IEEE 802.11i draft & Call For Interest on Link Security for IEEE 802 Networks

Dave Halasz

November 12, 2002

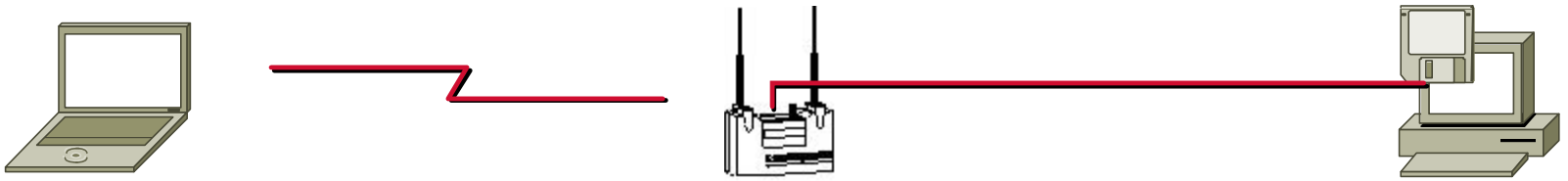
General notes about IEEE 802.11

- Divided into MAC & PHY
  - MAC protocol exists
    - IEEE 802.11 management, control and data packets
- IEEE 802.11 data packet size can be larger than ethernet size
- Easy to detect traffic
  - Data is literally broadcast
- Local denial of service is trivial with a jammer

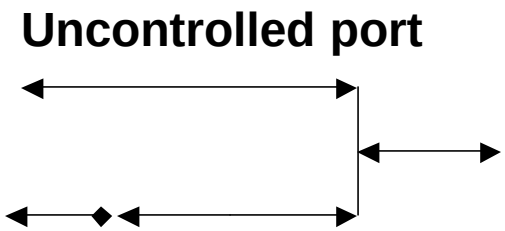
General notes cont.

- Two modes of operation
  - Independent Basic Service Set (Ad-Hoc Mode)
    - Small, independent network
  - Extended Service Set (Infrastructure Mode)
    - Use AP's to set a large network, with access to a distribution system.
      - EPON would map to this mode.

IEEE 802.11i uses IEEE 802.1X



Supplicant **Authenticator** **Authentication Server**



Proposed PICS for IEEE 802.11i

- http://www.ieee802.org/11/Documents/DocumentHolder/2-647.zip

- RSN Information Element (Tx'd in mngmt frames)
  - Group Key Cipher Suite
  - Pairwise Key Cipher Suite
  - Authenticated Key Management Suite List
    - Unspecified EAP/802.11i Key Management
    - Preshared key/802.11i Key Management
  - RSN Capabilities

- RSN – Robust Security Network, defined in IEEE 802.11i draft
- PICS - Protocol Implementation Conformance Statement
  - The supplier of a protocol implementation that is claimed to conform to IEEE Std shall complete the following…

Prop. PICS for IEEE 802.11i cont.

- New data privacy protocols
  - CCMP - Counter-Mode/CBC-MAC protocol
  - TKIP – Temporal Key Integrity Protocol, legacy support
  - WRAP - Wireless Robust Authenticated Protocol (AES-OCB)
- 802.11i Key Management
  - Key Hierarchy
    - Pairwise Key Hierarchy
    - Group Key Hierarchy
  - 4 way handshake
  - Group key handshake

RSN Information element

- **RSN Information Element**
  - **Transmitted in 802.11 management frames**
    - **Doesn’t work for other networks**
  - **Unauthenticated negotiation of security policy**
    - **Gets authenticated through 4 way handshake**

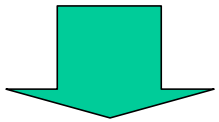
Data Privacy Protocols

- **CCMP Done over MPDU**
- **TKIP Authentication check done over MSDU, encryption done over MPDU**
- **WRAP Done over MSDU**
- **From IEEE 802.11-1999**
  - **3.31 medium access control (MAC) protocol data unit (MPDU): The unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY).**
  - **3.32 medium access control (MAC) service data unit (MSDU): Information that is delivered as a unit between MAC service access points (SAPs).**
- **Cannot block copy, work needed here**

Key Hierarchy

PMK: Pairwise Master Key

PRF(PMK, ANonce, SNonce, …)

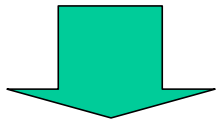


PTK: Pairwise Transient Key

ANonce: Authenticator Nonce
SNonce: Supplicant Nonce

GMK: Group Master Key

PRF(GMK, GNonce, …)



GTK: Group Transient Key

GNonce: Group Nonce

PRF: Pseudo Random Function

Key Management

GTK gets established in group handshake

GTK ⟷ GTK

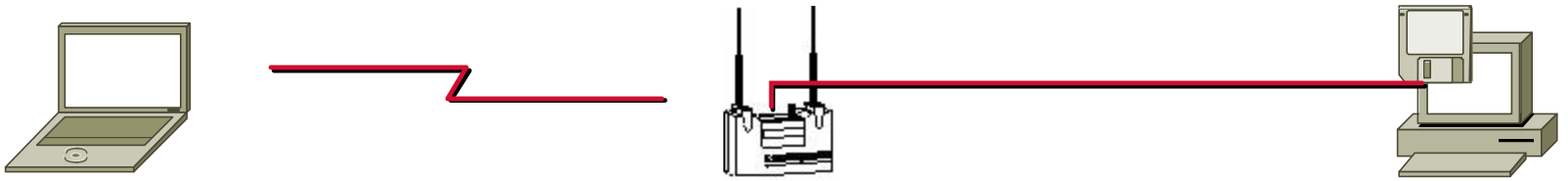
PTK gets established in 4 way handshake

PTK ⟷ PTK

PMK gets delivered to the authenticator

PMK ⟵

PMK — PMK gets established through EAP authentication method — PMK



Supplicant **Authenticator** **Authentication Server**

Key Management

- Key Hierarchy & Key handshakes
  - IEEE 802.1X key protocol (Different key descriptor)
  - General format useful
    - Includes the RSN IE, which is IEEE 802.11i specific

Summary

- **Negotiation of security policy is IEEE 802.11 specific.**
- **Data Privacy Protocols are IEEE 802.11i specific. However, some of this can be leveraged.**
- **Key Management including Key Hierarchy & Key Handshakes generally applicable to other IEEE 802 networks.**