CAPWAP System Security

T. Charles Clancy

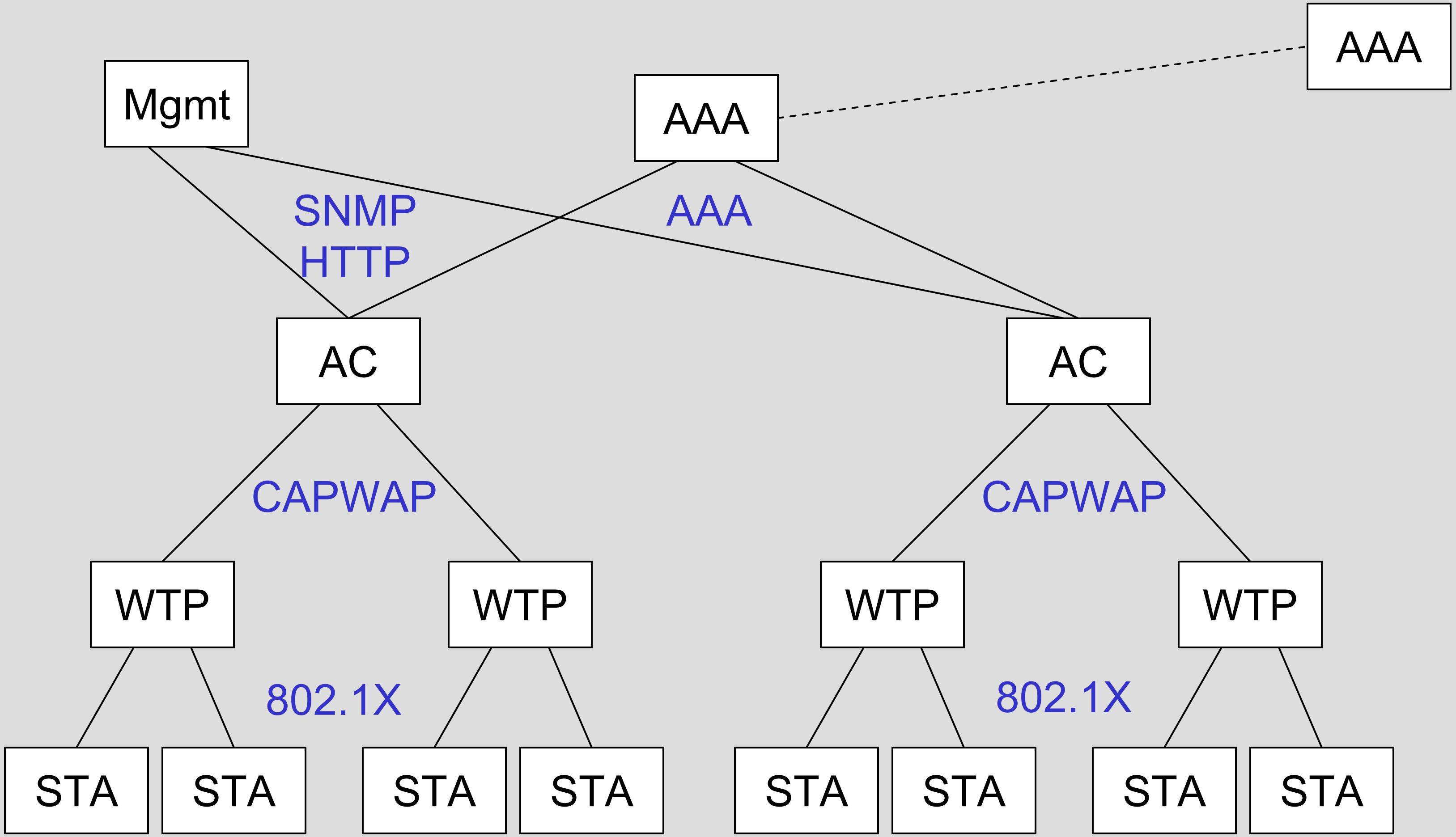
`clancy@cs.umd.edu`

Department of Computer Science
University of Maryland, College Park

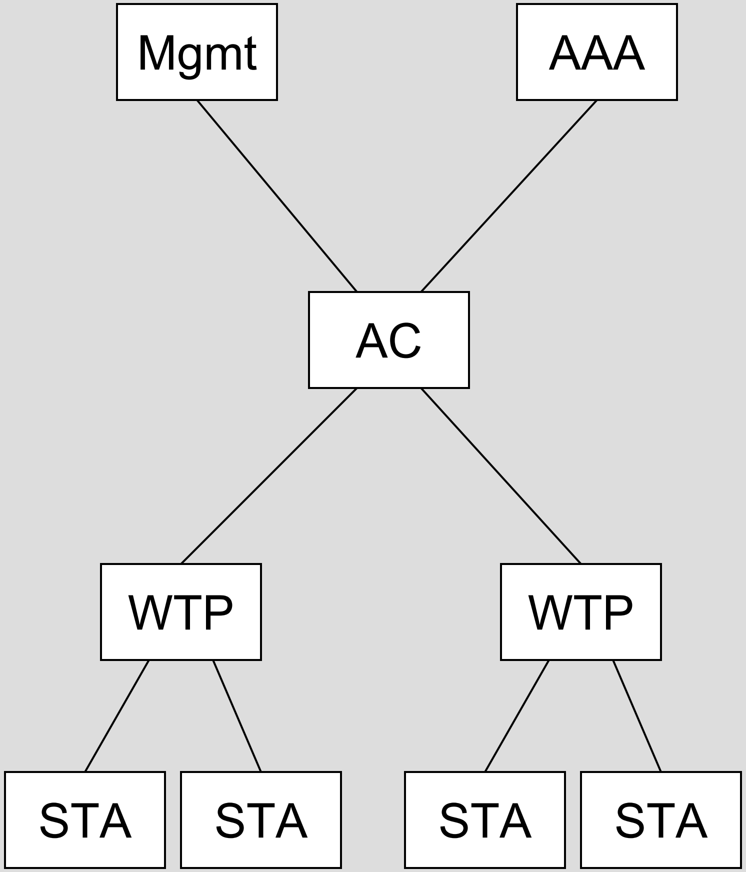
Laboratory for Telecommunication Sciences
US Department of Defense

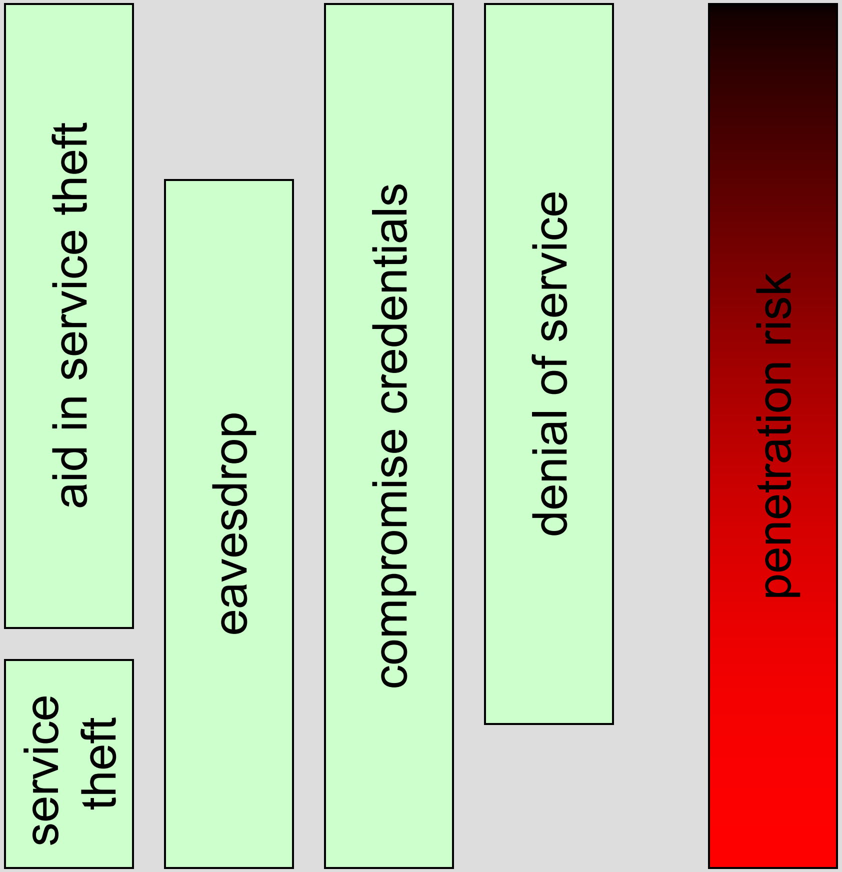
IETF 64, CAPWAP WG, November 7, 2005

{Security Protocol Hierarchy}

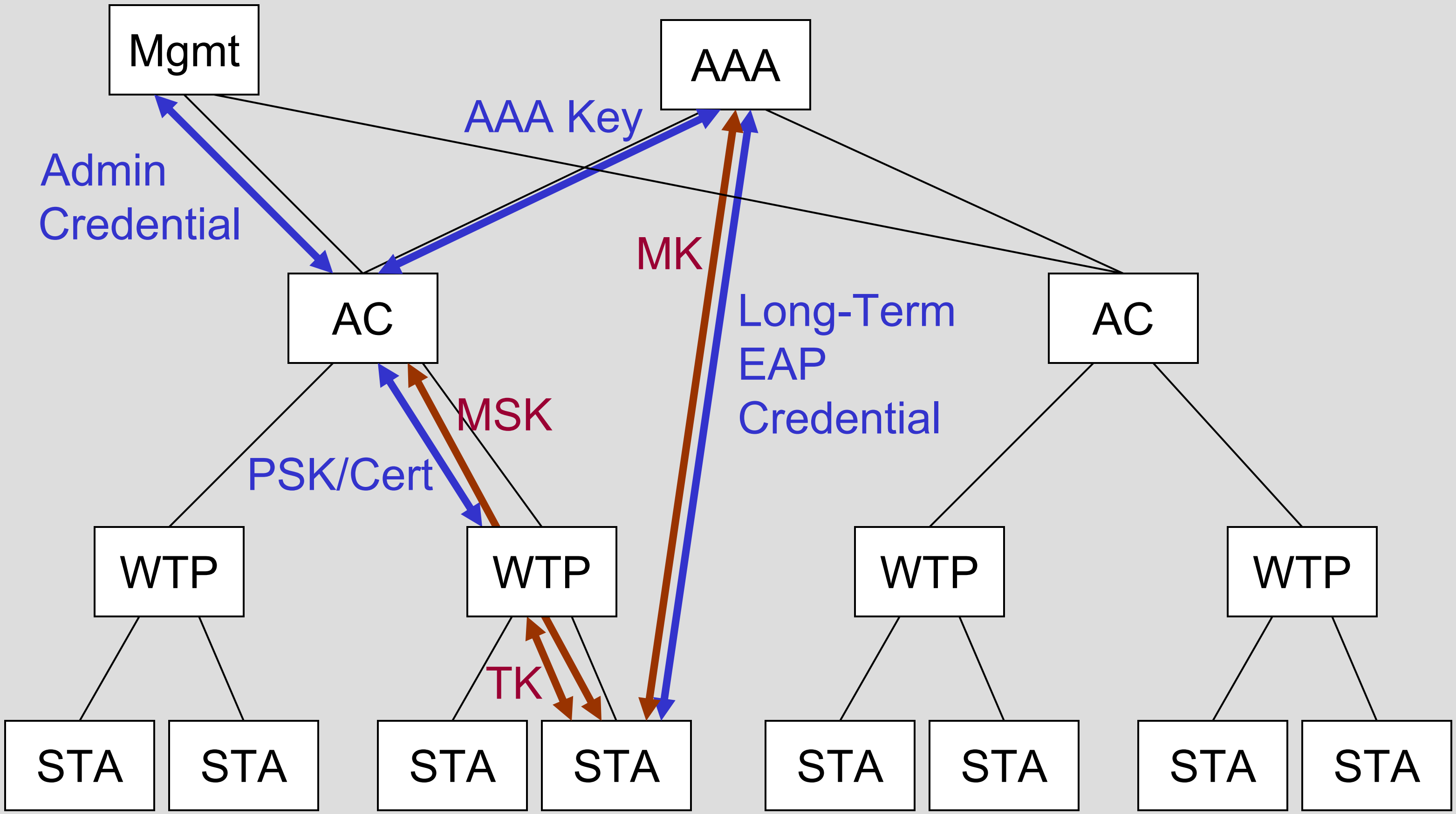


{Threat Model}





{Trust Relationships}



{System Security}

- Long-Term Trust Relationships:
  - WTP ↔ AC (CAPWAP PSK or Certificate)
  - AC ↔ AAA (AAA secret / RADIUS)
  - STA ↔ AAA (EAP Credential)
- Trust Chaining

WTP ↔ AC ↔ AAA ↔ STA

=> WTP ↔ STA

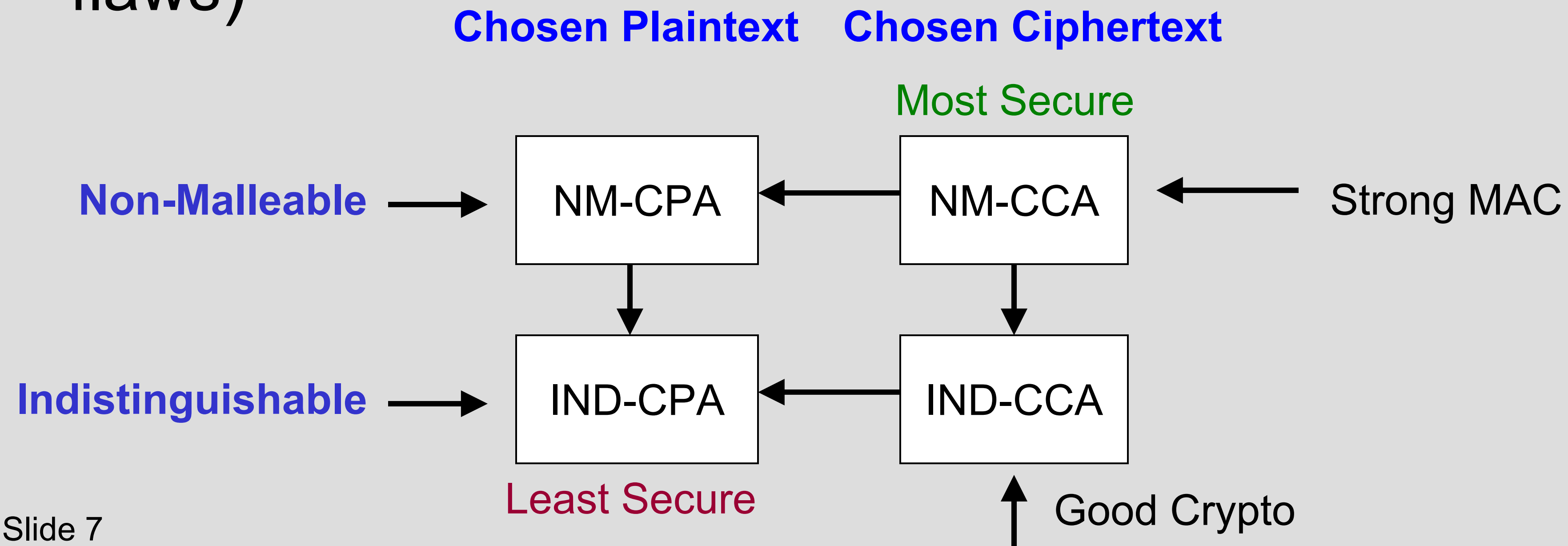
- Only as secure as the weakest link

{Implications}

- Strong mutual authentication at each level
- All transmitted packets MUST be protected by a keyed integrity check value to prevent forgery
- Encryption only required if transmitted data is sensitive (application specific)
- Eavesdropping easier on wireless links, thus encryption is RECOMMENDED

{Crypto Security}

- Ciphers MUST be IND-CPA-secure SHOULD be NM-CCA-secure
- **Example:** WEP is IND-CPA-secure (excluding FMS attack)
- **Example:** TKIP is IND-CCA-secure (due to Michael flaws)



Chosen Plaintext

Chosen Ciphertext

Most Secure

Non-Malleable

NM-CPA

NM-CCA

Strong MAC

Indistinguishable

IND-CPA

IND-CCA

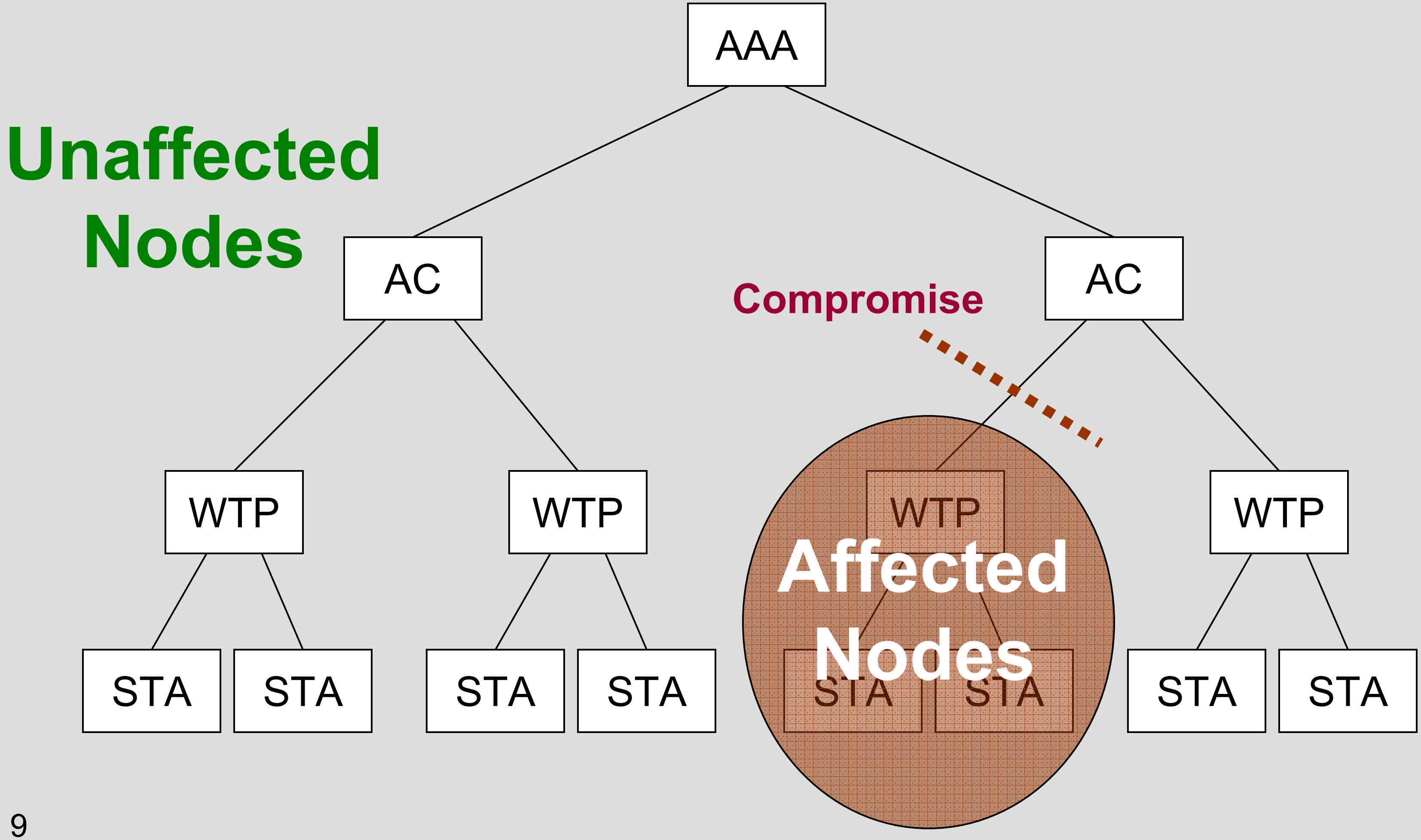
Least Secure

Good Crypto

{Good Ciphers and MACs }

- **Good Ciphers:** AES-CCMP, RSA-OAEP
- **Good MACs:** AES-CBC-MAC, HMAC-SHA1
- Replay prevention
  - Approach 1: have MAC cover packet header (AES-CCMP) – good
  - Approach 2: require strong, randomly initialized, incrementing IV – better
  - Approach 3: include a randomly initialized, explicit sequence number (DTLS) – best

{Attack Containment}



{Implications}

- To mitigate and contain compromises:
  - Each AC must have a unique shared secret with each AAA server
  - Each WTP must have a unique PSK or certificate for each AC
  - Each STA must have a unique TK with each WTP and unique MSK with each AC
    - Handoffs between WTPs MUST derive a fresh TK
    - 802.11i: execute a new four-way handshake
    - Handoffs between ACs MUST derive a fresh MSK
    - 802.11i: reauthenticate

{CAPWAP Management }

- Upper-layer management features:
  - SNMP interface
  - Firmware updates
- Must be strongly and mutually authenticated
- Management should be executed via the AC
  - Maintain hierarchy, preserve security properties
  - Single, centralized authentication point
  - Single point of failure, DoS possibility
- AC provides SNMP front end to the CAPWAP management protocol

{CAPWAP Protocol Requirements }

- Need **authentication**
  - – Symmetric key size ≥ 128 bits
  - – Public key size ≥ 2048 bits
  - – Explicit mutual authentication with key confirmation (prevent DoS)
  - – Unique credentials for each WTP
- Need **authorization**
  - – Must authorize WTPs connecting to ACs
  - – Possessing a certificate signed by *someone* is not sufficient for authorization

{CAPWAP Security Interactions }

- Need CAPWAP protocol policy such that:
  - AC ↔ AAA
    - Authentication is unique, strong, mutual, and explicit
    - Communications protected by strong ciphersuite
  - STA ↔ AAA
    - Authentication is unique, strong, mutual, and explicit
    - Communications protected by strong ciphershite
  - STA ↔ WTP
    - Communications protected by strong ciphersuite
    - WEP is NOT RECOMMENDED
  - Management ↔ AC
    - Authentication is unique, strong, mutual, and explicit
    - Communications protected by strong ciphershite