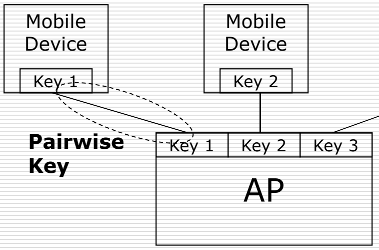
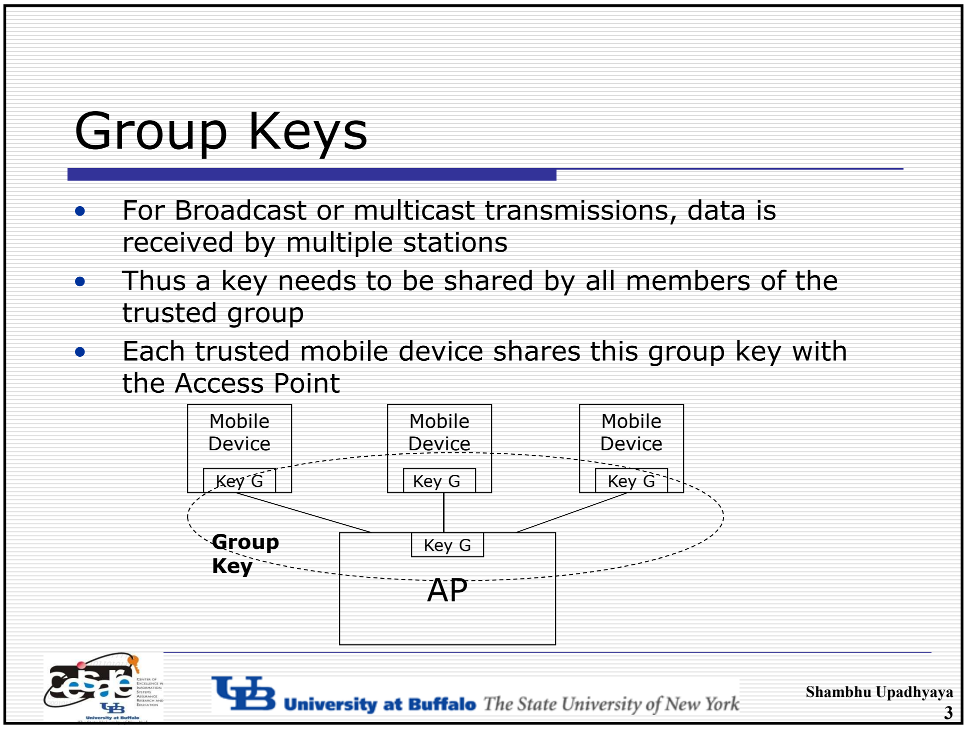
802.11 Security – Key Hierarchy

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 14)

Pairwise Keys

- Unicast data sent between two stations has to be private between them
- For this purpose a pairwise key is used which is known to the two parties
- Each mobile device has a unique pairwise key with the access point





Group Keys

- For Broadcast or multicast transmissions, data is received by multiple stations
- Thus a key needs to be shared by all members of the trusted group
- Each trusted mobile device shares this group key with the Access Point

Mobile Device

Key G

Mobile Device

Key G

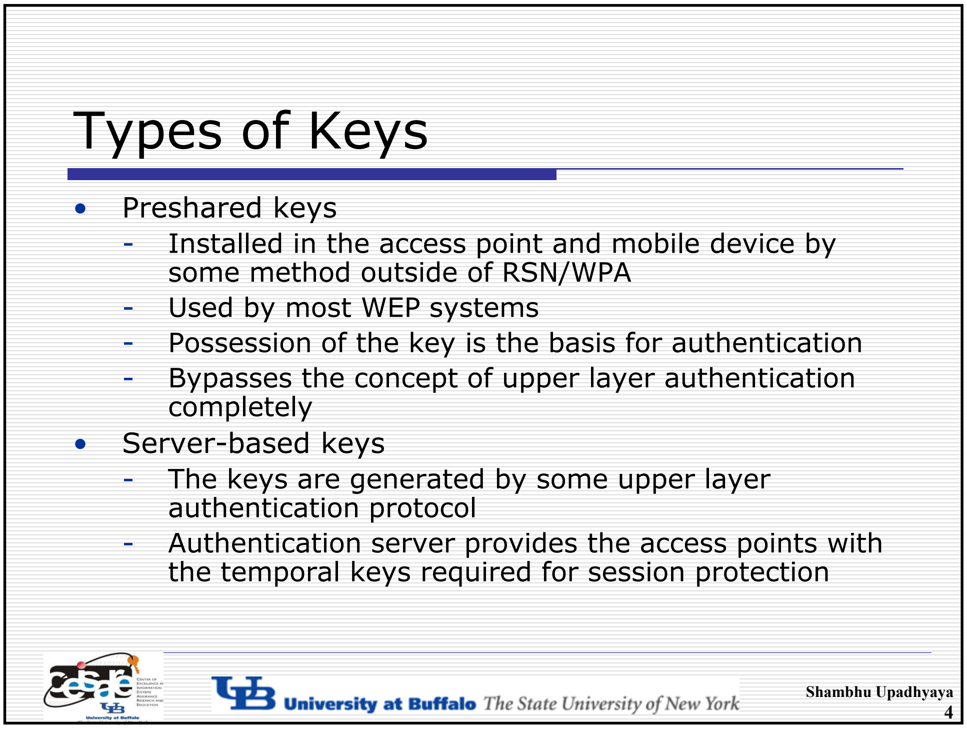
Mobile Device

Key G

Group Key

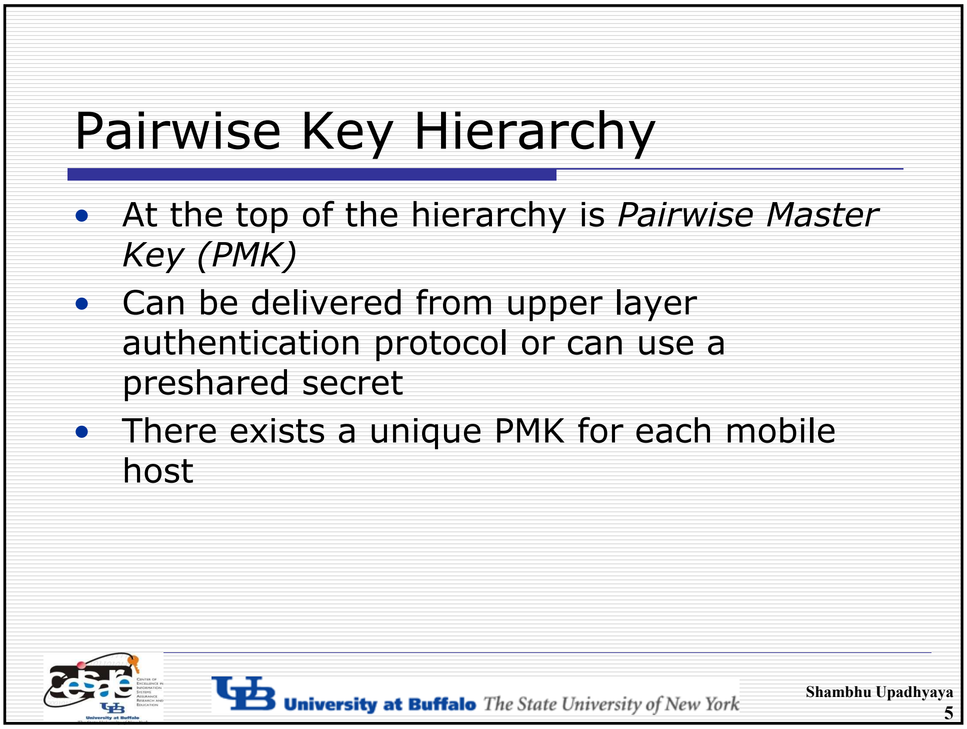
Key G

AP



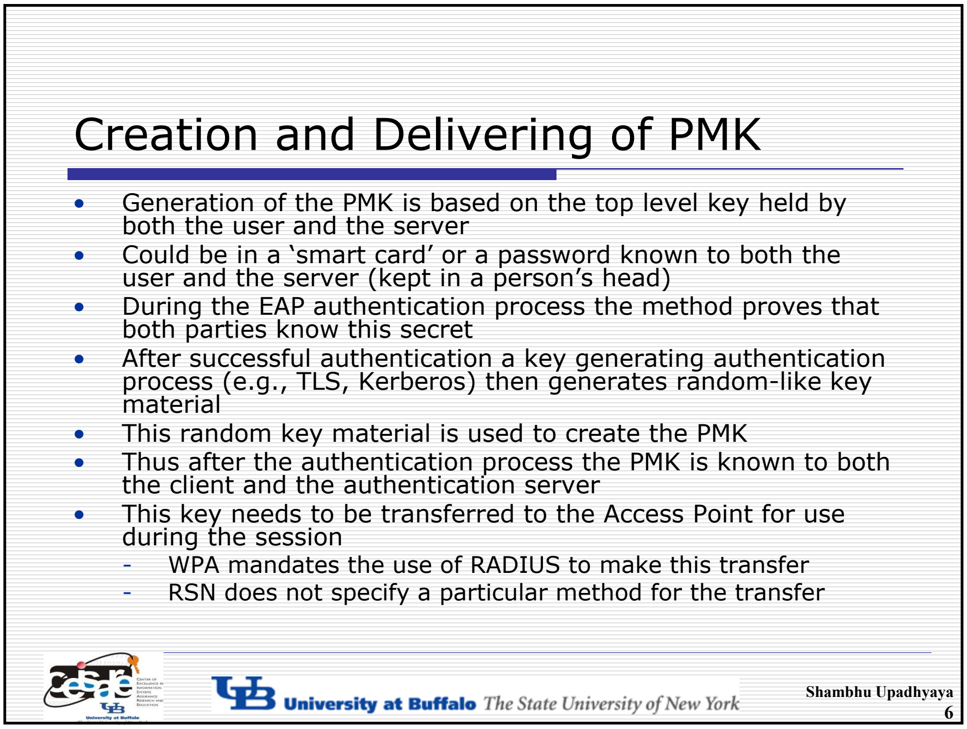
Types of Keys

- Preshared keys
  - Installed in the access point and mobile device by some method outside of RSN/WPA
  - Used by most WEP systems
  - Possession of the key is the basis for authentication
  - Bypasses the concept of upper layer authentication completely
- Server-based keys
  - The keys are generated by some upper layer authentication protocol
  - Authentication server provides the access points with the temporal keys required for session protection



Pairwise Key Hierarchy

- At the top of the hierarchy is *Pairwise Master Key (PMK)*
- Can be delivered from upper layer authentication protocol or can use a preshared secret
- There exists a unique PMK for each mobile host



Creation and Delivering of PMK

- Generation of the PMK is based on the top level key held by both the user and the server
- Could be in a ‘smart card’ or a password known to both the user and the server (kept in a person’s head)
- During the EAP authentication process the method proves that both parties know this secret
- After successful authentication a key generating authentication process (e.g., TLS, Kerberos) then generates random-like key material
- This random key material is used to create the PMK
- Thus after the authentication process the PMK is known to both the client and the authentication server
- This key needs to be transferred to the Access Point for use during the session
  - WPA mandates the use of RADIUS to make this transfer
  - RSN does not specify a particular method for the transfer

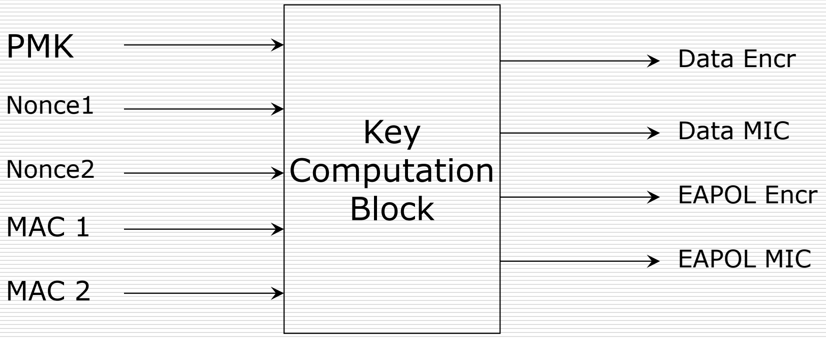
Computing Temporal Keys

- 802.1X model, data can start flowing once access point has the key, but WPA/RSN has more steps
- Now temporal keys are derived from this PMK for use during each session
- These keys are called temporal keys as they are recomputed each time the mobile device associates with the AP
- There are four keys derived for this purpose
  - Data Encryption Key (128 bits)
  - Data Integrity Key (128 bits)
  - EAPOL-Key Encryption Key (128 bits)
  - EAPOL-Key Integrity Key (128 bits)
- Collection of these four keys is called as *Pairwise Transient Key (PTK)*

Details of Temporal Keys

- First two keys are used to encrypt and protect the data
- Last two are used to protect communication between the access point and mobile device during the initial handshake
- As the temporal keys change every time a station reattaches with the AP, liveliness is ensured by including a couple of *Nonces* in the computation of the temporal keys
- A Nonce is a value which is “never” or “extremely unlikely” to be repeated
- Each device generates a nonce and passes it to the other device
- Also to bind identity of the devices to the keys, MAC addresses of the devices are included in computation

Temporal Key Generation



PMK

Nonce1

Nonce2

MAC 1

MAC 2

Key Computation Block

Data Encr

Data MIC

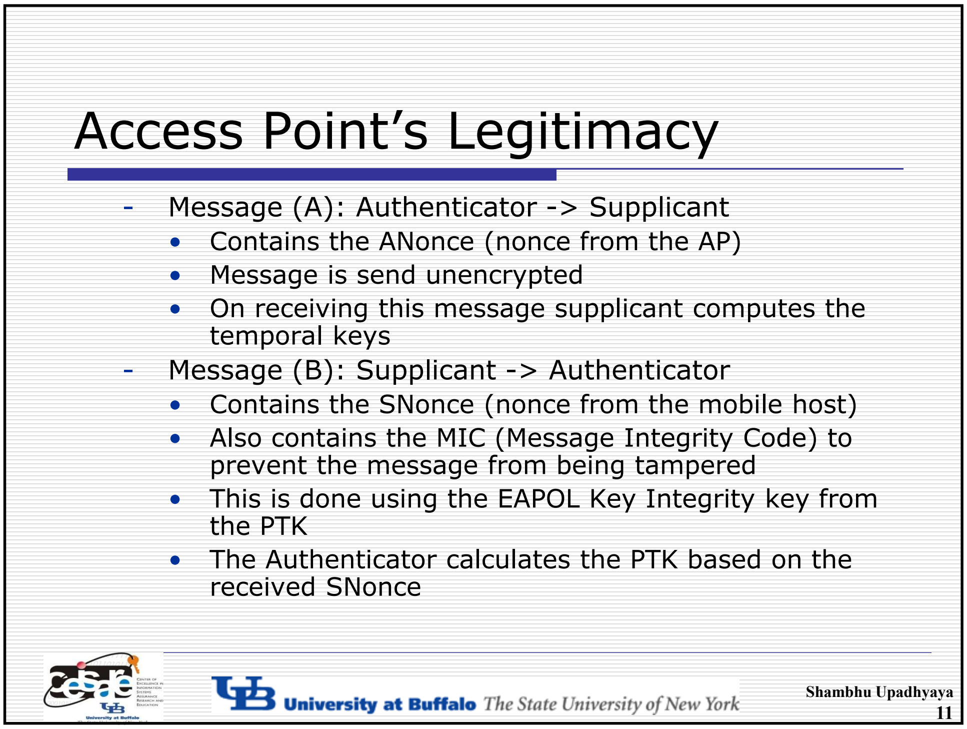
EAPOL Encr

EAPOL MIC

Temporal Key Computation

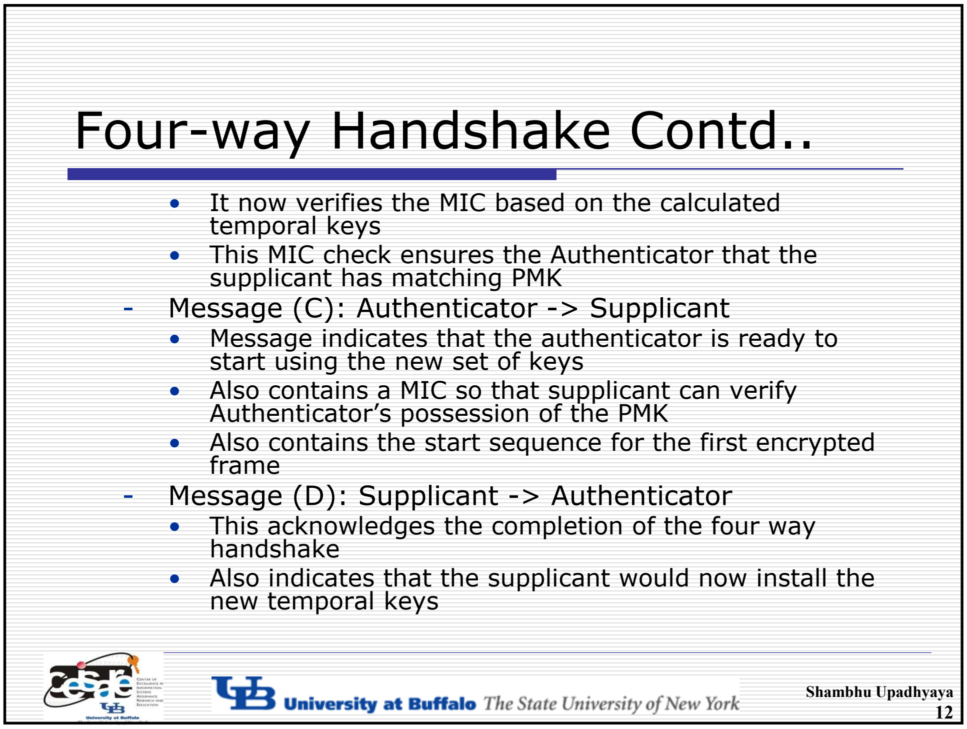
Exchanging and Verifying Key Information (Legitimizing AP)

- In the above exchange there is an implicit trust between the mobile host and the Access point
- To ensure that the Access Point is not rogue, it must authenticate itself with the mobile device
- To do this, the access point proves its possession of the PMK which it gets from the authentication server and can only be obtained by a legitimate AP
- This is done by carrying out a four-way mutual authentication between the AP and the mobile host using EAPOL Key Messages



Access Point’s Legitimacy

- Message (A): Authenticator -> Supplicant
  - Contains the ANonce (nonce from the AP)
  - Message is send unencrypted
  - On receiving this message supplicant computes the temporal keys
- Message (B): Supplicant -> Authenticator
  - Contains the SNonce (nonce from the mobile host)
  - Also contains the MIC (Message Integrity Code) to prevent the message from being tampered
  - This is done using the EAPOL Key Integrity key from the PTK
  - The Authenticator calculates the PTK based on the received SNonce



Four-way Handshake Contd..

  - It now verifies the MIC based on the calculated temporal keys
  - This MIC check ensures the Authenticator that the supplicant has matching PMK
- Message (C): Authenticator -> Supplicant
  - Message indicates that the authenticator is ready to start using the new set of keys
  - Also contains a MIC so that supplicant can verify Authenticator’s possession of the PMK
  - Also contains the start sequence for the first encrypted frame
- Message (D): Supplicant -> Authenticator
  - This acknowledges the completion of the four way handshake
  - Also indicates that the supplicant would now install the new temporal keys

Group Key Hierarchy

- Used for broadcast and multicast transmissions
- Broadcasts and multicasts can be sent from the access point only
- Pairwise keys cannot be used as the same transmission is to be heard by all stations
- Hence the same key is shared by all stations and is called the *Group key*

Group Key Hierarchy

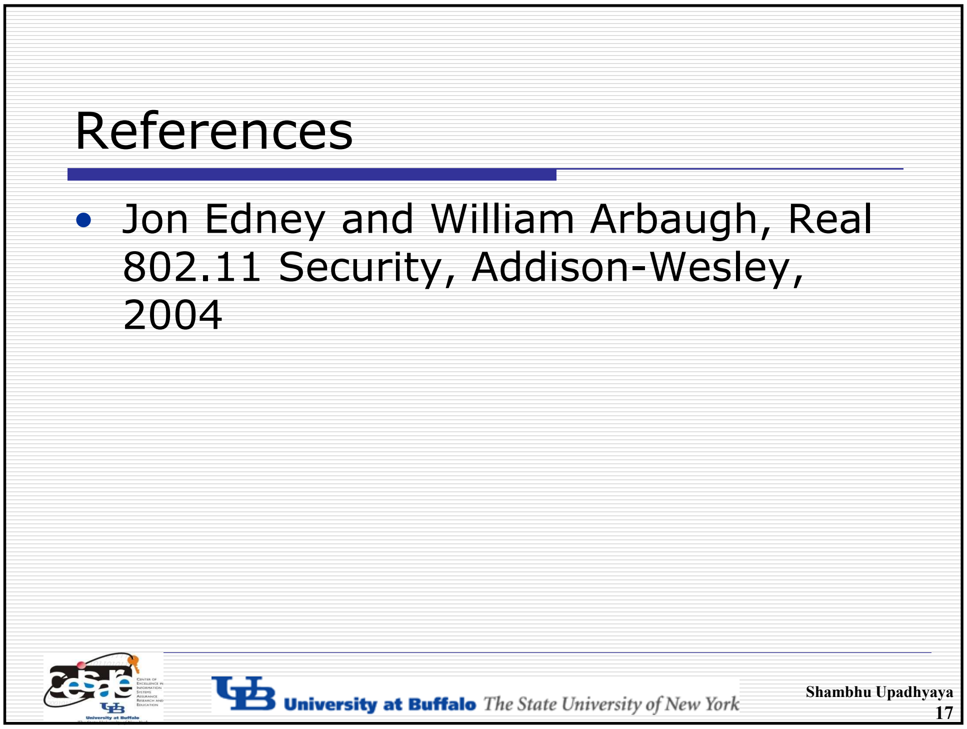
- Group keys pose a problem when a station leaves the network
- The pairwise keys are removed when a station disconnects but the group keys are still valid and can be used by the station to passively listen to the group transmissions
- This might be undesirable in some situations
- The solution to this problem is to change the group key once a station leaves the network

Group Key Hierarchy

- Changing and distributing group keys is easier than pairwise keys as there already exists a secure channel (using pairwise keys) over which the group key can be sent
- The access point performs the following functions during Group Key Rekeying
  - Create a 256 bit Group Master Key (GMK)
  - Derive a Group Transient Key (GTK) from which the temporal keys are obtained
  - After establishment of each pairwise secure connection
    - Send GTK to mobile device with current sequence number
    - Check for acknowledgement of the receipt

Group Key Hierarchy

- To provide an uninterrupted service, WEP provided the support for multiple keys
- Using this, four keys can be installed in a device at a time
- Each transmission carries a KeyID which specifies which of the keys to use for decryption
- Thus, if during a multicast transmission a station disconnects, the AP can continue transmission using the old key set till the new set of Group keys is calculated and distributed, after which it switches to the new keys set
- Also, GMK is not bound to a particular station and hence can be easily chosen by simply choosing a cryptographic quality random number



References

- Jon Edney and William Arbaugh, Real 802.11 Security, Addison-Wesley, 2004