffic before the authentication procedure is complete

**EAP Demystified**

**Authentication framework**
- EAP utilizes authentication-specific messages
- Authenticators only need to recognize a few well defined messages
  - Request/Response
  - Success/Failure
- EAP subtypes allow for new types of authentication methods to be added without requiring upgrades to the Authenticators
- You can write MyMethod over EAP

**How to Choose an EAP Method?**

- Driven by the back-end authentication system
- An EAP method for Wireless LAN should meet the three major goals
  - Strong cryptographic protection of user credentials
  - Mutual authentication
  - Key derivation

**EAP Authentication Methods**

- **EAP-MD5**
  - Does NOT provide for dynamic encryption – encryption key can’t be generated dynamically
  - User authenticated by password
  - Network NOT authenticated to user (no mutual authentication)
- **EAP-TLS**
  - Provides for dynamic encryption
  - User and network mutually authenticated using certificates
  - Meet the three goals
  - Has limited use due to the requirement of the PKI (digital certificate)
- **EAP-TTLS and PEAP**
  - Provides for dynamic encryption
  - Network authenticated using certificate (outer authentication), the protocol is similar to EAP-TLS
  - Client authentication tunneled inside of EAP-TLS (inner authentication)
  - Significantly decreases the number of digital certificates
  - Non-cryptographic or older EAP methods such as PAP and CHAP can be applied for inner authentication because a secure tunnel has been created
  - Inner and outer authentication can use different user name, even anonymous usernames
**TLS Basic Protocol**

- Choose secret \( S \)
- Compute \( K = f(S, \text{RAlice}, \text{RBob}) \)
- Alice
- I want to talk, Ciphers I support, \( R_{\text{Alice}} \)
- Certificate, cipher I choose, \( R_{\text{Alice}} \)
- \( \{S\}_{\text{has}} \) (keyed hash of handshake msgs), Certificate
- Finished!
- Bob
- Compute \( K = f(S, \text{RAlice}, \text{RBob}) \)
- Data protected with keys derived from \( K \)

**TLS over EAP**

- CLIENT
  - EAP-Response Identity
  - EAP-TLS: Client-Hello
  - EAP-TLS: Server-Hello
  - EAP-TLS: Server-TLS Certificate
  - EAP-TLS: Client-Cert: Request
  - Finished
- SERVER
  - EAP-Request Identity
  - EAP-TLS: Certf. Verification
  - EAP-TLS: Change Cipher
  - Finished
- EAP-TLS (empty)
- EAP - Success

**TLS and WPA/RSN**

- **TLS handshake process accomplishes three things:**
  - Server authentication (optionally for client)
  - A master key for the session
  - Cipher suites to protect the communication (multiple keys are derived)

- **In WPA**
  - Encryption and integrity protection is provided by WEP or TKIP

- **In RSN**
  - Encryption and integrity protection is provided by TKIP or AES-COMP

- **For WPA and RSN,**
  - All we need from TLS is the authentication function and the master key generation function

**EAP Over LAN**

- **EAP RFC does not specify how messages should be passed around**
  - It was originally designed for use with dial-up authentication via a modem

- **EAP messages have to be encapsulated in order to be transmitted in a Wi-Fi network**
  - Prepend the MAC address? – most simple way

- **IEEE 802.1X defines EAPOL: EAP Over LAN**
  - Not just prepend the MAC header. Defines more messages and fields
  - EAPOL-Start message to a special group-multicast address (reserved for 802.1X authenticators) to announce the existence of a supplicant
  - EAPOL-Key from the authenticator to send encryption keys to the suppliant
    - How to encrypt the key? – no definition
  - EAPOL-Packet, for transmitting the original EAP messages
  - EAPOL-Logoff
  - EAPOL-Encapsulated-ASF-Alert (not used by WPA and RSN)

**EAPOL Message Flow**

- EAPOL-Start (optional)
  - Request Identity
  - Response Identity
  - Request/Method
  - Response/Method
  - EAP-Success
  - EAPOL-key
  - Data
  - EAPOL-Logoff

**802.1X Architecture – Revisited**

- Authenticator acts as a bridge
- 802.1X is a framework, not a complete specification in and of itself. The actual authentication mechanism is implemented by the authentication server
Wireless devices act as supplicants, applying for access by sending messages to the authenticator.

All done in software

For SOHO, authentication server could be a simple process inside the AP

- Eg. Just a list of user names and passwords
- No need for RADIUS since the authenticator and the authentication server do not need to communicate
- The number of supported authentication methods would be limited

In Wireless LAN, an AP needs to create a logical port with an authenticator for each supplicant (wireless user)

- The number of 802.1X entities in operation is the same as the number of associated mobile devices

- If authentication server and authenticator both reside in the AP, no RADIUS protocol is needed

- In wireless LAN, EAPOL can proceed only after the association is complete since no port exists; Association process allows supplicant and AP to exchange MAC address

Typical 802.1X Exchange on 802.11

- Association Request
- Association Response
- EAPOL-Start (optional)
- Request Identity
- Response Identity
- Request/Method
- Response/Method
- EAP-Success
- EAPOL-key
- Data
- EAPOL-Logoff

(RADIUS packet)

802.1X Message Exchange on 802.11

- Keys are exchanged only after successful authentication
  - EAPOL-Key can be used periodically to dynamically update keys
  - Will be further explained later when discussing TKIP
- EAPOL starts after the association process is complete
  - Association process exchanges MAC address first

How 802.1X works
802.1X Meets Wireless -- Summary

- Associations (wireless clients with access points) become virtual “ports”
- Frequent reauthentications reset key information and insure no session hijacking has occurred
- EAPoL-Key frame used to provide dynamic encryption -- dynamically refresh session keys
- Now used as the basis for enterprise authentication in WPA and WPA2 (802.11i)

RADIUS – Remote Access Dial-In User Service

- Optional in RSN, originally designed for TCP/IP type of networks
- A protocol for the communication between the NAS (network access server) and the AS (authentication server)
  - Dial-up modem pool server (NAS) at Point-of-Presence
  - RADIUS server (AS)
- In Wi-Fi networks
  - NAS is AP
  - AS is the server with the authentication database

How RADIUS Works

- The core protocol contains four messages:
  - Access-Request (NASÆAS)
  - Access-Challenge (NASÅAS)
  - Access-Accept (ASÆNAS)
  - Access-Reject (ASÆNAS)
- RADIUS is used for dial-in system authentication, with two options:
  - PAP Operation: username/password sent as plaintexts
  - CHAP Operation: based on challenge response

Basic Format of RADIUS Message

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Authenticator</th>
<th>Attributes...</th>
</tr>
</thead>
</table>

- Code identifies the four types of RADIUS messages
  - Access-Request: 1
  - Access-Accept: 2
  - Access-Reject: 3
  - Access-Challenge: 11
- Identifier: a number incremented for each message; used to match up requests and replies
- Authenticator:
  - For Access-Request, a 16B nonce is included.
  - This nonce together with the shared key (between AS and NAS) is used for encrypting the password (together with the shared key) if password value is sent as an attribute
  - For response messages, the nonce with the key will be used for integrity check to counter replay attacks. The integrity check value will be inserted to the Authenticator field. – How to compute?
- Attributes
  - Information carried in RADIUS message is contained within attributes
  - Each attribute contains the fields of Type, Length and Data

EAP over RADIUS

- Defined in RFC 2869
- The EAP message is sent inside one or more special attributes that have a type value of 79

Improvement of 802.1X over WEP

- 802.1x provides support for a centralized security management model for user authentication.
- The primary encryption keys are unique to each station so the traffic on any single key is significantly reduced.
  - Either pre-shared (eg. A password for SOHO) or generated through an upper layer authentication protocol (eg. TLS)
  - When used with an AS, the encryption keys are generated dynamically and don't require a network administrator for configuration or intervention by the user
- It provides support for strong upper layer authentication.