Link Security
A Tutorial

Bill McIntosh

Fortress Technologies, Inc.

Five basic security services

- Data confidentiality
- Data integrity
- Access control and access rights
- Authentication/Roaming
- Non-repudiation

These services provide assurance against the security threats of unauthorized resource use, masquerade, unauthorized data disclosure, unauthorized data modification, and repudiation, respectively.

Part 1: What is Link Level Security?

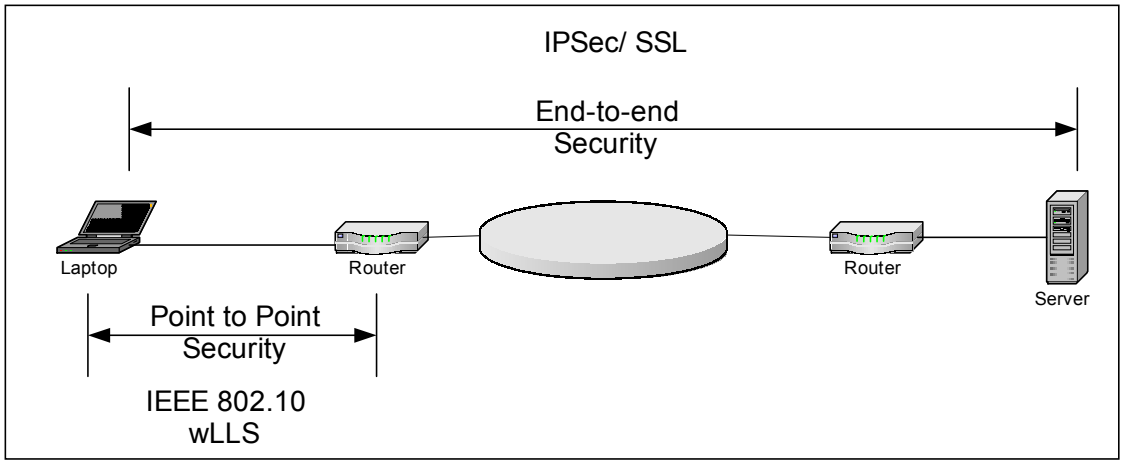
We need to define what is link level security and why we need it?

Link Layer Security?

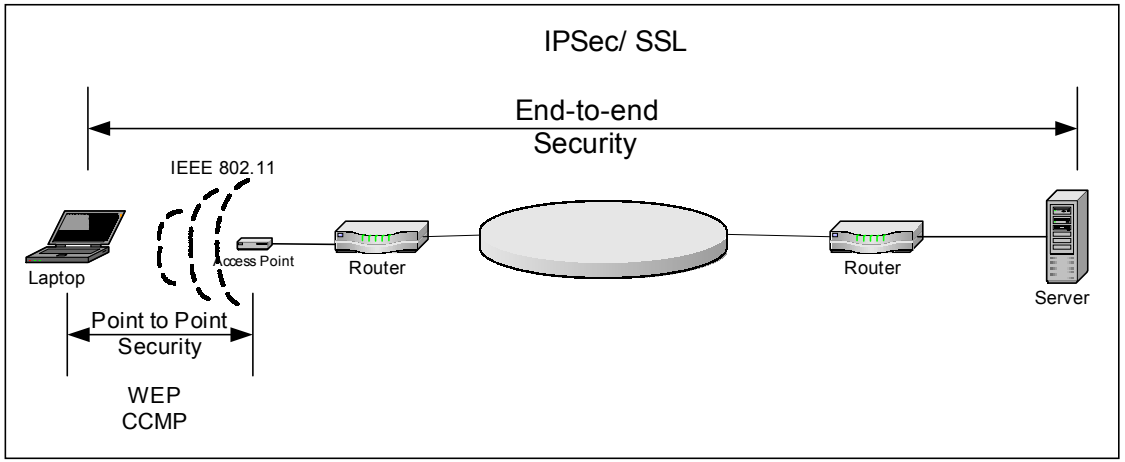
A method of securing a packet and its information above the MAC layer on a point-to-point connection:

1. hide the data contents and upper layer (above layer two) protocol information.
2. protect a packet from having its contents changed.
3. limit who or what is allowed to gain access to the overall network through the point-to-point connection.
4. limit denial of service attacks on a point-to-point segment.
5. eliminate denial of service attacks being perpetrated further in the network.

Link Layer and Upper Layer



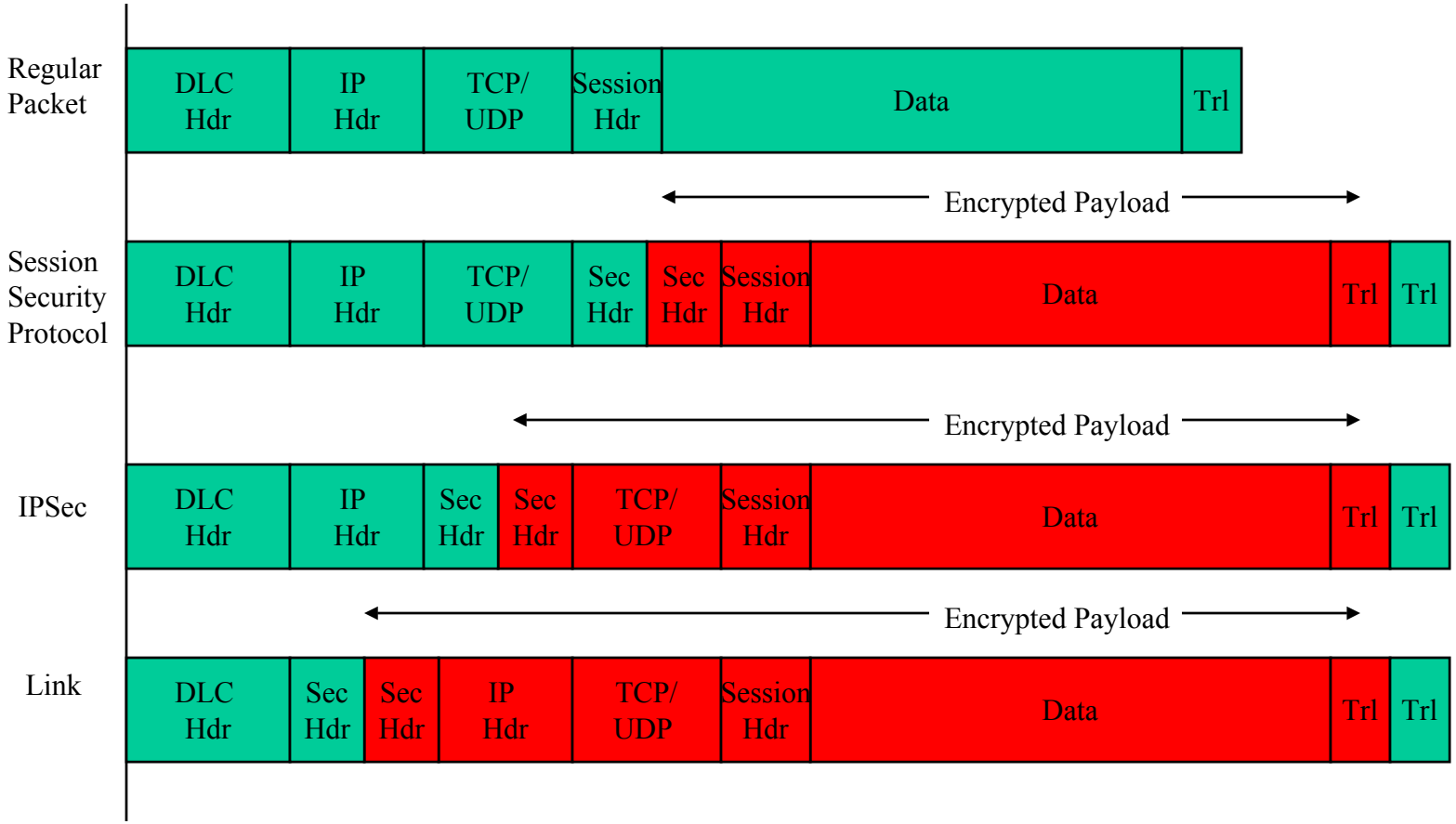
MAC Layer and Upper Layer



Why is it Needed?

- Many forms of data link technologies are vulnerable to compromise:
  - WLAN
  - WPAN (Bluetooth)
  - Fixed Wireless
  - Any Public Segment
- Two Rules of Thumb:
  - It's the responsibility of the network provider that every link in the network is protected (i.e. Link Level Security).
  - It's the responsibility of the user and application provider that the application is secure (i.e. SSL, IPSec, Application Security).

Packet Layouts



Part 1 Conclusion

- Answered what link layer security is and why it is needed .
  - Cannot view IP or other upper layer header information (such as IP addresses):
    - With IP addresses exposed, hackers can easily compromise a network.
    - ARP poisoning Denial-of-Service attacks can be launched if IP header information is not protected
  - You can't fool with my packet and cause damage.
  - If no end-to-end security protocol (like IPSec) is used, it will guarantee that, at least on that segment, no one will view or compromise by message.
  - A hacker cannot attach to that segment to steal valuable network bandwidth.
  - Control who enters and where they go.

Part 2: The Mechanics

What are the protocols, technologies and methods that make up link level security?

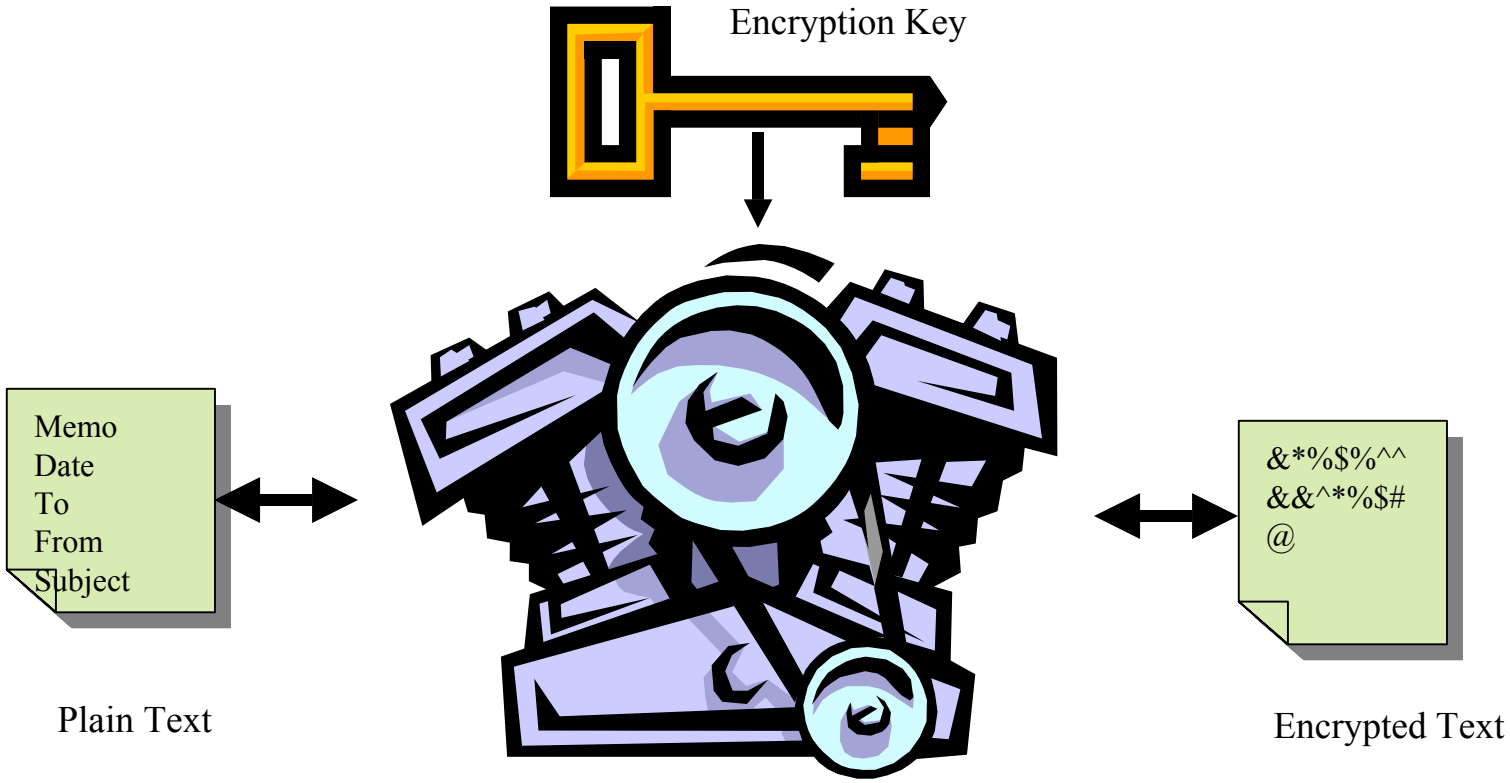
Here they are!

- Data confidentiality
  - Encryption
  - Key Management
- Data integrity
  - Hashing
  - Replay Protection
- Access Control/Rights
  - Port Components
  - 802.1x
- Authentication/Roaming
  - EAP
  - Radius
  - Roaming
- Non-repudiation

Encryption

- Encryption technology converts network messages into formats that are specially-designed to prevent third parties from accessing their contents.
- There are two types of encryption protocol:
  - Stream Cipher
  - Block Cipher

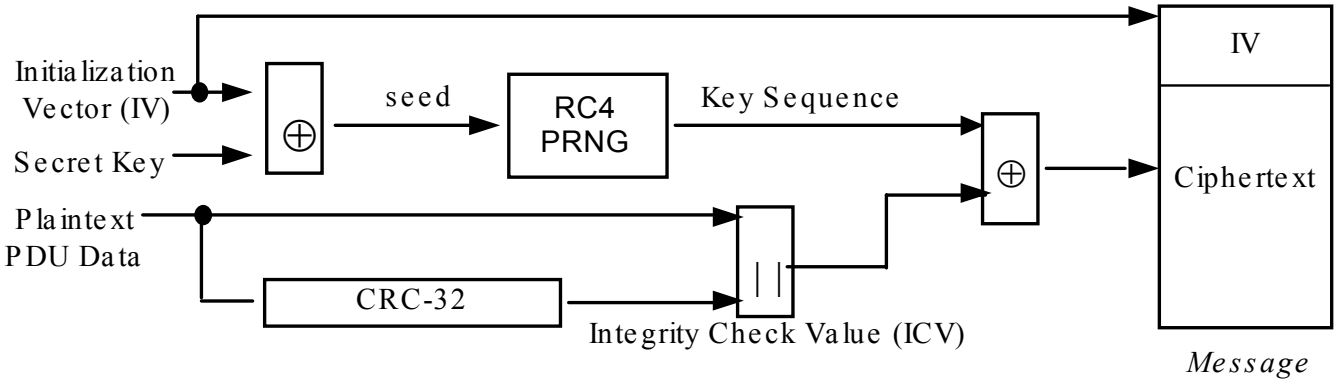
Encryption


Encryption Key
Memo
Date
To
From
Subject
Plain Text
Encryption Engine
&*%$%^^
&&^*%$#
@
Encrypted Text

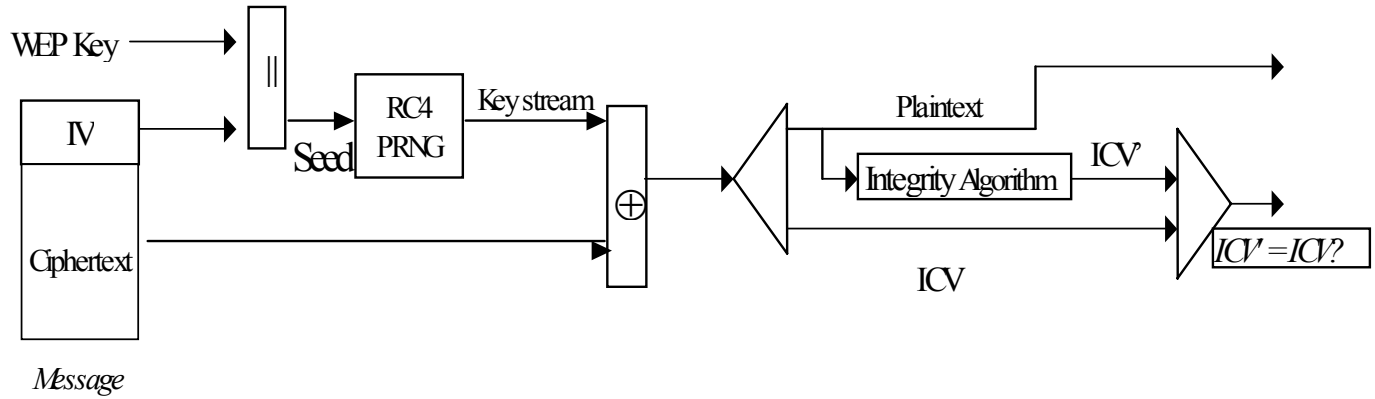
Stream Cipher

- A stream cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.
- Encryption is accomplished by combining the key stream with the plaintext, usually with the bitwise XOR operation.
- Types
  - RC-4 (Used in WEP)

Example: WEP (RC4)



a. Transmit



b. Receive

Block Cipher

- A block cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.
- Types
  - DES
  - Triple DES
  - AES

Modes of Operation

- The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form).
- Encryption algorithms are seldom used directly, cryptographic mode is used instead.
- A cryptographic mode usually combines:
  - the basic cipher
  - some sort of feedback
  - some simple operations
- Ensures that an identical block of text produces different encrypted data.

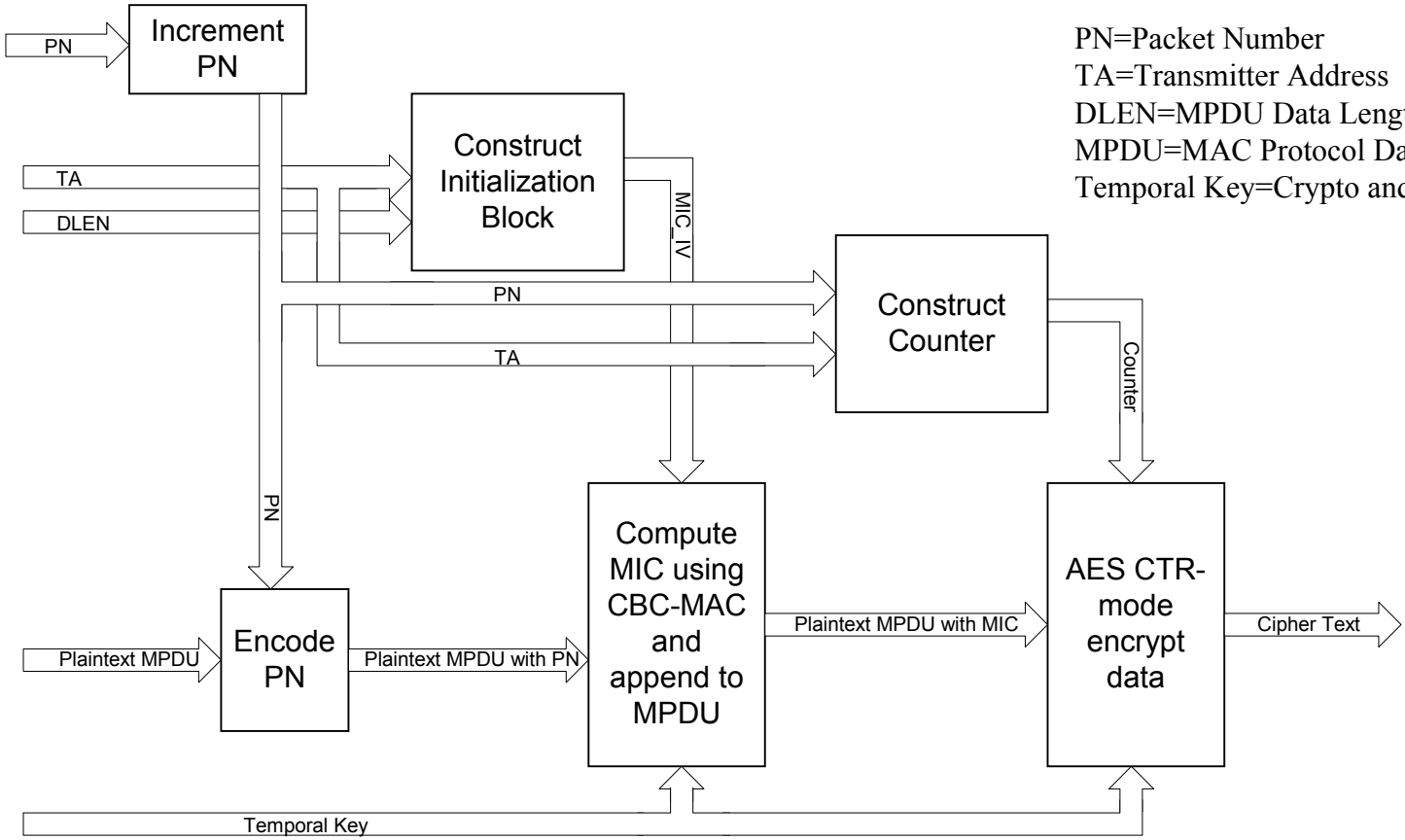
Some Modes

- Some modes of operation for use with an underlying symmetric key block cipher algorithm:
  - Electronic Codebook (ECB),
  - Cipher Block Chaining (CBC),
  - Cipher Feedback (CFB),
  - Output Feedback (OFB),
  - Counter (CTR).
  - Counter with *Cipher Block Chaining Message Authentication Code* (CCM),

Example: IEEE 802.11i Mode

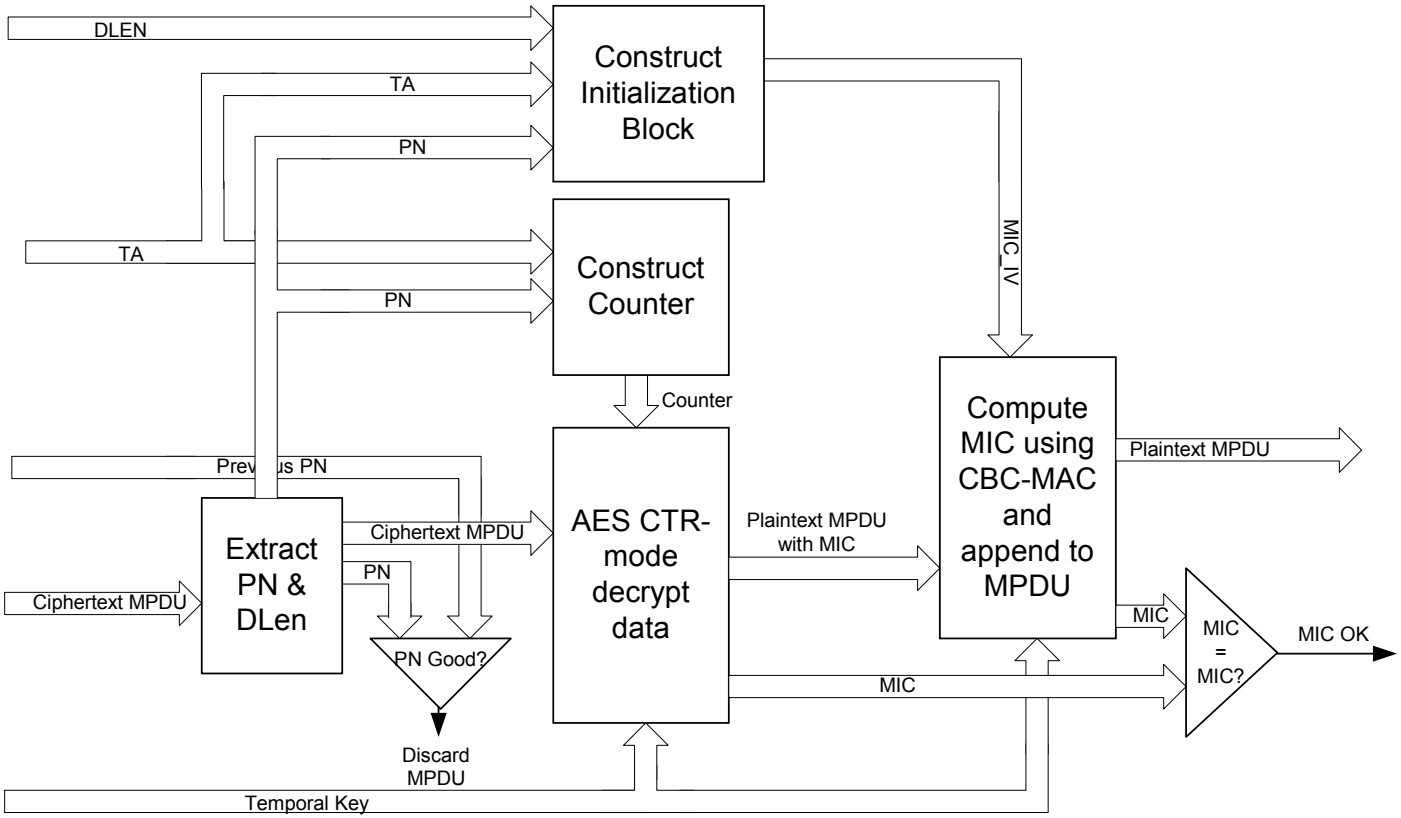
- Defines the CCMP protocol.
- Based on AES using the CCM mode of operation.
- The CCM mode combines:
  - ***Counter*** (CTR) mode privacy and;
  - ***Cipher Block Chaining Message Authentication Code*** (CBC-MAC) authentication.

Example: CCMP Encapsulation



PN=Packet Number
TA=Transmitter Address
DLEN=MPDU Data Length
MPDU=MAC Protocol Data Unit
Temporal Key=Crypto and Integrity Key

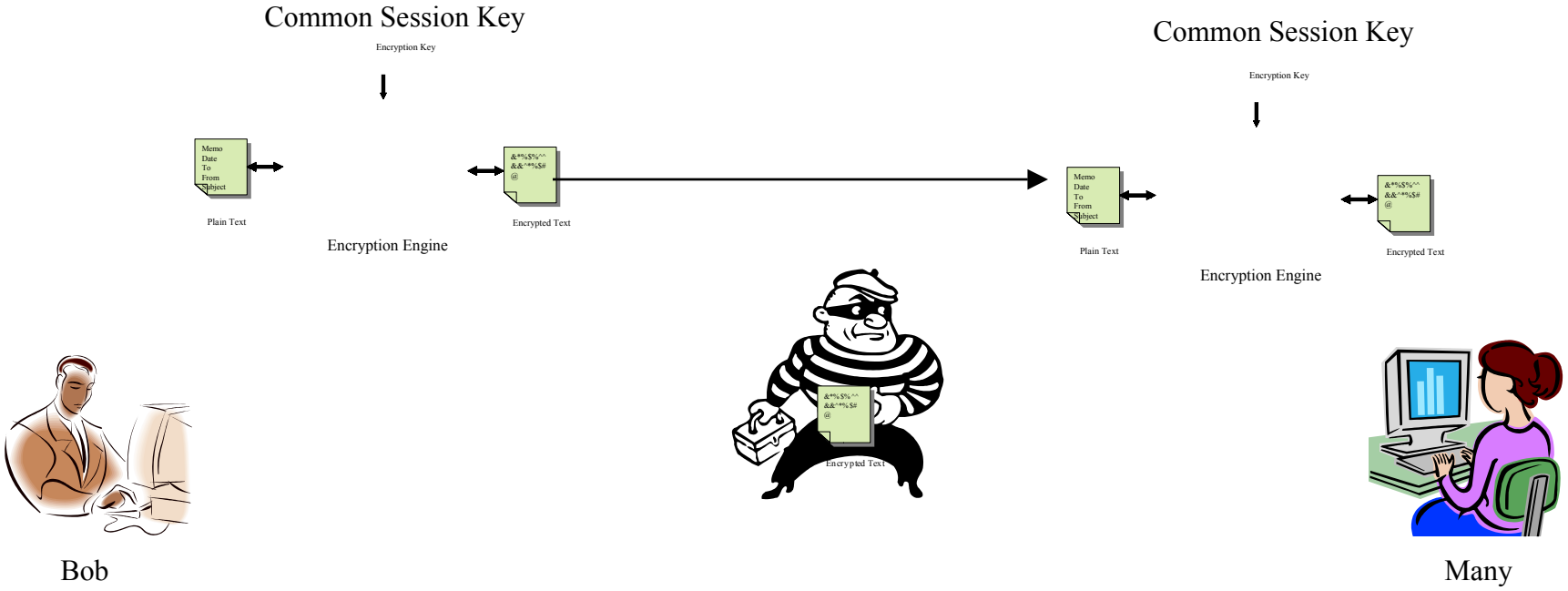
Example: CCMP Decapsulation



Key Management

- This is how you come up with the keys that will be used for encryption and authentication.
- Two kinds:
  - Shared Static Keys
  - Dynamic Keys
    - Generally-speaking, there are three types of dynamic key establishment techniques:
      1. techniques based on asymmetric (public key) algorithms,
      2. techniques based on symmetric (secret key) algorithms.
      3. hybrid techniques are also commonly used, whereby public key techniques are used to establish symmetric (secret) key encryption keys, which are then used to establish other symmetric (secret) keys.

Shared Static Key

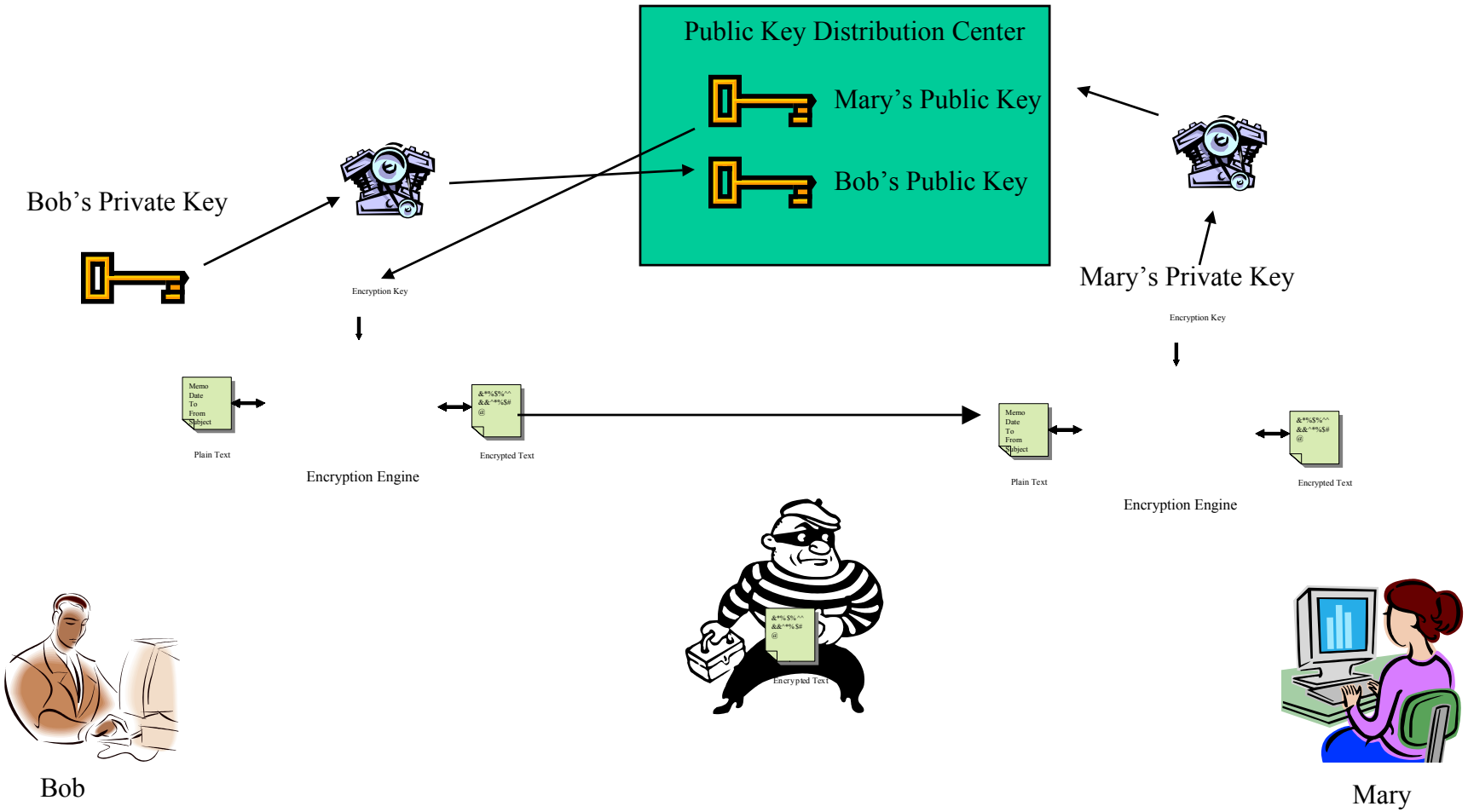


Public Key Algorithms

Different key on each side

- RSA
- Knapsack
- El-Gamal
- Elliptic Curve Cryptosystems

Public Key

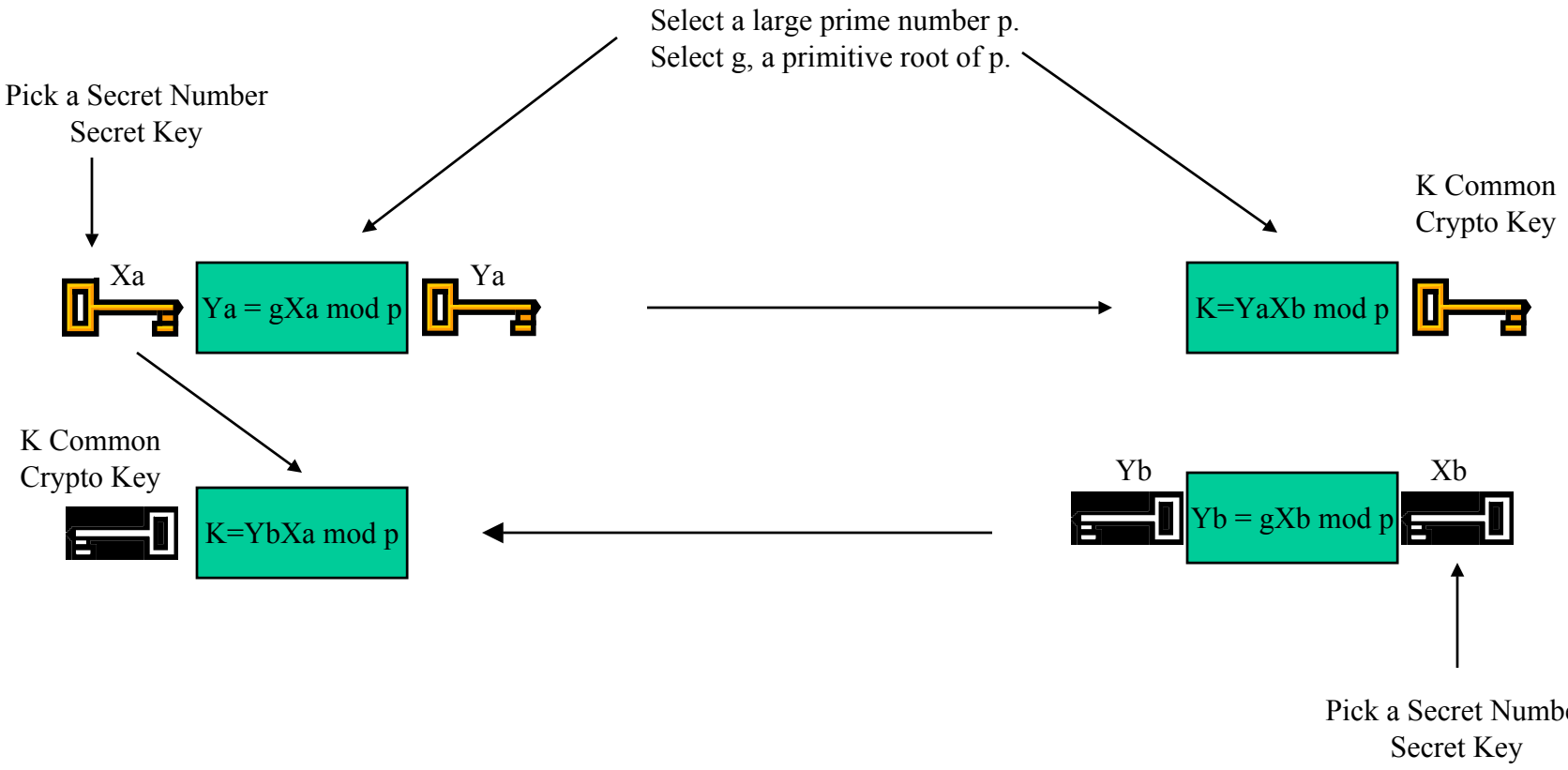

Public Key Distribution Center
Mary's Public Key
Bob's Public Key
Bob's Private Key
Encryption Key
Mary's Private Key
Encryption Key
Memo
Date
To
From
Subject
Plain Text
Encryption Engine
Encrypted Text
Plain Text
Encryption Engine
Encrypted Text
Encrypted Text
Bob
Mary

Secret Key Algorithms

Same key on each side.

- DES
- Triple DES
- AES

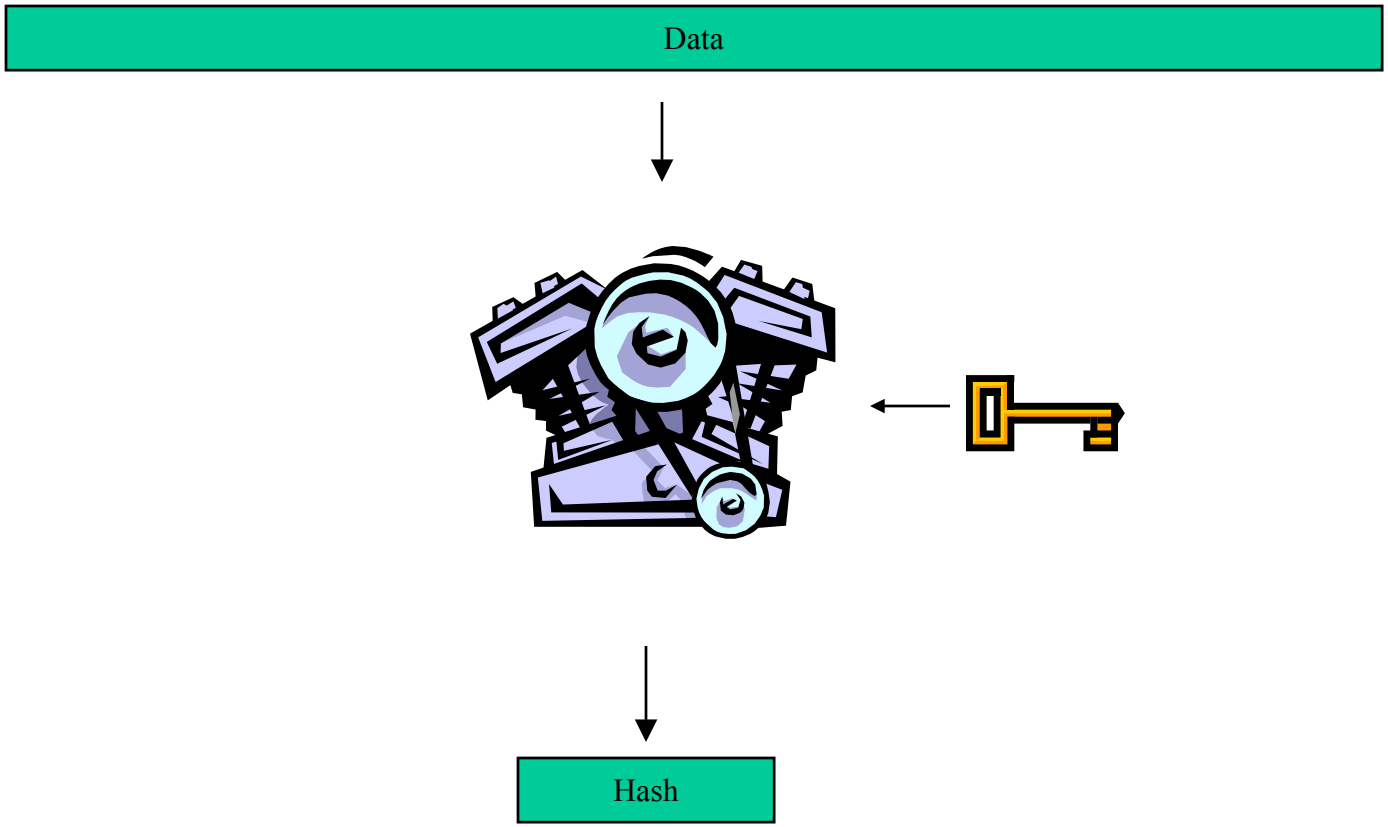
Agreeing on a Secret Key Diffie-Hellman



Data Integrity

- The integrity of a packet is checked by using a secure hash algorithm.
- Hash functions take a message as input and produce an output referred to as a *hashcode*, *hash-result*, *hash-value*, or simply *hash*.
- Hash functions are used for data integrity in conjunction with digital signature schemes, where for several reasons a message is typically hashed first, and then the hash-value, as a representative of the message, is signed in place of the original message.
- Unkeyed or a keyed hash function.

Hash



Unkeyed Hash Algorithms

- Hash functions based on:
  - *block ciphers,*
  - *customized hash functions,*
  - *hash functions,*
  - *modular arithmetic.*

Keyed Hash (MAC/MIC)

- A distinct class of hash functions, called message authentication codes (MACs) or message integrity code (MICs), allows message authentication by symmetric techniques.
- MAC algorithms may be viewed as hash functions which take two functionally distinct inputs, a message and a secret key, and produce a fixed-size (say n-bit) output, with the design intent that it be infeasible in practice to produce the same output without knowledge of the key.

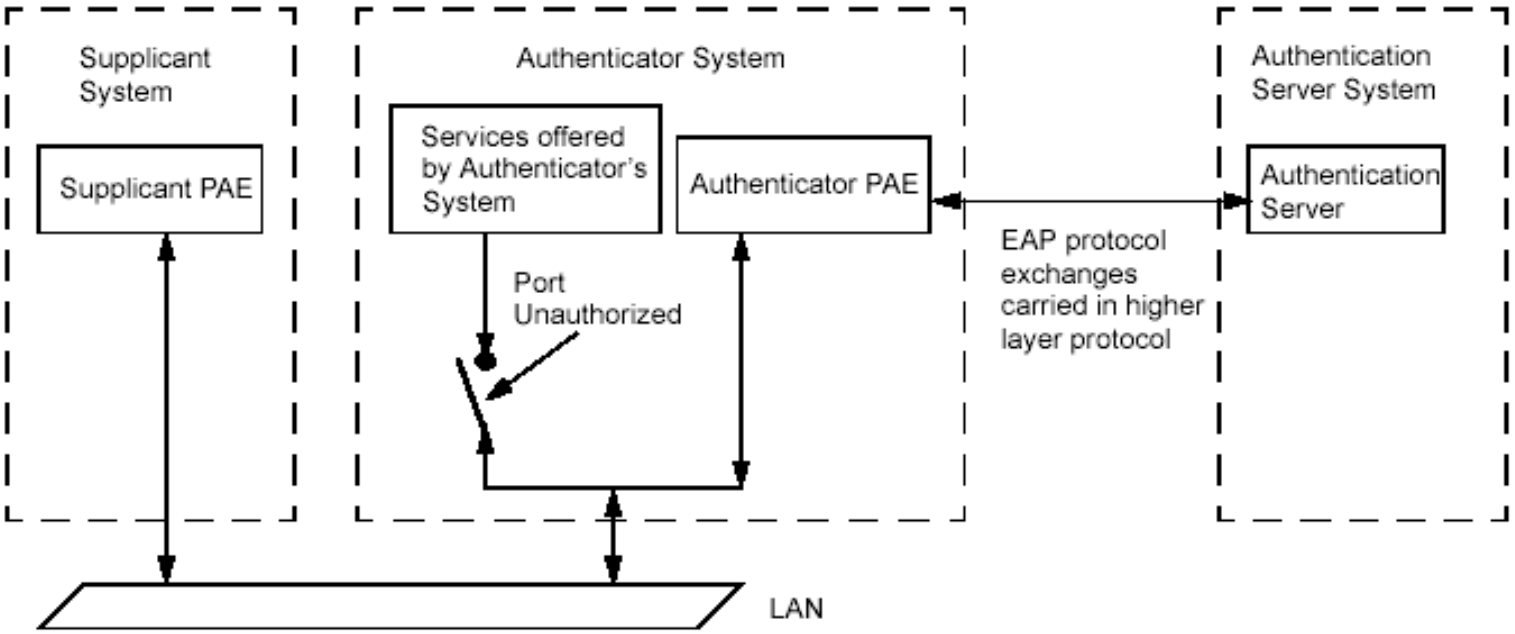
Anti-Replay

- Anti-replay ensures packet security by making it impossible for a hacker to intercept message packets and insert changed packets into the data stream between a source computer and a destination computer.
- By detecting packets that match the sequence numbers of those that have already arrived, the anti-replay mechanism helps to ensure that invalid packets are discarded.

Access Control/Access Rights

- Access Control is any mechanism by which a system grants or revokes the right to access a network.
- Access Control can be performed by allowing or denying access base on:
  - a user requiring to submit a Login and Password that will be sent to an authentication server for approval.
  - The user has a particular device that would be approved by an access control server.
  - The user contacts an administrator, the administrator configures packet filters.
- Access Rights is any mechanism that limit where in a network or on a devices a user can access.

Authentication System 802.1x Model



RADIUS Servers

- **RADIUS (Remote Authentication Dial-In User Service)**
- An IETF-defined protocol for administering and securing remote access to a network.
- User Login and Password information is forwarded to a RADIUS authentication server that validates the user and returns the information necessary for the access server to initiate a session with the user.
- A dictionary file kept in the RADIUS database determines the types of attributes that can be included in the user profile. The user repeats this process to initiate every session.

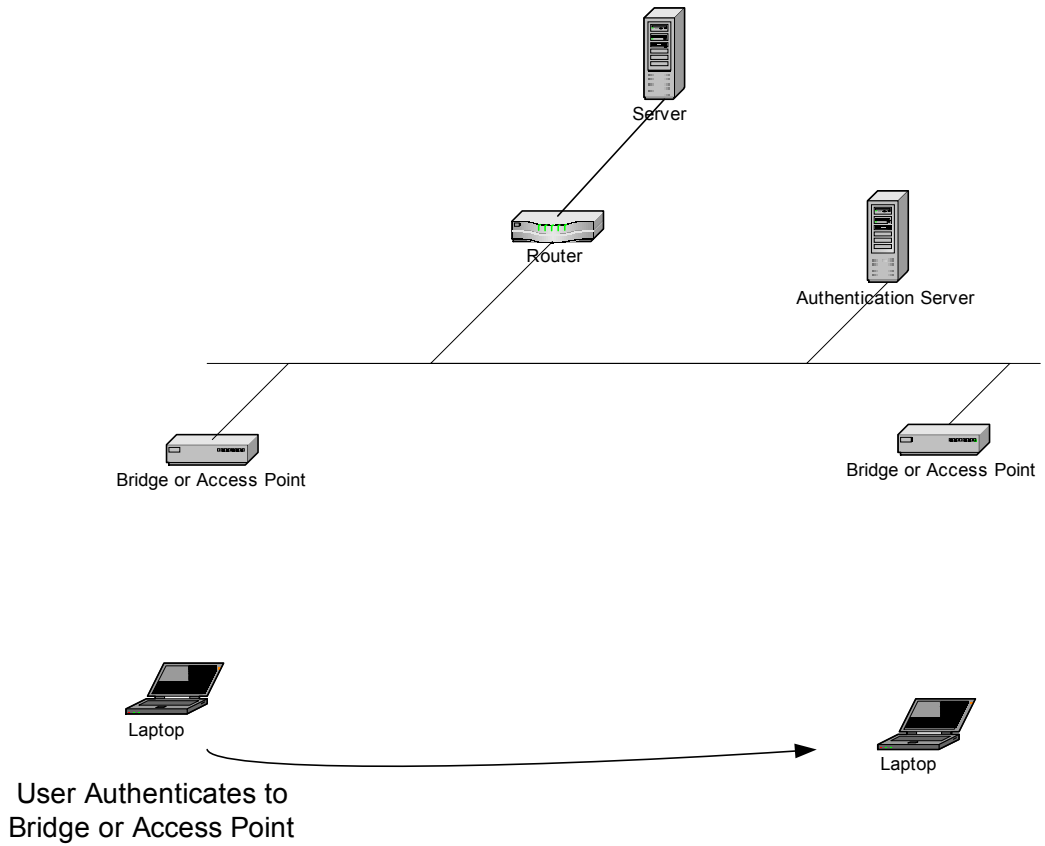
Forms of Authentication

- Device Authentication
  - Used to allow a particular device onto a network (My PDA can go on a network).
- User Authentication
  - Used to allow a particular user onto a network (Bill is allowed on the engineering network).
- Hybrid
  - A user has access to a network with a particular device.

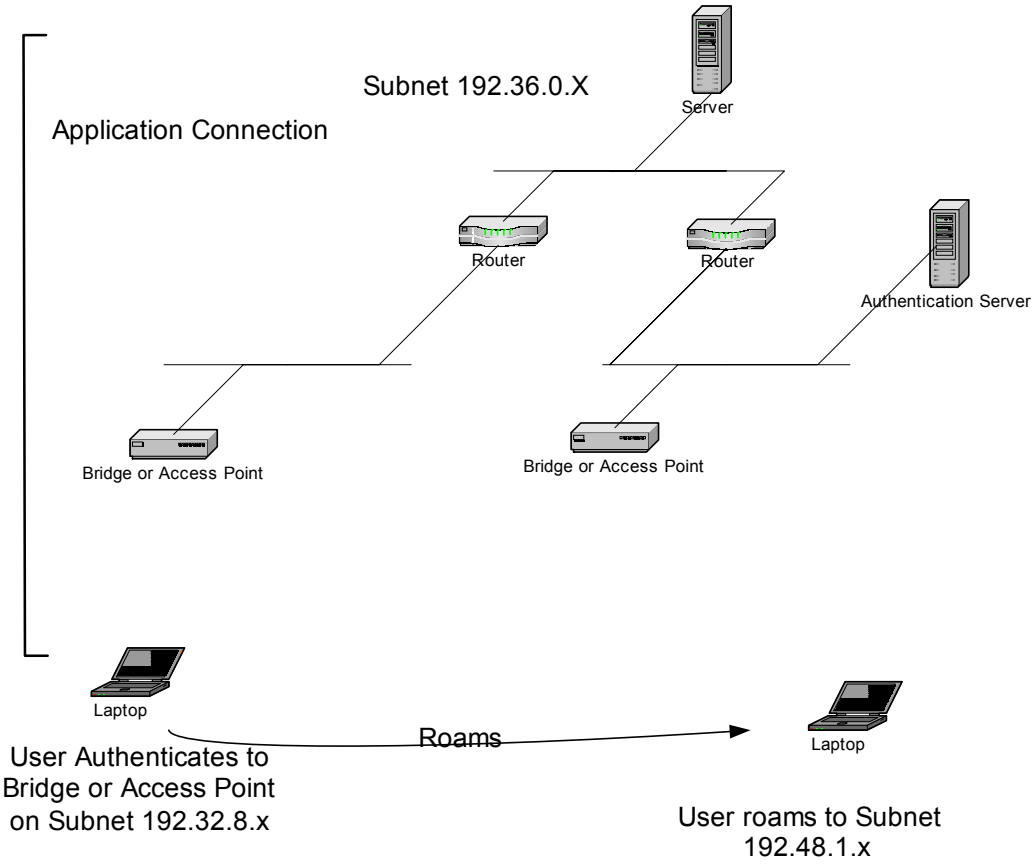
Roaming

- Three types of roaming:
  - Roam between authenticator gateways on the same IP subnet without requiring new user and password input.
  - Roam between authenticator gateways on different IP subnets without requiring new user and password input.
  - Roam between authenticator gateways on different IP subnets while perserving IP addressing and state information.

Roaming same Subnet



Roaming between Subnets



Non-Repudiation

- Usually a higher layer function.
- "Non-repudiation with proof of origin" provides the recipient of data with evidence that proves the origin of the data, and thus protects the recipient against an attempt by the originator to falsely deny sending the data. This service can be viewed as a stronger version of a data origin authentication service, in that it proves authenticity to a third party.

Part 2: Conclusion

- Five areas of security.
- Two type of encryption algorithm.
- Modes of Operation
- Data Integrity and Hash
- Anti-Replay
- Access Control/Rights/Authentication/Roaming
- Non-Repudiation

Part 3: Some MAC/Link Protocols

- IEEE 802.11i
- IEEE 802.10
- Wireless Link Level Security Protocol

Problems with WEP

- 40-bit WEP key
- Weak IVs
- IV Replay
- Known packet attack
- Known packet start attack
- Bit Flipping attack

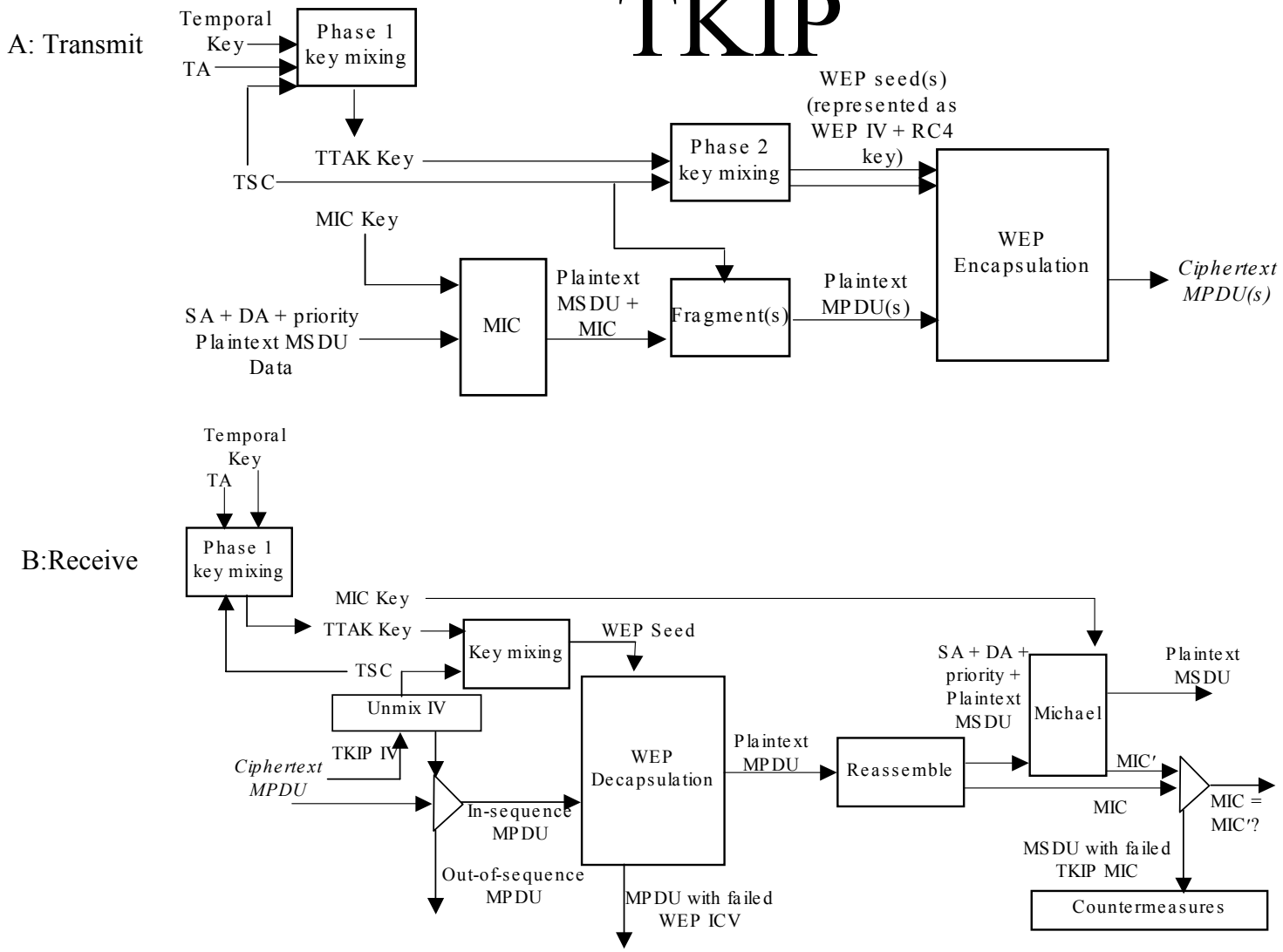
IEEE 802.11i

- A Robust Security Network provides a number of security features to the IEEE 802.11 architecture. These features notably include:
  - improvement specifically for legacy wLAN equipment in TKIP.
  - enhanced data security and encapsulation mechanism, called CCMP
  - key management algorithms;
  - dynamic cryptographic keys;
  - enhanced authentication mechanisms for both APs and STAs;
- An RSN makes extensive use of IEEE 802.1X protocols with IEEE 802.11 to provide the authentication and key management.
- An RSN introduces several components into the IEEE 802.11architecture. These components are only present in RSN systems:
  - The first new component is an ***IEEE 802.1X Port***.
  - A second component is the ***Authentication Server*** (AS).

TKIP fixes WEP

- The Temporal Key Integrity Protocol (TKIP) is a cipher suite enhancing the WEP protocol on pre-RSN hardware.
- TKIP computes the MIC over the MSDU source address, destination address, priority, and data, and appends the computed MIC to the MSDU; TKIP discards any MIC padding prior to appending the MIC.
- TKIP fragments the MSDU into one or more MPDUs; TKIP assigns a monotonically incrementing TSC value to each MPDU it generates, taking care that all the MPDUs generated from the same MSDU use counter values from the same 16-bit counter space.
- For each MPDU, TKIP uses the key mixing function to compute the WEP seed.
- TKIP represents the WEP seed as a WEP IV and RC4 key, and passes these with each MPDU to WEP for encapsulation. WEP uses the WEP seed as a WEP default key, identified by a key id associated with the temporal key.

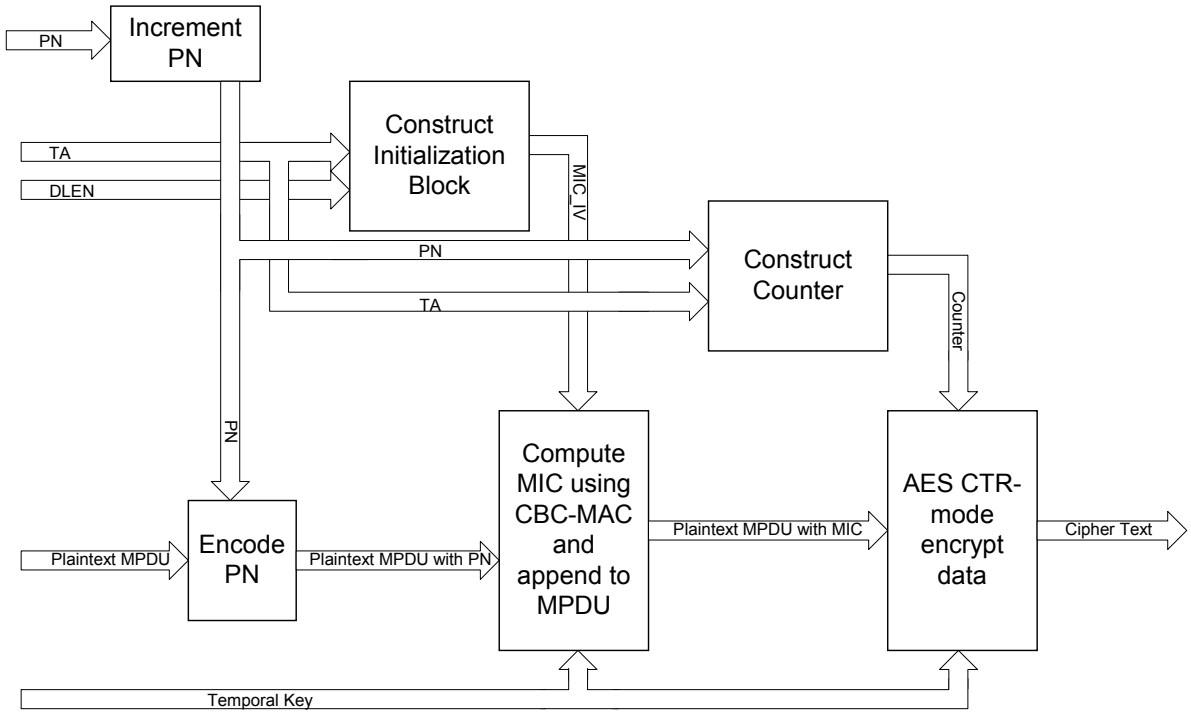
TKIP


A: Transmit
Temporal Key
TA
Phase 1 key mixing
TTAK Key
TSC
Phase 2 key mixing
WEP seed(s) (represented as WEP IV + RC4 key)
MIC Key
MIC
Plaintext MSDU + MIC
SA + DA + priority Plaintext MSDU Data
Fragment(s)
Plaintext MPDU(s)
WEP Encapsulation
Ciphertext MPDU(s)
B:Receive
Temporal Key
TA
Phase 1 key mixing
MIC Key
TTAK Key
TSC
Key mixing
WEP Seed
Unmix IV
TKIP IV
Ciphertext MPDU
In-sequence MPDU
Out-of-sequence MPDU
WEP Decapsulation
MPDU with failed WEP ICV
Plaintext MPDU
Reassemble
SA + DA + priority + Plaintext MSDU
Michael
Plaintext MSDU
MIC′
MIC
MIC = MIC′?
MSDU with failed TKIP MIC
Countermeasures

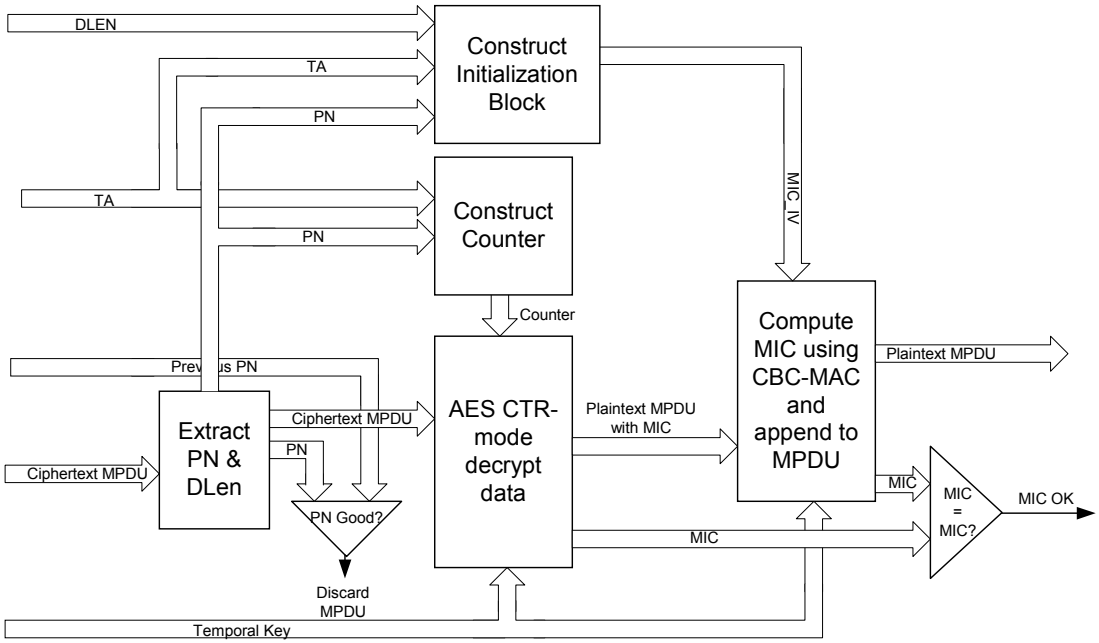
CCMP

- The CCMP protocol is based on AES using the CCM mode of operation.
- The CCM mode combines ***Counter*** (CTR) mode privacy and ***Cipher Block Chaining Message Authentication Code*** (CBC-MAC) authentication.
- CCM uses the same temporal key for both CTR mode and the CBC-MAC.
- CCM assumes a fresh temporal key for every session. Reuse of a temporal key and packet number voids all security guarantees.

CCMP encapsulation block diagram



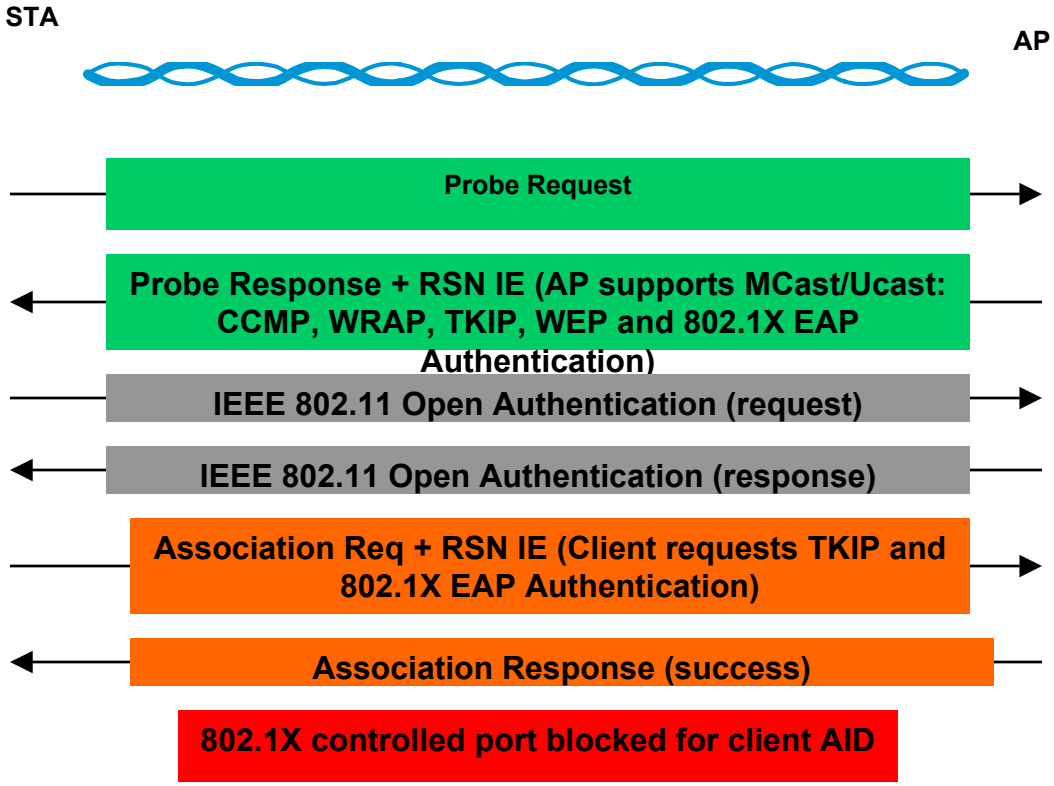
CCMP decapsulation block diagram



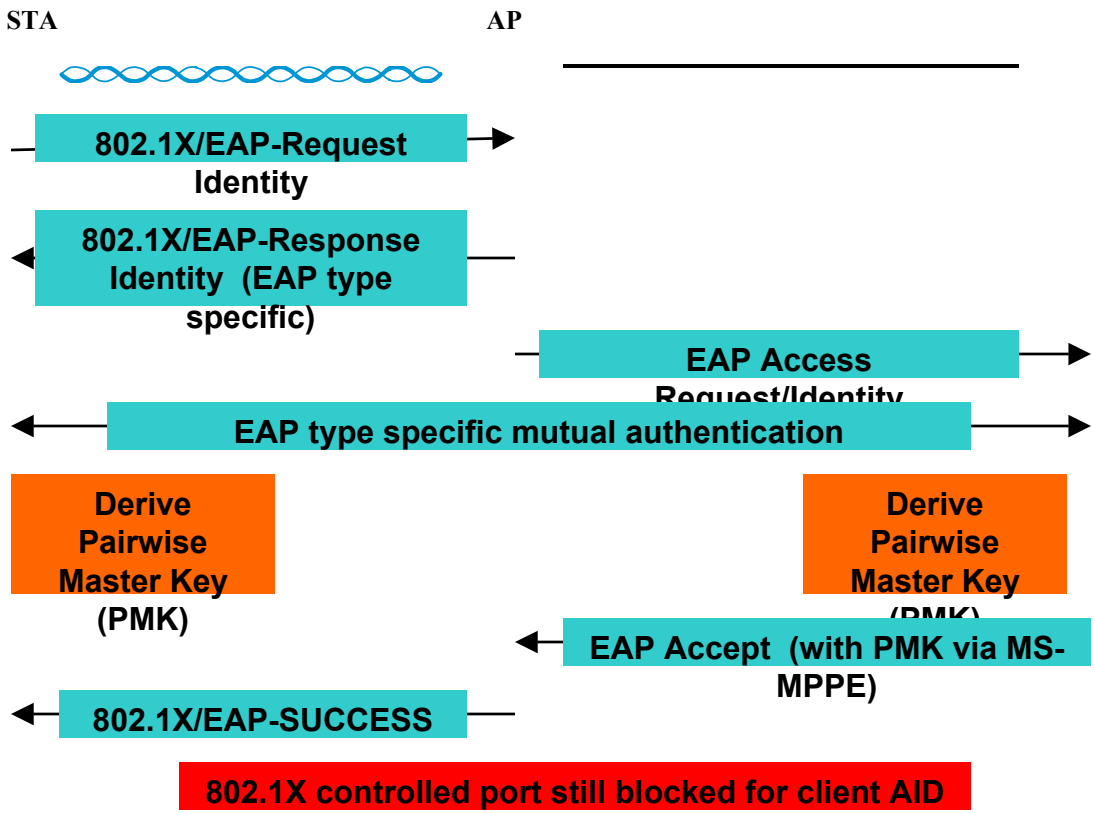
RSN security association management

- IEEE 802.11 uses the notion of a security association to describe secure operation.
- Secure communications are possible only within the context of a security association, as this is the context providing the state—cryptographic keys, counters, sequence spaces, etc.—needed for correct operation of the IEEE 802.11 cipher suites.

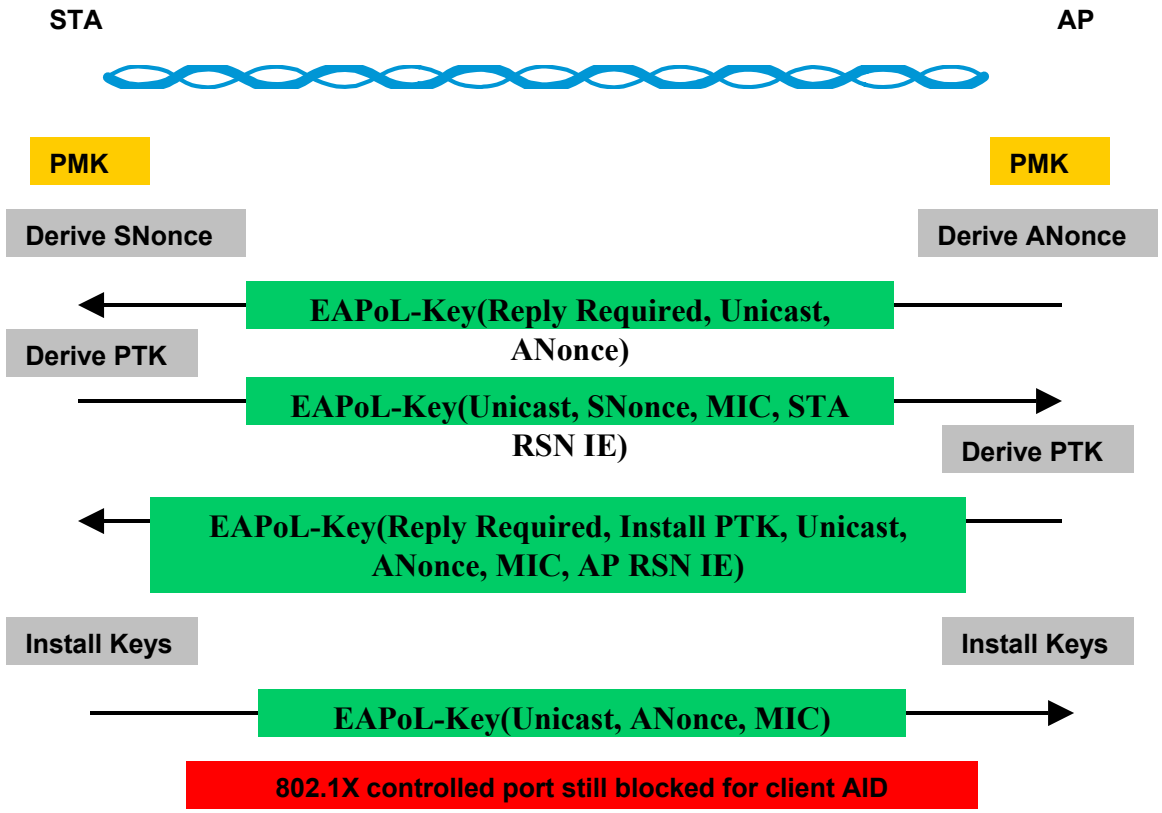
Establishing the IEEE 802.11 connection and negotiation



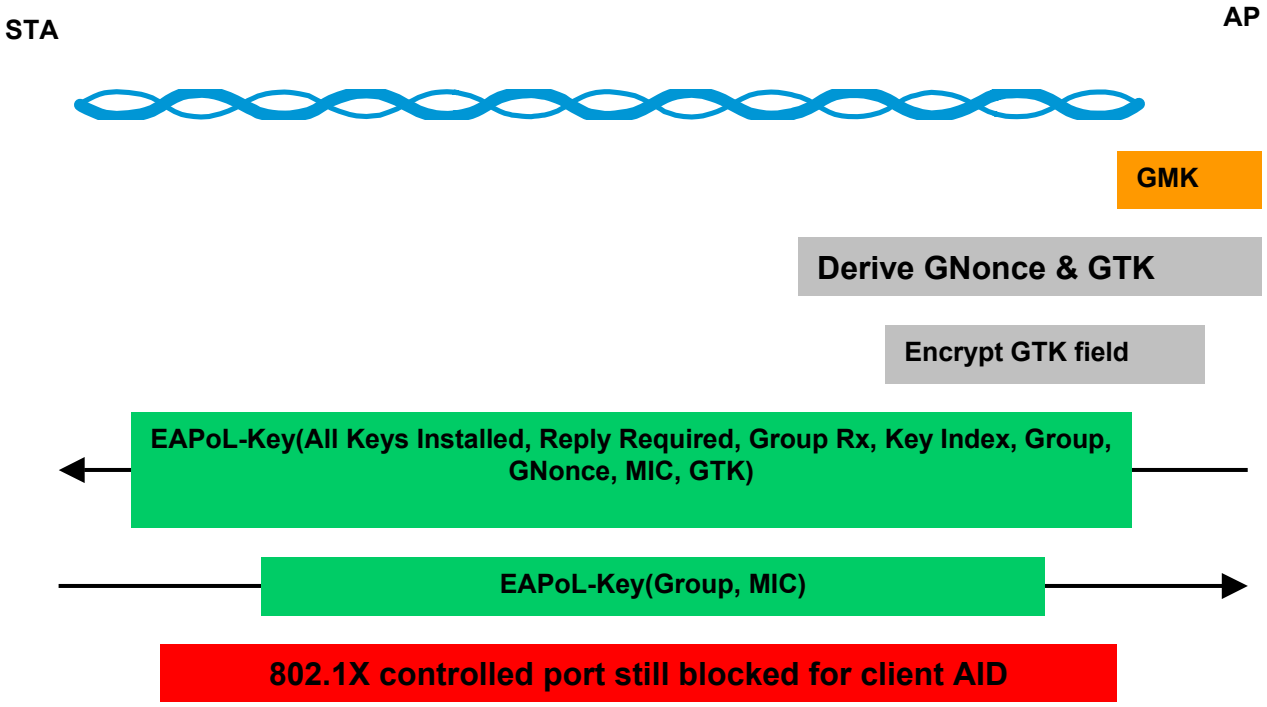
IEEE 802.1X EAP authentication



Establishing pairwise keys



Group key delivery



IEEE 802.10

- This entity provides services that permit the secure exchange of data at Layer 2.
- As part of the Logical Link Control (LLC) sublayer, the SDE entity provides a connectionless service immediately above the Medium Access Control (MAC) sublayer in IEEE 802 LANs and MANs.
- It provides security across the MAC sublayer using cryptographic mechanisms and security services provided transparently at the boundary to the LLC entity.
- Develop its own Key Management Protocol

IEEE 802.10

Structure of the SDE PDU

802.10 Key Management

- The key management model and protocol support three key distribution techniques:
  - manual key distribution,
  - center-based key distribution,
  - certificate-based key distribution.

Manual Distributed Key

Center Based Key Distribution

Center-based key translation

Certificate-based key distribution

Multicast key distribution

wLLS

- Link Level Security Protocol
- AES, 3DES
- Dual Diffie-Hellman Key Engine
- SHA-1 Packet Integrity
- Anti Replay
- Device Authentication
- User Authentication using EAP
- FIPS

wLLS Packet

wLLS Key Negotiation

Threat Protection

- *known-key attack*. In this attack an adversary obtains some keys used previously and then uses this information to determine new keys.
- *replay*. In this attack an adversary records a communication session and replays the entire session, or a portion thereof, at some later point in time.
- *impersonation*. Here an adversary assumes the identity of one of the legitimate parties
- in a network.
- *dictionary*. This is usually an attack against passwords. Typically, a password is stored in a computer file as the image of an unkeyed hash function. When a user logs on and enters a password, it is hashed and the image is compared to the stored value. An adversary can take a list of probable passwords, hash all entries in this list, and then compare this to the list of true encrypted passwords with the hope of finding matches.

Attacks on protocols

- *forward search*. This attack is similar in spirit to the dictionary attack and is used to decrypt messages. An example of this method was cited in Example 1.60.
- *interleaving attack*. This type of attack usually involves some form of impersonation in an authentication protocol.

Part 3: Conclusion

- The new IEEE 802.11i recommendations:
  - TKIP for legacy wLAN products
  - CCMP for highly secure networks
  - IEEE 802.1x Port Control
  - Authentication and Radius
- IEEE 802.10
- wLLS
- Threats

Editorial Comment

- Proponent of using 802.11i.
- Millions of wireless devices will support 802.11i very soon.
- I believe there are only minor changes to make it a link level security protocol.
- The changes have to do with:
  - embedded functions at the MAC layer;
  - fragmentation.
- Our goal would be to secure a point-to-point connection from a gateway across access points and bridges to mobile devices

Questions or Comments