802.11i Overview

Date: 2005-02-09

Authors:

Name	Company	Address	Phone	email
Clint Chaplin	Symbol Technologies	6480 Via Del Oro, San Jose, CA, USA 95119-1208	+1(408)528-2766	cchaplin@sj.symbol.com
Emily Qi	Intel Corporation	JF3-206, 2111 N.E. 25th Ave., Hillsboro, OR, USA 97124	+1-503-264-7799	emily.h.qi@intel.com
Henry Ptasinski	Broadcom	190 Matilda Place, Sunnyvale, CA, USA 94086	+1-408-543-3316	henryp@broadcom.com
Jesse Walker	Intel Corporation	JF3-206, 2111 N.E. 25th Ave, Hillsboro, OR, USA 97214	+1-503-712-1849	jesse.walker@intel.com
Sheung Li	Atheros Communications	529 Almanor Ave, Sunnyvale, CA, USA	+1-408-773-5295	sheung@atheros.com

Abstract

This document provides an overview of IEEE Std. 802.11i for ISO/IEC JTC1/SC6 WG1

Agenda

- Assumptions and Motivation
- Overall Architecture
- Description of 802.11i Features
- Some Complementary Standards
- On-going Work

Part I: Assumptions, Motivation, and Goals

Assumptions

- **802.11 LANs are a form *Local* Area Networks**
  - Deployed by individuals or organizations as a local resource
  - Access to other resources outside scope of 802.11i
- **Must conform to the dominant market access control model**
  - 802.11 deployers want to transform commonly held resource (local unlicensed bandwidth) into a private access controlled resource in a small neighborhood of an access point, e.g., inside one's home, corporation, or small business
  - This is how 802.11 is deployed in almost all markets worldwide
- **Protections for public WLANs not precluded, but public WLANs not the design center**
  - Numerous operator experiments with 802.11, but business models still under development
  - Public WLANs can be addressed later, after business models are established that identify unique operator requirements

Motivation

- **Meet market expectations, by delivering local control over resources**
  - Enterprises generally unwilling to admit access based on authentication credentials issued by someone else
  - Different market segments require different authentication mechanisms
- **Defuse market concern over deploying insecure wireless LANs**
  - "Raise all boats," not just improve market position of 802.11i participants
- **Balance cost and security**
  - Commercial grade cryptography only: provide only as much security as the market is willing to pay for

Goals

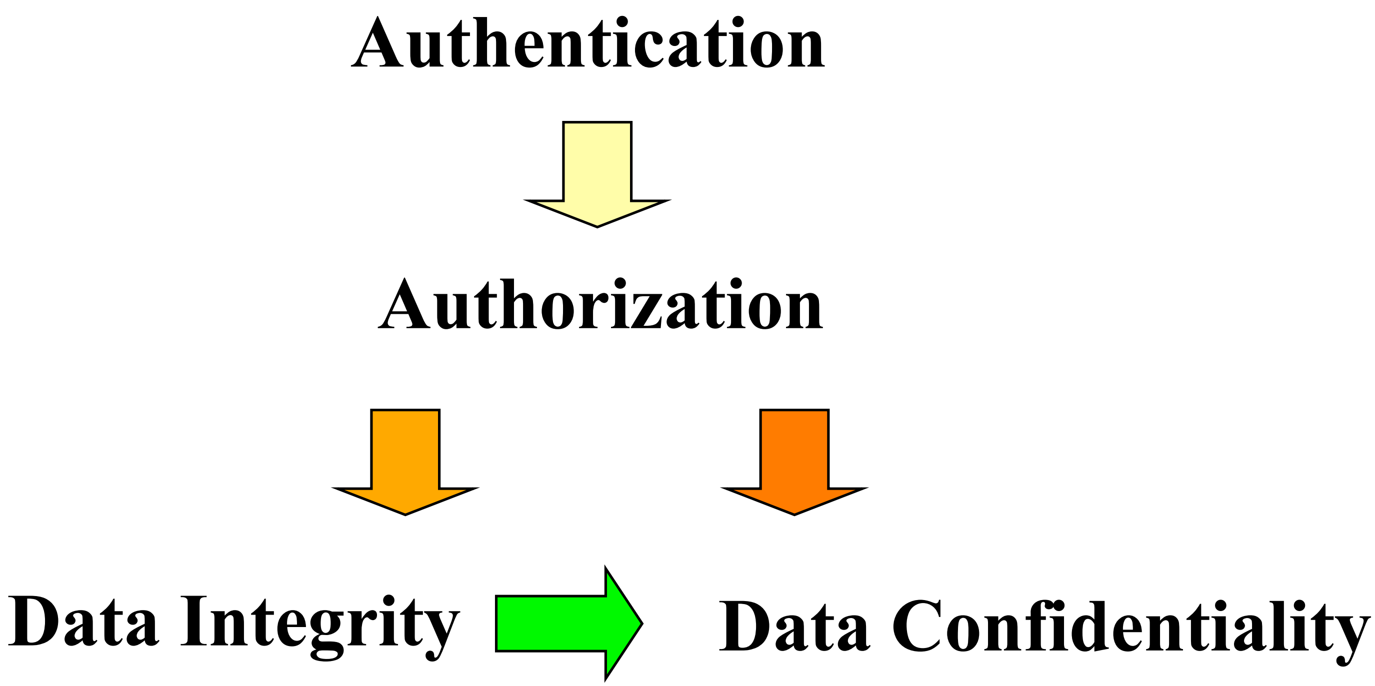
- **Develop 802.11i through a process open to all**
- **Anyone must be able to fully implement the entire standard or any part of it: no secret algorithms**
- **Market driven feature development**
  - Address all perceived security problems of WEP
  - Maximize the security achievable with existing authentication databases
  - Do NOT address problems market does not care about: it will generally neither pay for nor use such features
  - Provide backward and forward compatibility
  - Deliver as rapidly as possible
- **Separation of concerns**
  - Do not duplicate work done elsewhere, like the IETF
- **Flexible architecture adaptable to different deployment models**
  - Enterprise, Small business, consumer and home, and perhaps operator
- **Obtain outside review of design**
  - To minimize chances of another WEP

Part II:
Description of 802.11i

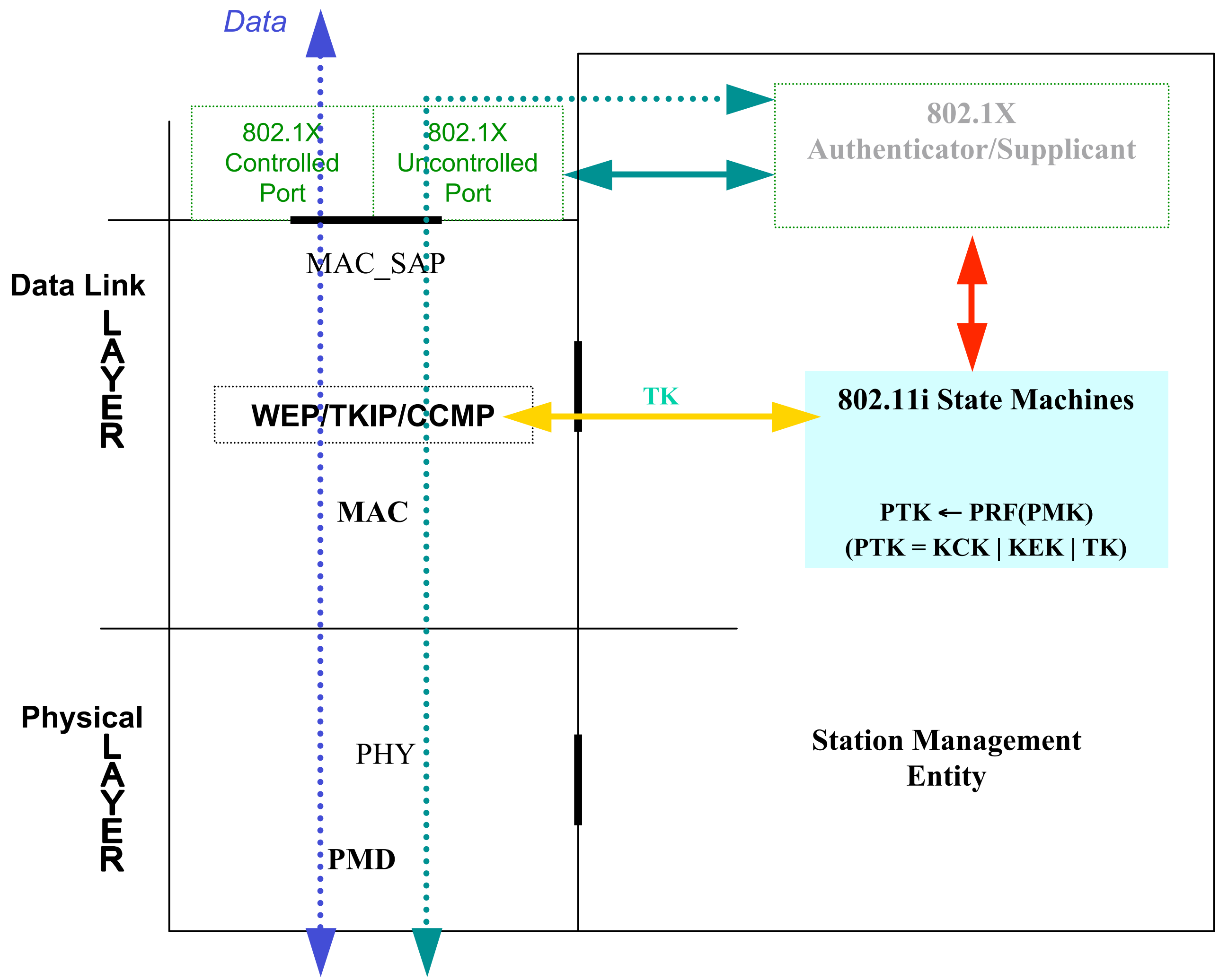
802.11i Facilities

- 802.11i Architecture
- TKIP
- AES-CCMP
- Discovery and Negotiation
- Key Management
- Coordination with Authentication

Security Service Dependencies



802.11i Architecture



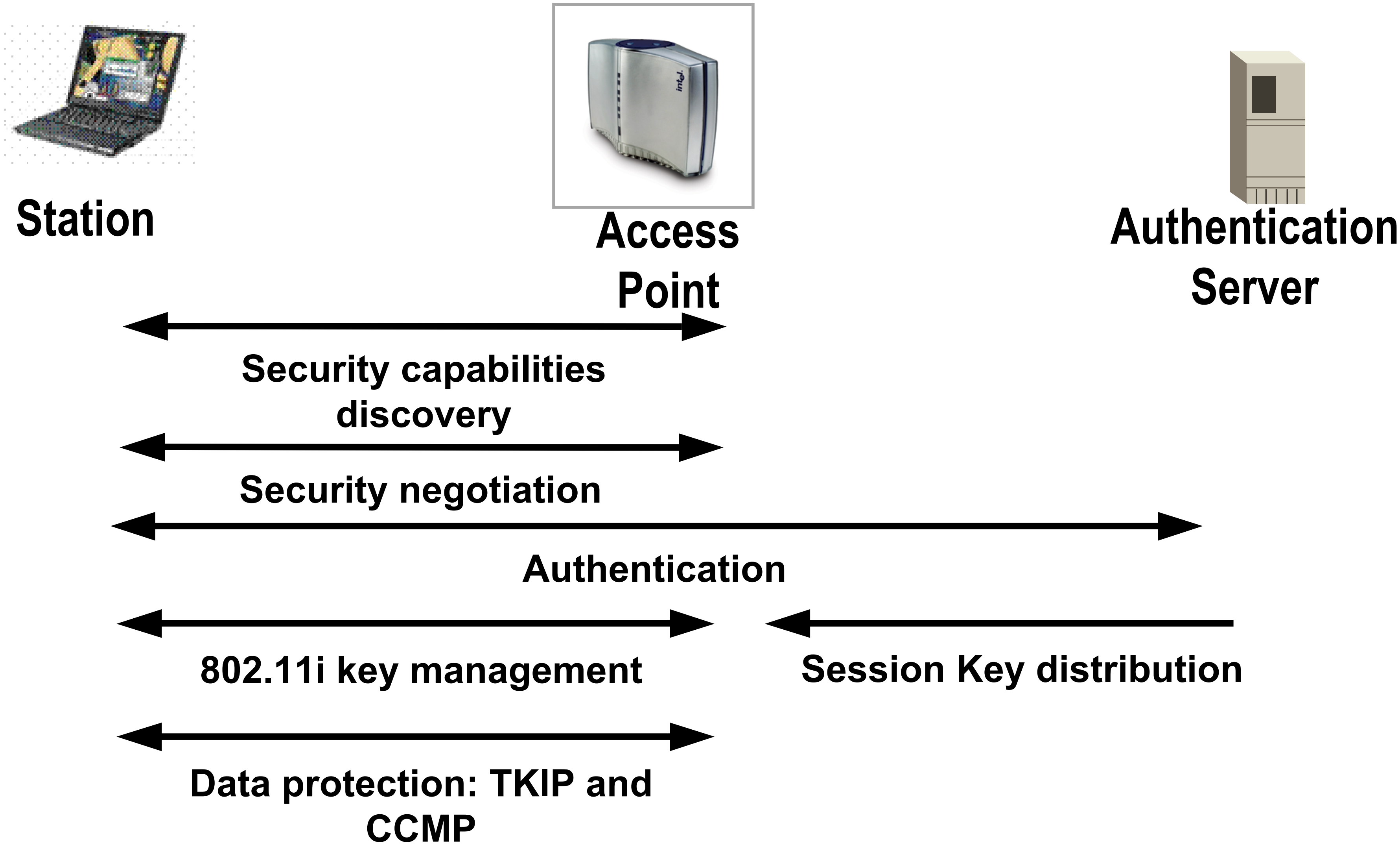
802.11i Concepts

- **AES-CCMP – all new security protocol based on AES-128 in CCM mode**
- **TKIP – designed as a software patch to upgrade WEP in already-deployed equipment**
- **WEP – the original 802.11i security protocol**
- **RSNA State Machines – exercises control over 802.11i**
- **PRF – Pseudo-Random Function, for session key construction**
- **PMK – Pairwise Master Key = session authorization token**
- **KCK – Key Confirmation Key = session "authentication" key**
- **KEK – Key Encryption Key = session key for encrypting keys**
- **TK – Temporal Key = session "encryption" key**
- **4-Way Handshake – 802.11i key management protocol**
- **RSN IE -- Data structure for advertising and negotiating security capabilities**

External Components used by 802.11i

- **802.1X – an external standard used to provide an authentication framework, coordinate authentication and key management**
- **802.1X Uncontrolled Port – passes 802.1X messages only**
- **802.1X Controlled Port – passes or blocks all other data messages**
- **802.1X Authenticator/Supplicant – local protocol entity to coordinate authentication and key management with remote entity**
- **Authentication Server (AS) – a logical construction that centralizes authentication and access control decision making**

Operating an 802.11i Link

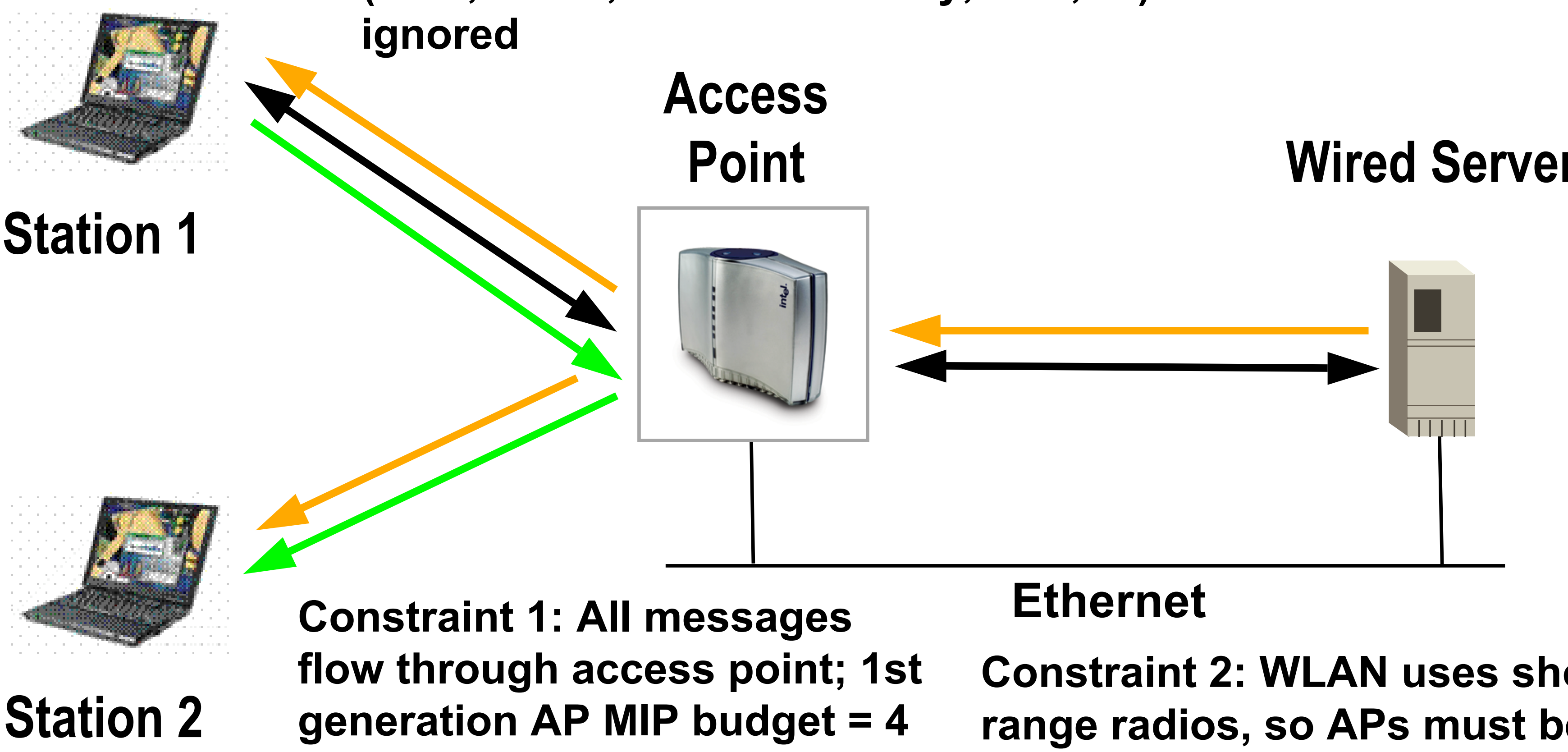


TKIP Identification and Goals

- **TKIP: *T*emporal *K*ey *I*ntegrity *P*rotocol**
- **Deploy as a software patch in already deployed equipment**
  - Must conform to 1st generation Access Point MIP budget
- **Short term only, to permit migration from existing equipment to more capable equipment without violating security constraints**
  - Patch old equipment from WEP to TKIP first
  - Interoperate between patched and unpatched first generation equipment until all have been patched
  - Finally deploy new equipment
- **Security Goals: Address all known WEP problems**
  - Prevent Frame Forgeries
  - Prevent Replay
  - Correct WEP's mis-use of encryption
  - Never reuse keys

Design Constraints

Constraint 3: Multicast integral to modern networking (ARP, UPnP, Active Directory, SLP, …) and cannot be ignored



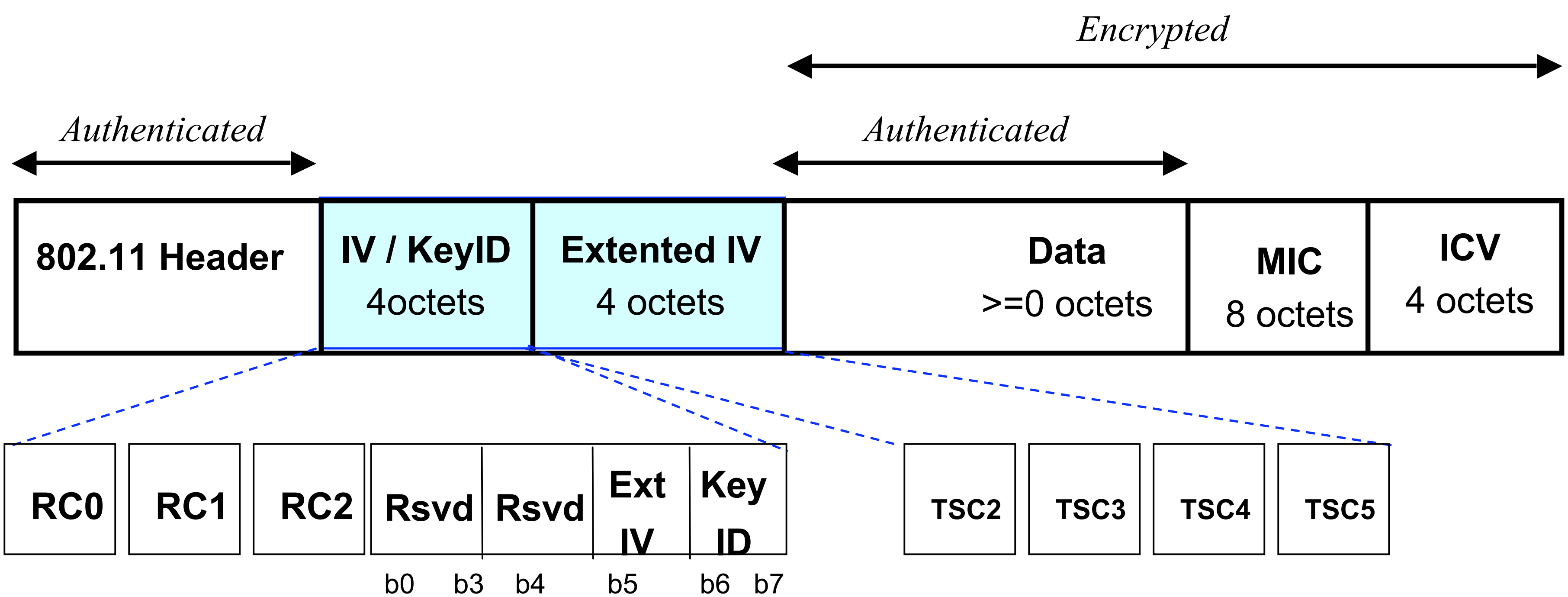
Constraint 1: All messages flow through access point; 1st generation AP MIP budget = 4 Million instructions/sec

Constraint 2: WLAN uses short range radios, so APs must be ubiquitous, so lowest cost

TKIP Overview

- **TKIP: *T*emporal *K*ey *I*ntegrity *P*rotocol**
- **Features**
  - New Message Integrity Code (MIC) called Michael to detect forgery attempts
    - Since existing APs are MIP constrained, Michael cannot always provide desired level of assurance
  - Supplement Michael with Counter-measures, to increase forgery deterrence
  - Enforce frame order with a Replay protection mechanism
  - Extend WEP sequence space, to limit complexity of key renegotiation
  - Rescue WEP's mis-use of RC4 encryption that allows reused of WEP hardware, because environment is so MIP constrained.
  - Make operation visible through appropriate counters
    - Under WEP it was infeasible to detect when you were under attack
- **Meets goal of field upgradeable WEP fix**

TKIP Design (1) – MPDU Format s



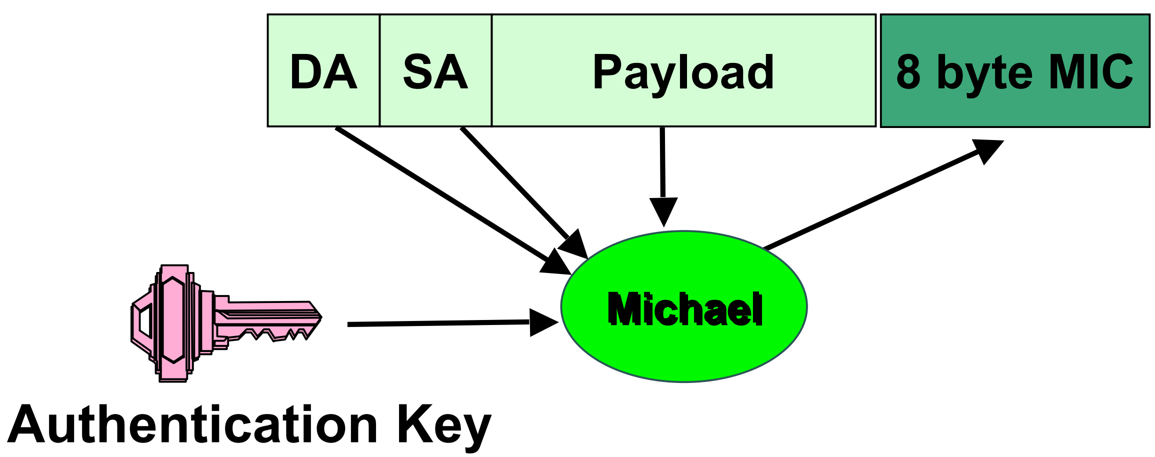
TKIP Design (2) – Keys

- **1 128 bit encryption key**
  - Constrain forced by some WEP off-load hardware
  - So somehow must prevent key reuse
- **2 64-bit data integrity keys**
  - AP and STA each use a different key for transmit

TKIP Design (3) -- Michael

Protect against forgeries

- Must be cheap: CPU budget ≤ 5 instructions/byte
- Unfortunately is weak: a 2^{29} message differential attack exists
- Computed over MSDUs, while WEP operates on MPDUs
- Uses two 64-bit keys, one in each link direction



TKIP Design (4) – Countermeasures

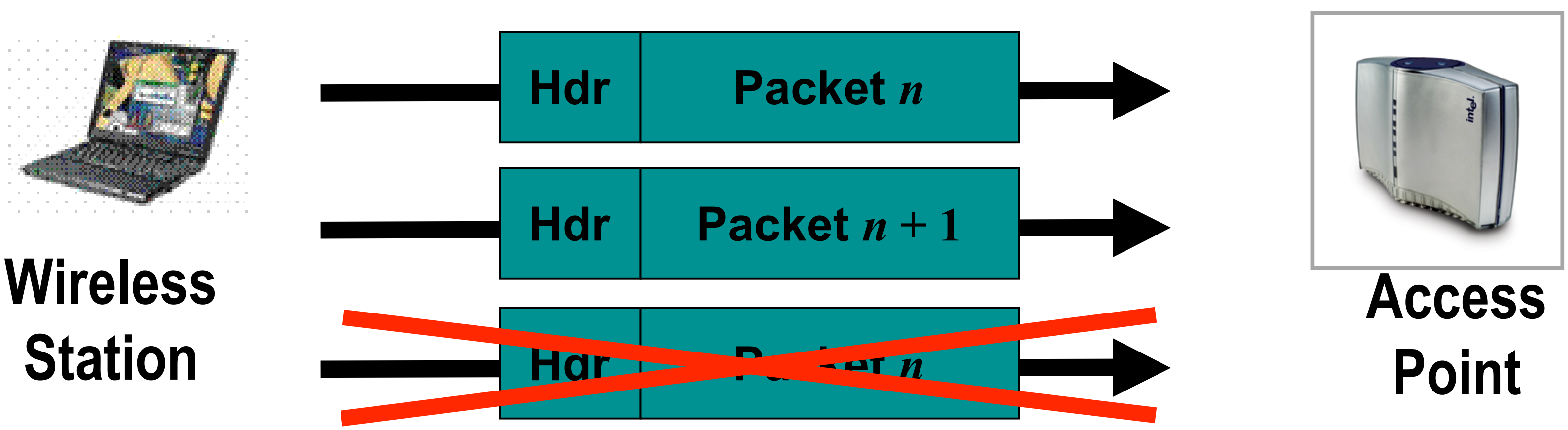
- **Check CRC, ICV, and IV before verifying MIC**
  - Minimizes chances of false positives
  - If MIC failure, almost certain active attack underway
- **If an active attack is detected:**
  - Stop using session keys
  - Rate limit key generation to 1 per minute
- **Why 1 Minute?**
  - Michael design goal is 20 bits of security
    - But best attack we know is 2^{29}
  - Need to rate limit how fast attacker can generate forgery attempts
  - Since infeasible to rate limit attacker, instead rate limit attacker's effective attempts, i.e., how many WLAN will respond to
  - 1 year $\approx 2^{19}$ seconds
  - If design meets its design goal, this means on average at most 1successful forgery per year
    - If the 2^{29} is best attack, then 1 successful forgery every 500 years

TKIP Design (5) – Replay Protection

Protect against replay

- reset packet sequence # to 0 on rekey
- increment sequence # by 1 on each packet
- drop any packet received out of sequence
- work with 802.11e QoS: QoS intentionally reorders packets

Within each QoS Traffic Class:



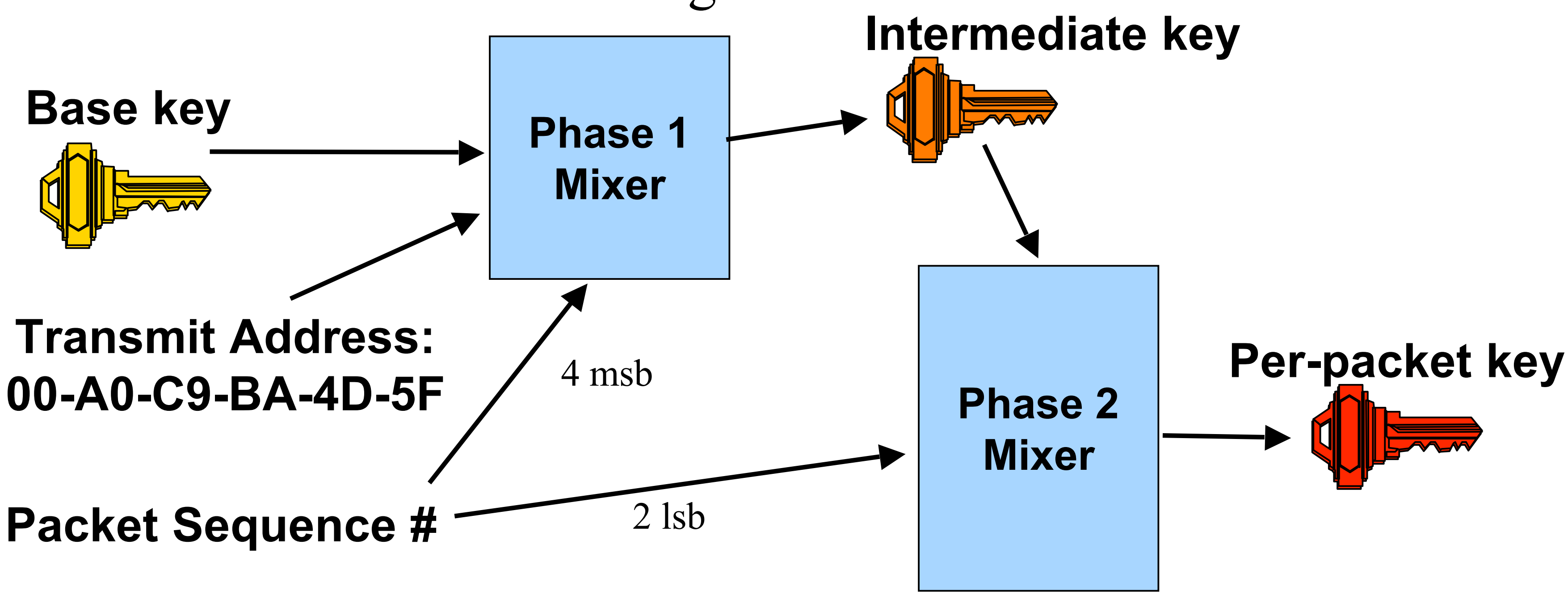
TKIP Replay Discussion

- **Sequence numbers for different MPDUs (fragments) of same MSDU must be sequential, or fragmentation attacks enabled**

TKIP Design (6) – Key Mixing

Stop WEP's encryption abuse

- Build a better per-packet encryption key…
- … by preventing weak-key attacks and decorrelating WEP IV and per-packet key
- must be efficient on existing hardware



TKIP Security Discussion

- **Michael transforms forgery attacks into less harmful denial of service attacks**
  - Differential cryptanalysis shows that an attacker can produce valid MIC in roughly 2^{29} tries by random guessing
  - Counter-measures added to rate limit effect of forgery attack
  - Encrypt the MIC, to limit knowledge attacker gains from either a successful or unsuccessful forgeries
- **Replay mechanism detects and discards replay**
- **Key mixing recovers WEP hardware by eliminating encryption abuse**
  - Auto-correlation analysis shows that keys produced by key mixing are correlated for sequence numbers *n* and *n*+65536
  - But we know of no other vulnerabilities and no way to exploit this
- **Mixing Transmit address defends against address hijacking and key reuse**

TKIP Summary

- **TKIP appears to provide weak but genuine security**
  – External review by Ron Rivest, David Wagner, John Kelsey, Susan Langford, and others
- **TKIP meets goal of software deployment on almost all existing equipment**
  – Does not appear to significantly degrade performance over WEP
  – Meets market's requirement for a migration path based on pre-existing installed base
- **TKIP is interoperable**
  – Interoperability demonstrated through the standard Wi-Fi test suite
- **Attacks become visible through TKIP counters and counter-measure invocation**
- **Bonus Feature (not part of original design goals): TKIP is forward compatible with**
  – 802.11e, 802.11k, 802.11r, 802.11s, 802.11t, 802.11v, and 802.11w

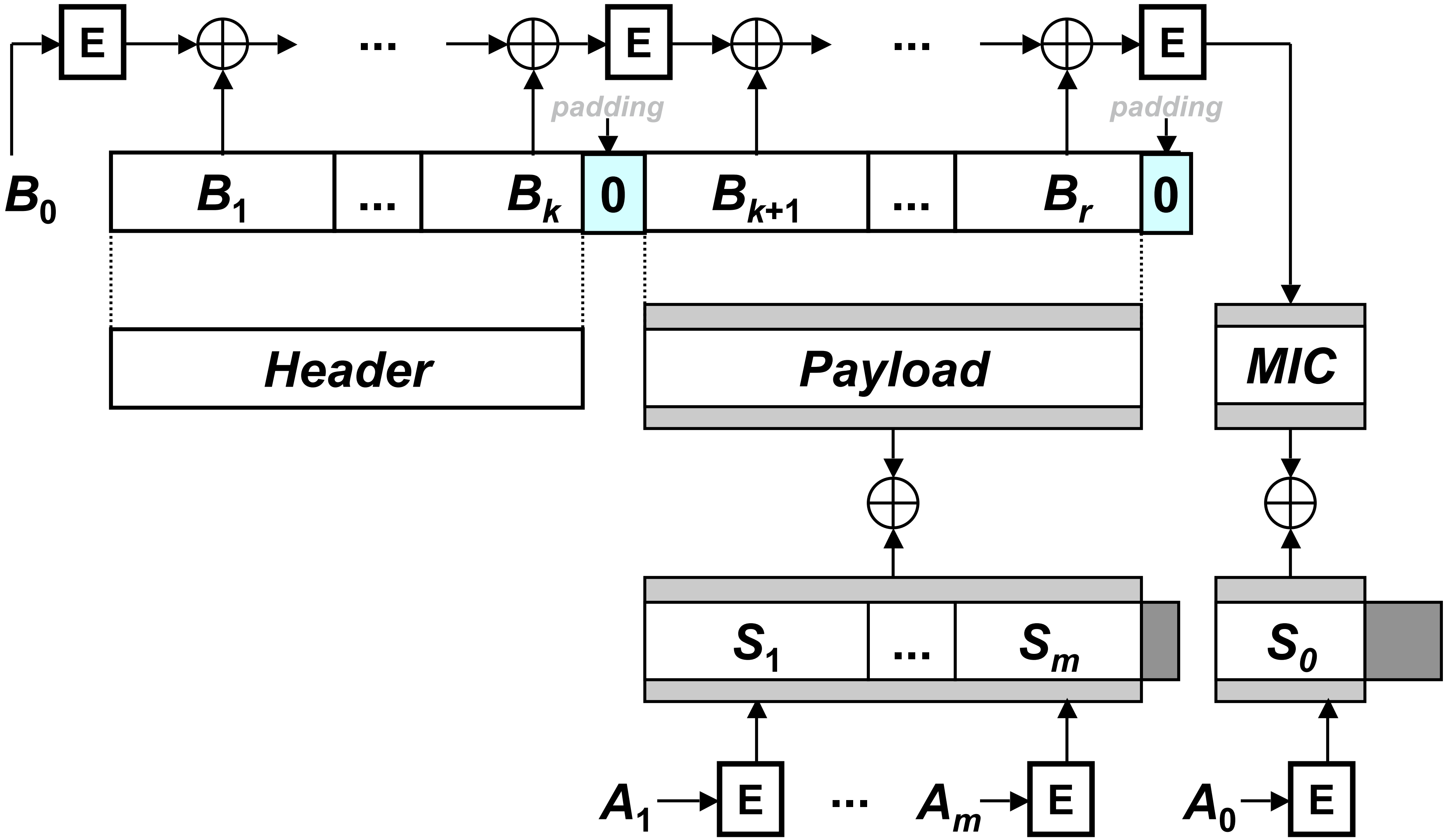
AES-CCMP Identification and Goals

- **AES-CCMP: 128 bit *AES* in *C*ounter Mode with *C*BC-*M*AC *P*rotocol**
- **All new design with few concessions to WEP**
  - Costs ≈ 40 instructions/byte in software, so requires new Access Point hardware
- **Long term solution**
  - Apply lessons learned from IPsec and 802.10 designs
  - Base on state-of-the art crypto
  - Extensible, to allow reconfiguration with any other 128 bit block cipher
  - Forward compatibility required with all 802.11 amendments, both planned and under development
- **Security Goals: Address all known WEP problems**
  - Prevent Frame Forgeries
  - Prevent Replay
  - Correct WEP's mis-use of encryption
  - Never reuse keys

Counter Mode with CBC-MAC

- **Authenticated Encryption combining Counter (CTR) mode and CBC-MAC, using a single key**
  - CCM mode assumes 128 bit block cipher
  - IEEE Std 802.11i uses AES
- **Designed for IEEE Std 802.11i**
  - By D. Whiting, N. Ferguson, and R. Housley
  - Intended only for packet environment
  - No attempt to accommodate streams

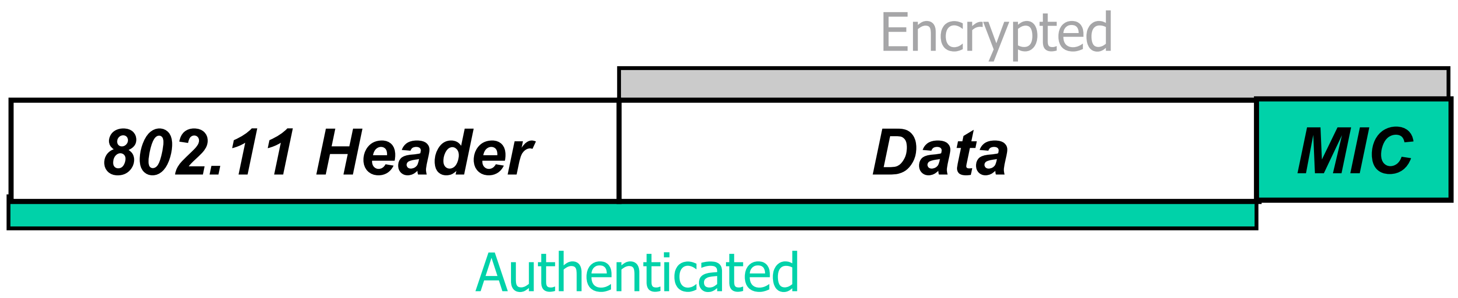
CCM Mode


E
…
E
…
E
padding
padding
B0
B1
…
Bk
0
Bk+1
…
Br
0
Header
Payload
MIC
S1
…
Sm
S0
A1
E
…
Am
E
A0
E

CCM Properties

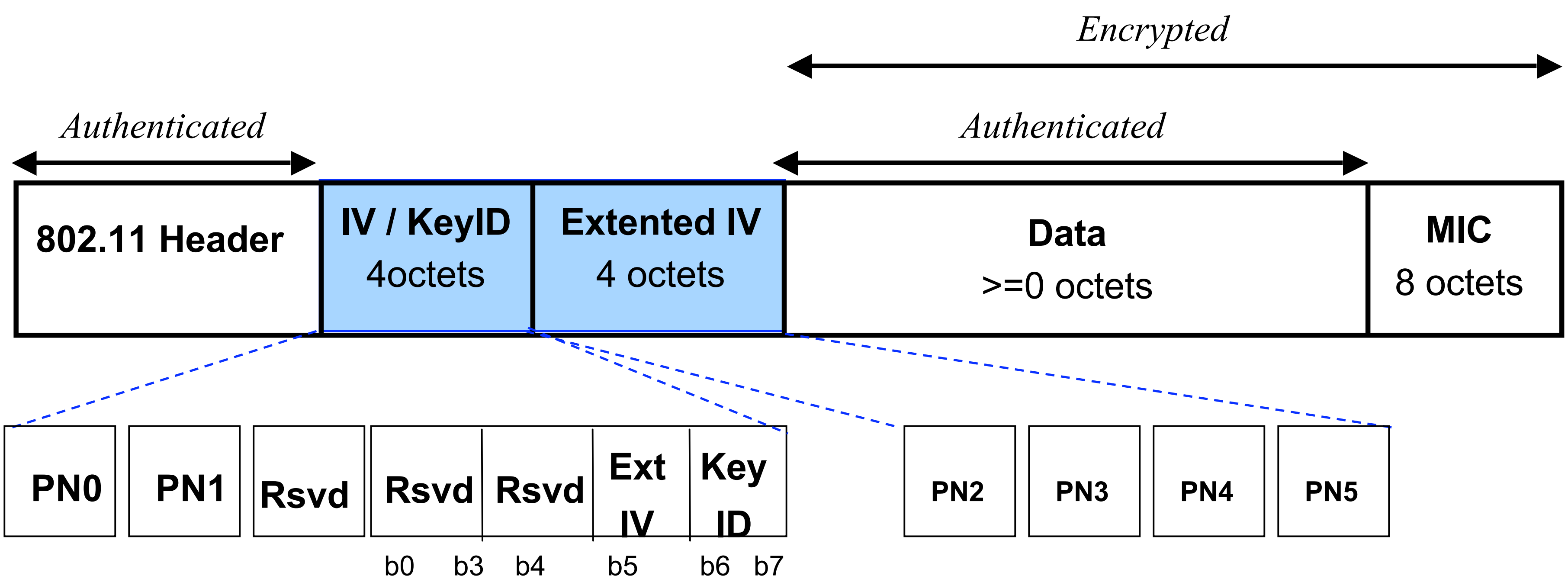
- **CTR + CBC-MAC (CCM) based on a block cipher**
- **CCM provides authenticity and privacy**
  - A CBC-MAC of the plaintext is appended to the plaintext to form an *encoded* plaintext
  - The encoded plaintext is encrypted in CTR mode
- **CCM is packet oriented**
- **CCM can leave any number of initial blocks of the plaintext unencrypted**
- **CCM has a security level as good as other proposed combined modes of operation, including OCB**
  - Danish cryptographer Jakob Jonsson proved CCM is secure if block cipher is secure – EUROCRYPT 2002

CCMP Overview



- **Use CBC-MAC to compute a MIC on the plaintext header, length of the plaintext header, and the payload**
- **Use CTR mode to encrypt the payload**
  - Counter values 1, 2, 3, …
- **Use CTR mode to encrypt the MIC**
  - Counter value 0

CCMP MPDU Format



CCM Usage by CCMP

- **Needs one fresh 128-bit key**
  - Same 128-bit Temporal key used by both AP and STA
  - CBC-MAC IV, CTR constructions make this valid
- **Nonce (A_0, B_0) construction in CCMP's use of CCM:**
  - A_0 = Tag_0 || 0x00 || Transmit-Address || Frame-Sequence-Number
  - B_0 = Tag_1 || 0x00 || Transmit-Address || Frame-Sequence-Number
  - Transmit-address is 6 octets
  - Frame-Sequence-Number is 8 octets and includes the QoS Priority
  - Sequence-Number must be sequential within a single MSDU
- **802.11 Header bits manipulated by normal protocol operation set to 0 prior to application of AES-CCM**
- **Sequence numbers must be sequential within MPDUs from same MSDU**

AES-CCMP Summary

- **AES-CCMP appears to meet all 802.11i security goals**
  - External review by Ron Rivest, David Wagner, Phil Rogaway, and others
- **AES-CCMP is interoperable**
  - Interoperability demonstrated through the standard Wi-Fi test suite
- **AES can be replaced with any other secure 128 bit Cipher**
- **No known intellectual property encumbrances**
- **Reports attacks through counters**
- **Forward compatible with all on-going work**
  - In particular, with 802.11e, 802.11k, 802.11n, 802.11r, 802.11s, 802.11t, 802.11v, and 802.11w

Data Protection Protocol Comparison

	<u>**WEP**</u>	<u>**TKIP**</u>	<u>**CCMP**</u>
Cipher	**RC4**	**RC4**	**AES**
Key Size	**40 or 104 bits**	**128 bits encryption, 64 bit auth**	**128 bits**
Key Life	**24-bit IV, wrap**	**48-bit IV**	**48-bit IV**
Packet Key	**Concat.**	**Mixing Fnc**	**Not Needed**
Integrity			
Data	**CRC-32**	**Michael**	**CCM**
Header	**None**	**Michael**	**CCM**
Replay	**None**	**Use IV**	**Use IV**
Key Mgmt	**None**	**802.11i 4-Way Handshake**	**802.11i 4-Way Handshake**

Some Open Data Protection Issues

- **802.11i protects broadcast/multicast by a shared key**
  - This restricts confidentiality to the group,
  - But forgeries possible by insider attacks
  - Limits use of broadcast/multicast to idempotent, i.e., safely repeatable, messages, such as ARP requests and service advertisements
  - Protection for other types of multicast traffic not yet a perceived market need, so no work initiated at this time
- **No protection for 802.11 management frames**
  - This is a perceived problem
  - Reassociation addressed by 802.11r
  - Disassociation, Deauthenticate, and Action Frames addressed by 802.11w
- **No protection for PHY level attacks**
  - Outside what can be addressed by MAC enhancements
  - Perceived need, but lack of proposed algorithms to charter work at this time

Discovery and Negotiation and Goals

- **Discovery – Find the security policy of available WLANs**
  - What Authenticated Key Management (AKM) Protocol, Unicast and Multicast Ciphersuites are available?
- **Negotiation – Enable parties to agree on the security policy to use with an association**
  - Agree on which of those options enabled to use
- **Goals:**
  - Interoperability with already-deployed and non-802.11i equipment
  - Create mechanism for extending 802.11i framework to permit AKMs, Ciphersuites not defined by 802.11i
  - Minimize new overhead in Beacons

RSN Information Element

Element ID	Length	Version	
Group Key Ciphersuite Selector			
Pairwise Ciphersuite Count		Pairwise Ciphersuite List	
Pairwise Ciphersuite List		AKM Count	
AKM List			
Capabilities		PMK ID Count	
PMK ID List			

Defined Ciphersuites, AKMs

Defined Ciphersuites

- 00-0F-AC:1 WEP-40
- 00-0F-AC:2 TKIP
- 00-0F-AC:4 AES-CCMP (default)
- 00-0F-AC:5 WEP-104
- Vendor OUI:Any Vendor specific
- Other Reserved

Defined AKMs

- 00-0F-AC:1 802.1X Authentication + 4-Way Handshake
- 00-0F-AC:2 PSK + 4-Way Handshake
- Vendor OUI:Any Vendor specific
- Other Reserved

Discovery

Station

Access Point

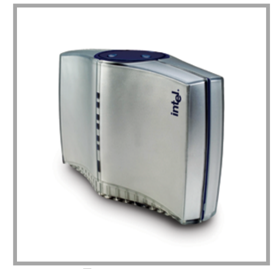
Probe Request

Beacon or Probe Response + RSN IE (AP supports CCMP Mcast, CCMP Ucast, 802.1X Auth)

Advertises WLAN security policy

Negotiation

Station



Access Point

STA Selects Unicast Cipher Suite, Authentication and Key Management Suite from Advertised

Association Req + RSN IE (STA requests CCMP Mcast, CCMP Ucast, 802.1X Auth) →

← Association Response (success)

Discovery and Negotiation Discussion

- **Backward compatible with WEP**
  - WEP-only STAs do not recognize RSN IE, nor do they include it is their Association messages
- **Extensible: RSN IE permits the addition of new ciphersuites and AKMs not contemplated by 802.11i**
- **RSN IE can be compressed to 4 octets by using the defaults, minimizing cost in Beacons**
- **Group Ciphersuite must be lowest common denominator ciphersuite**
- **802.11i key management (below) protects against downgrade attacks**

Why not Deprecate WEP?

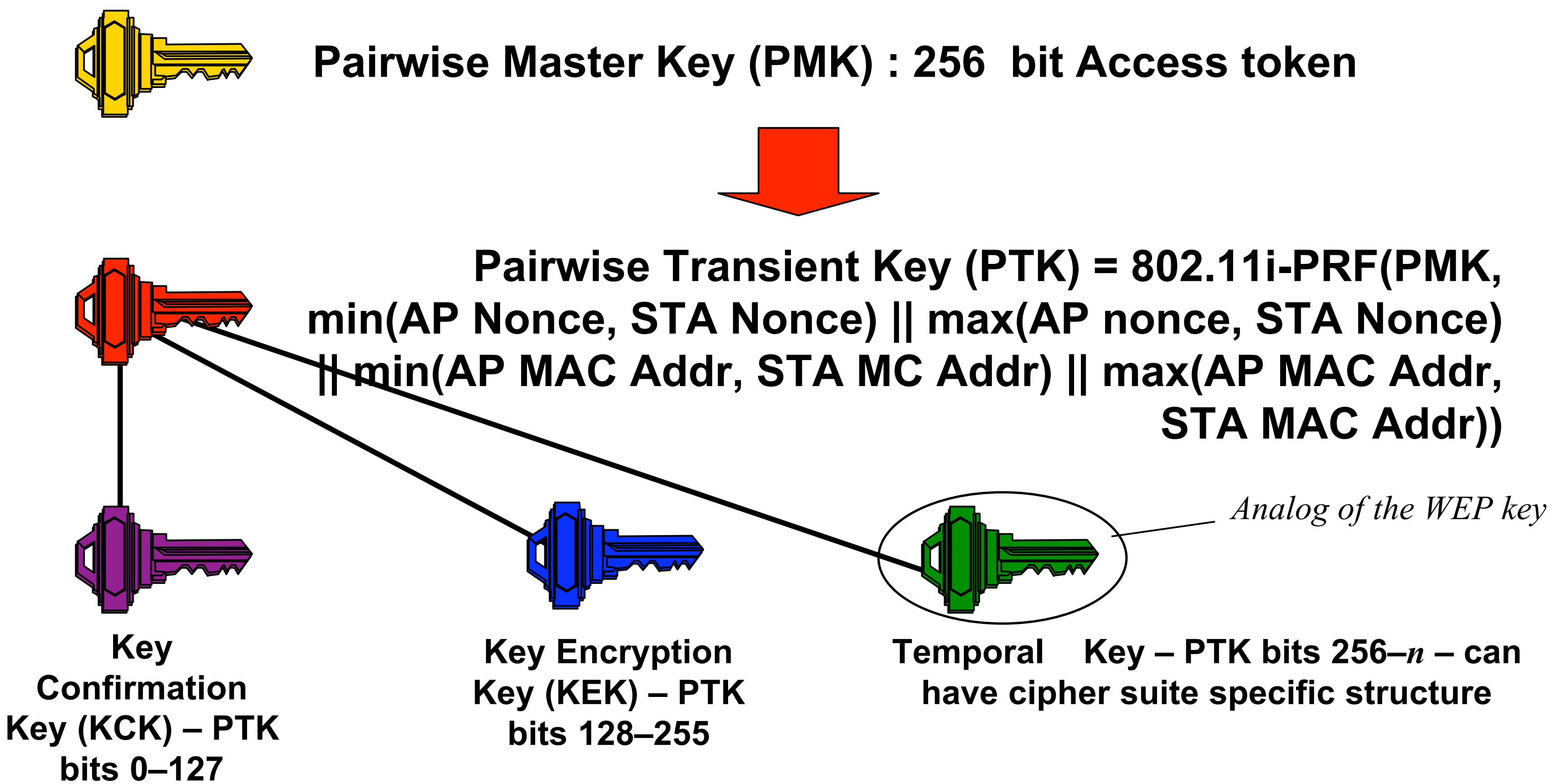
- **Economically infeasible**
  - tens of millions of already deployed systems
  - In general, too costly to deploy a parallel system
    - Sometimes feasible during “normal” refresh cycle
- **Operationally infeasible**
  - Experience with IPv4, Netware, DECnet, etc., shows it takes weeks or months or even years to upgrade software on every system
  - WLAN would be unavailable for some systems during upgrade
  - Prior experience says someone, somewhere will have deployed a mission critical application that cannot be interrupted for an upgrade

Key Management Goals

Given a "good" PMK

- Guarantee fresh session key
- Demonstrate liveness of peer PMK holder
- Bind session key to the communicating AP and STA
- Synchronize session key use
- Distribute the Group Key
- Protect Discovery and Negotiation from Downgrade attack
- Establish a (statistically) unique session identifier

802.11i Pairwise Key Hierarchy



Key Derivation

802.11i-PRF(*K*, *A*, *B*, *Len*)

$R \leftarrow$ “”

for $i \leftarrow 0$ **to** $((Len+159)/160) - 1$ **do**

$R \leftarrow R \,||\, \text{HMAC-SHA1}(K, A \,||\, B \,||\, i)$

return Truncate-to-len(R, Len)

Example for AES-CCMP:

PTK ← 802.11i-PRF(PMK, “Pairwise key expansion”, min(AP-Addr, STA-Addr) || max(AP-Addr, STA-Addr) || min(ANonce, SNonce) || max(ANonce, SNonce), 384)

Key Derivation Discussion

- **Using min, max in key derivation destroys prefix-free property but improves interoperability**
  - Same key prefix could in principal be derived in different contexts
  - No known way to exploit this weakness in the existing design
- **Construction vulnerable to sliding parameter attacks**
  - e.g., A = “0x00 0x00”, B = “0x01 0x02” on one invocation, A = “0x00”, B = “0x00 0x01 0x2” on the next
  - But no opportunities known to launch this kind of attack in existing design
- **Derived PTK has at most 160 bits of entropy**
  - HMAC-SHA1 begins by replacing PMK with SHA1(PMK)
  - But 160 bits of entropy considered sufficient for commercial grade security
  - This will be a concern after 2010, but not before
- **Why HMAC-SHA1?**
  - Good enough for IKE
  - SHA1 already supported by most 802.1X implementations
  - HMAC-SHA1 appears safe as a key derivation method

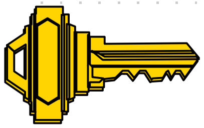
EAPOL Key Message

<table>
<tr><td colspan="2">Descriptor Type – 1 octet</td></tr>
<tr><td>Key Information – 2 octets</td><td>Key Length – 2 octets</td></tr>
<tr><td colspan="2">Replay Counter – 8 octets</td></tr>
<tr><td colspan="2">Nonce – 32 octets</td></tr>
<tr><td colspan="2">IV – 16 octets</td></tr>
<tr><td colspan="2">RSC – 8 octets</td></tr>
<tr><td colspan="2">Key ID – 8 octets</td></tr>
<tr><td colspan="2">MIC – 16 octets</td></tr>
<tr><td>Data Length – 2 octets</td><td>Data – n octets</td></tr>
</table>

4-Way Handshake

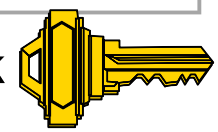
STA

AP



PMK

PMK



Pick Random ANonce

EAPOL-Key(Reply Required, Unicast, ANonce)

Pick Random SNonce, Derive PTK = 802.11i-PRF(PMK, ANonce || SNonce || AP MAC Addr || STA MAC Addr)

EAPOL-Key(Unicast, SNonce, MIC, STA RSN IE)

Derive PTK

EAPOL-Key(Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE, GTK)

EAPOL-Key(Unicast, MIC)

4-Way Handshake Discussion (1)

- **ANonce, SNonce 256 bit random values**
  - Design assumes ANonce, SNonce produced by cryptographic random number generator
  - Annex H.5 suggests techniques for random number generation
- **802.11i requires AP to commit to ANonce value for each 4-Way Handshake instance, since otherwise STA subject to Message 1 flooding attacks**
  - A Message 3 with correct ANonce value will eventually arrive
- **Protocol overloads ANonce, SNonce for both key separation and liveness**

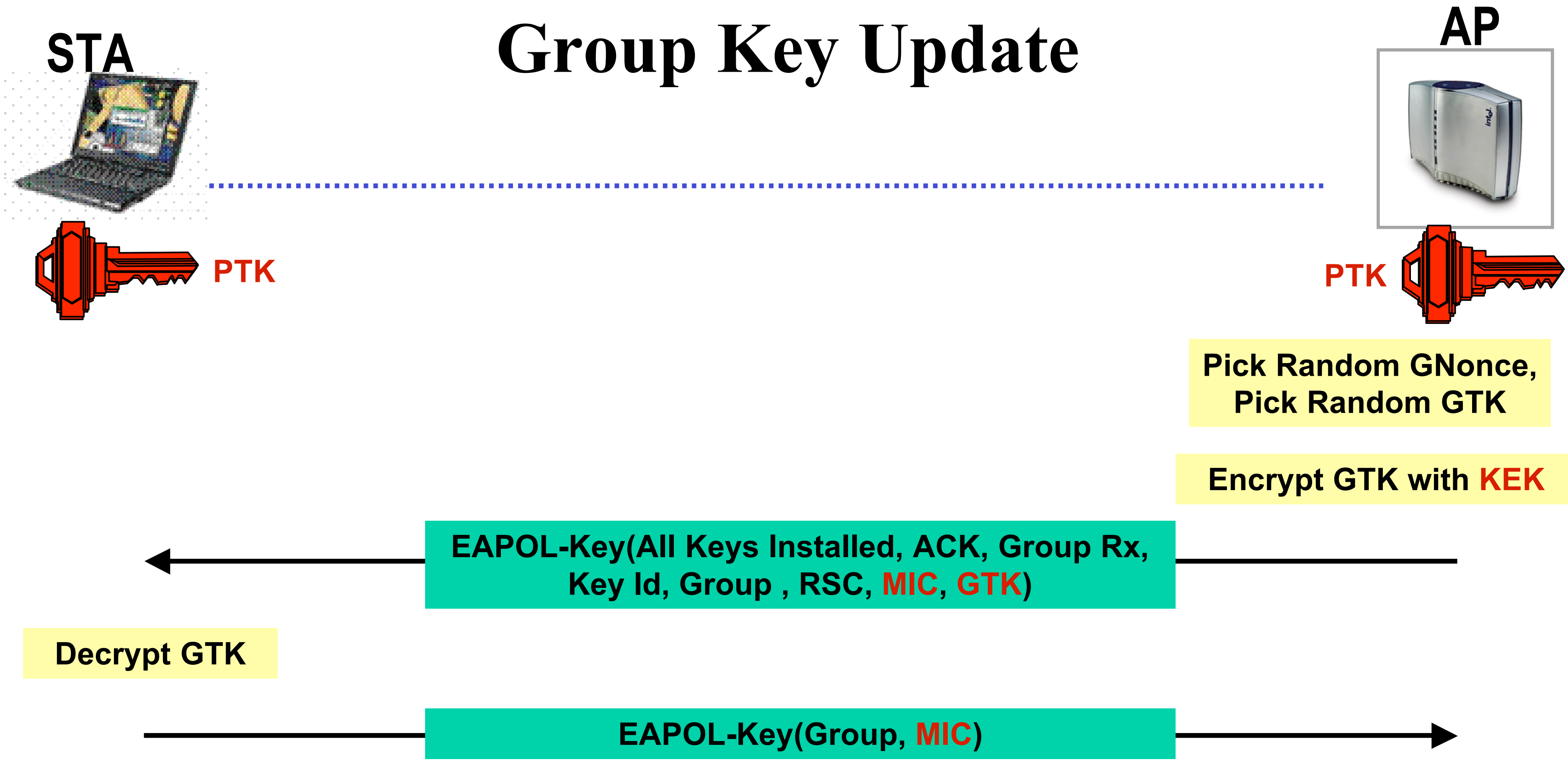
4-Way Handshake Discussion (2)

- **Race condition if Message 3 or 4 is lost**
  - Message 3 sent in plaintext, but Message 4 after TK is installed
  - Retransmitted Message 3's are lost because not encrypted under TK
  - Experience shows this is not a problem in normal operations
- **Message 4 has no cryptographic value**
  - But it is useful to suppress retries of Message 3
- **GTK wrapped using the NIST Key Wrap algorithm**
  - Security properties of this are not understood
  - But we don't know anything better

Achieving Key Management Goals

- **PTK construction guarantee fresh session key**
  - Since ANonce and SNonce are random 256 bit stings, there is a statistically insignificant chance that the PTK will ever repeat
- **Message 2 demonstrates STA is live to AP; Message 3 demonstrates AP is live to the STA**
- **PTK construction binds PTK to STA and AP**
- **Messages 3 and 4 synchronize TK use**
- **Message 3 distributes group key to the STA**
- **Message 2 protects STA's RSN IE negotiating from Downgrade attack**
- **Message 3 protects AP's RSN IE advertising policy from Downgrade attack**
- **PTK can be named uniquely by <PMKID, AP-Addr, STA-Addr, ANonce, SNonce>**

Group Key Update



Group Key Update Discussion

- **Design supports removing a member from the group**
  - If PMK is distinct for each STA, use of the KEK and KCK allow "revocation" of old group key by distributing new GTK to the new set of authorized parties

Coordination with Authentication

- **On Association, RNSA State Machines signal authentication function (802.1X by default)**
- **802.11i design assumes authentication function blocks data traffic**
- **802.11i design assumes that authentication makes PMK available when it completes successfully and has authorized peer to access the link**
  - Note both STA and AP make an authorization decision
- **802.11i executes 4-Way Handshake when PMK becomes available**
- **802.11i signals authentication function when 4-Way Handshake completes**
- **802.11i design assumes authentication function unblocks data traffic when 4-Way Handshake completes**

Part III:
Some Complementary Standards

Topics Discussed

- Authentication Requirements
- IEEE Std 802.1X
- IETF EAP
- IETF EAP-TLS
- IETF PEAP
- IETF RADIUS and Diameter
- IEEE Std 802.11i PSK

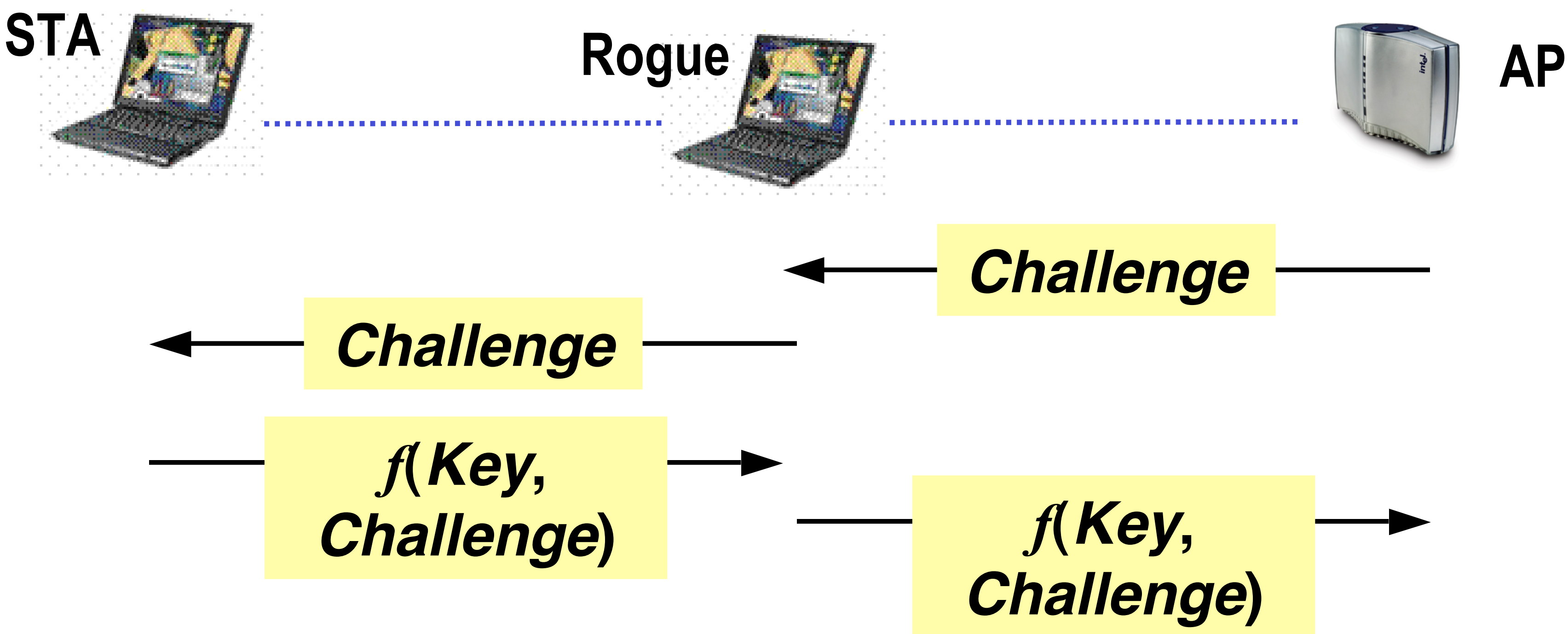
Authentication Requirements: Economic Context for Design

- **Authentication, not data link protection, was the original security problem posed to the 802.11 WG**
- **Enterprises worldwide have invested billions of dollars, euros, yen, … in RADIUS authentication databases for remote access and network log-in**
- **Market provided explicit guidance that solutions not permitting enterprises to capitalize on this investment are Dead On Arrival**
  - Even before WEP revelations, enterprises shunned 802.11 because its authentication didn't allow reuse of existing RADIUS databases
- **Central Question: *How to maximize the security achievable by utilizing RADIUS authentication databases with 802.11i?***

Authentication Requirements

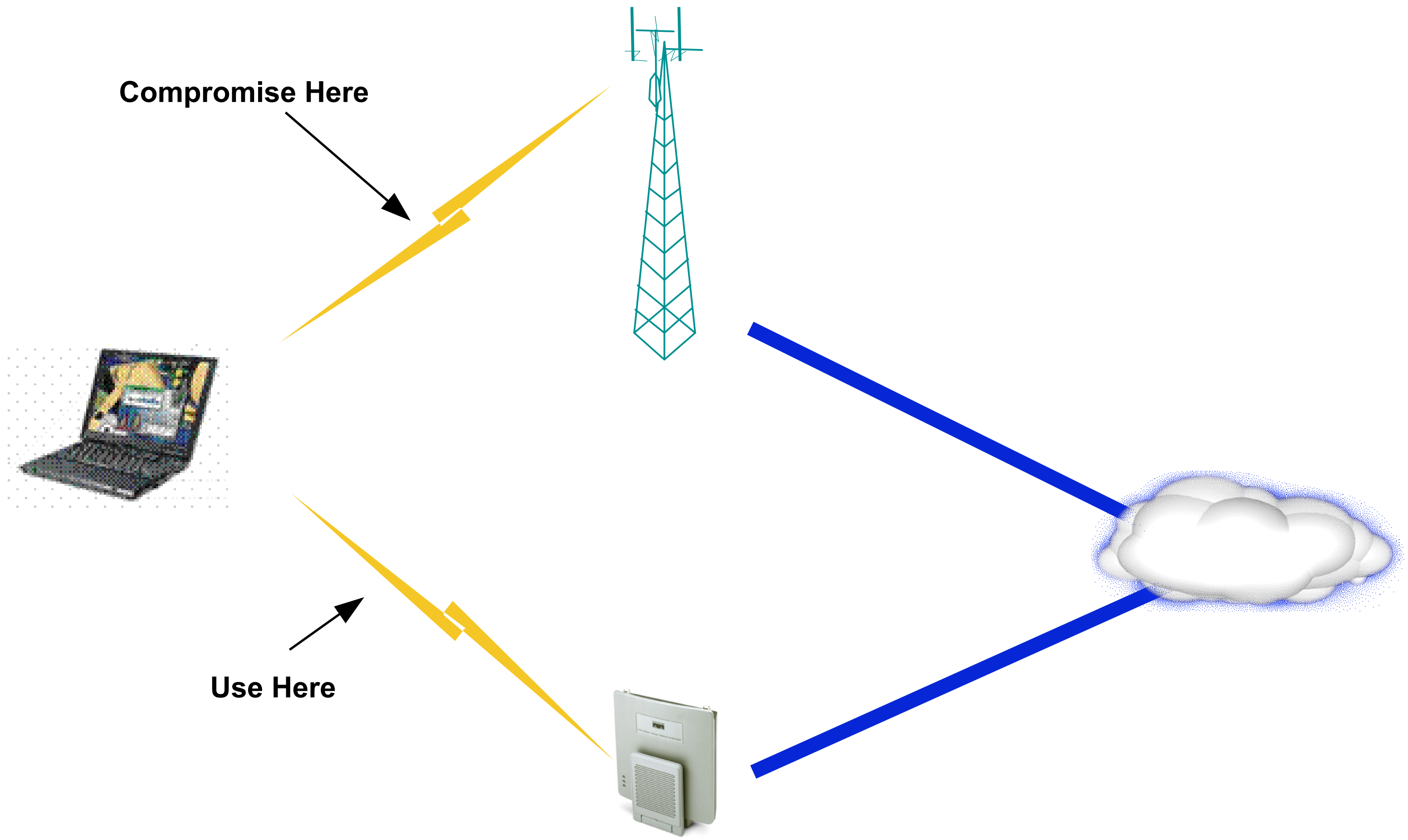
- Mutual Authentication
- Session Identifiers
- Session Key generation
- Immunity from off-line dictionary
- Immunity from man-in-the-middle attacks
- Protected ciphersuite negotiation

Unilateral, Bilateral Authentication Issues

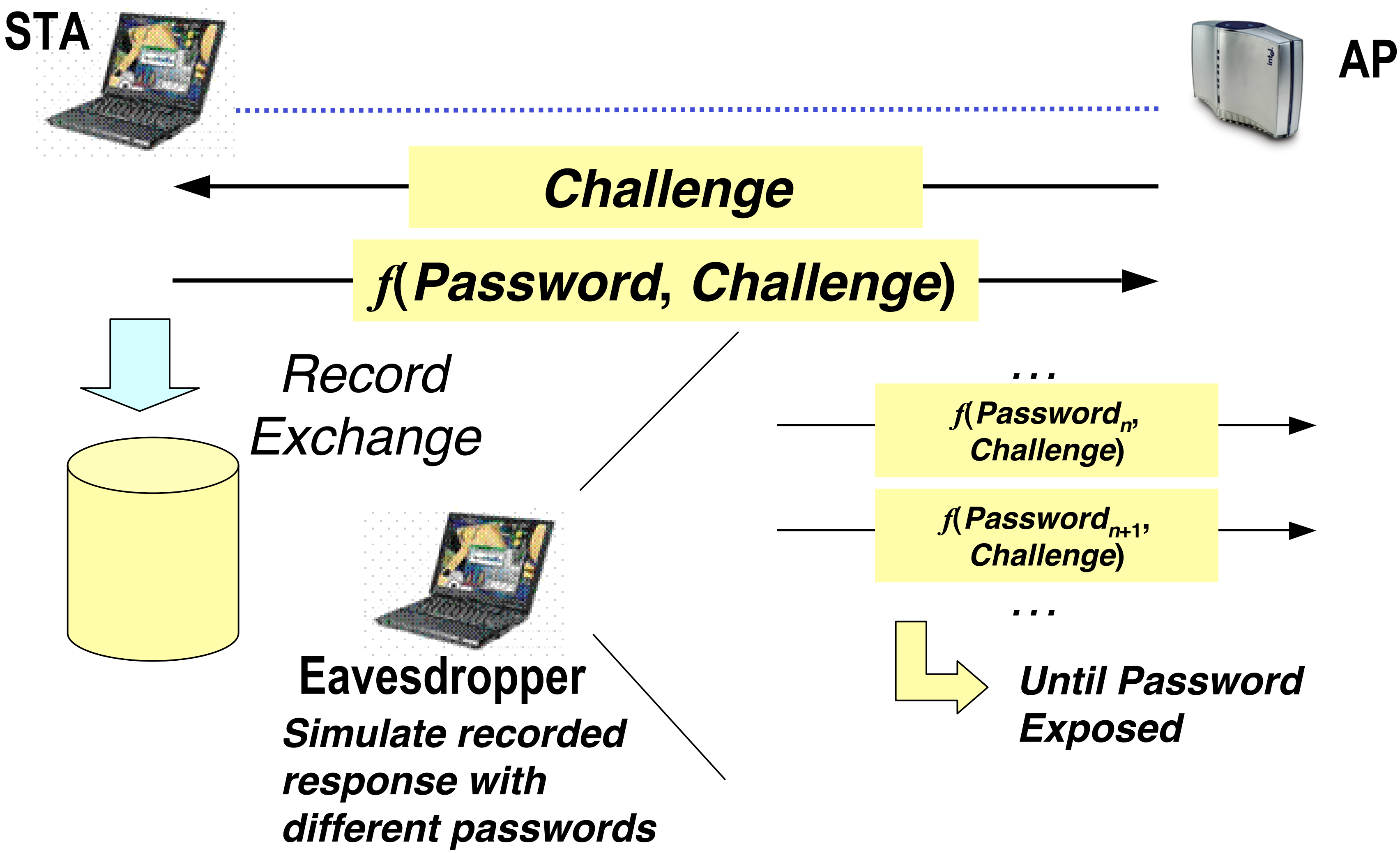


Rogue has authenticated as STA!

Credentials Reuse and MITM Attacks



Dictionary Attack in WEP



Concerns given the Central Question

- **How to force mutual authentication?**
  - Most methods that utilize RADIUS databases do not support mutual authentication
- **How to force session identifiers?**
  - Most methods that utilize RADIUS databases do not generate session identifiers
- **How to force session key generation?**
  - Most methods that utilize RADIUS databases do not generate session keys
- **What to do about credentials reuse?**
- **Can design prepare the market for something "better", e.g., PKI?**
- **Authentication methods not properly a LAN function, so outside the scope of 802 without a special waiver**

Direction Taken

- **Reuse IEEE Std 802.1X as the 802.11 authentication framework**
- **Make Enterprise requirements the design center**
  - Consumers were deploying 802.11 without security
  - Operators did not have mature business model to provide requirements
  - 802.1X uses EAP, which reuses RADIUS databases
  - Enterprises would not deploy solutions that do not reuse RADIUS databases
- **Identify incompatibilities of 802.1X model with wireless, and then drive changes to 802.1X and EAP in IEEE 802.1 WG and IETF, respectively**
- **Use EAP-TLS when practicable, and use PEAP to protect legacy RADIUS methods when not**
- **Deployment restrictions exist to extract maximum security from this model**
  - But these are consistent with enterprise usage

Is 802.1X, EAP, etc., Part of 802.11i?

- **IEEE Std 802.1X is *NOT* part of IEEE Std 802.11i**
- **IEEE Std 802.11i provides extensibility to indicate use of additional authentication and key management mechanisms**
  - See slide 39
  - Vendor proprietary mechanisms have been implemented
- **802.11i specifies assumptions made of 802.1X and how 802.11 uses 802.1X**
  - 802.11i assumes 802.1X provides a good session key
  - 802.11i assumes it is feasible to synchronize authentication and link protection
- **Separate stand-alone standard, so that the two can evolve independently**
  - Market wants to apply 802.1X to more than WLAN
  - This approach is usually considered good engineering practice

802.1X Description

- 802.1X Concepts
- 802.1X Communication Architecture
- 802.1X Ports
- 802.1X Scaling

802.1X Concepts

- **Port Access Entity – a primitive firewall controlling message flow through a LAN port**
  - Assumes either a Supplicant or Authenticator role
- **Supplicant – in the STA for 802.11i**
- **Authenticator – in the AP for 802.11i**
- **Authentication Server – A logical entity centralizing authentication and access control decision for the infrastructure**
  - May be embedded in AP
  - May be stand-alone server
  - May be in an access controller
- **Controlled Port – for blocking/passing "normal" data traffic**
- **Uncontrolled Port – for 802.1X traffic only**

802.1X Communication Architecture

Supplicant

Authenticator

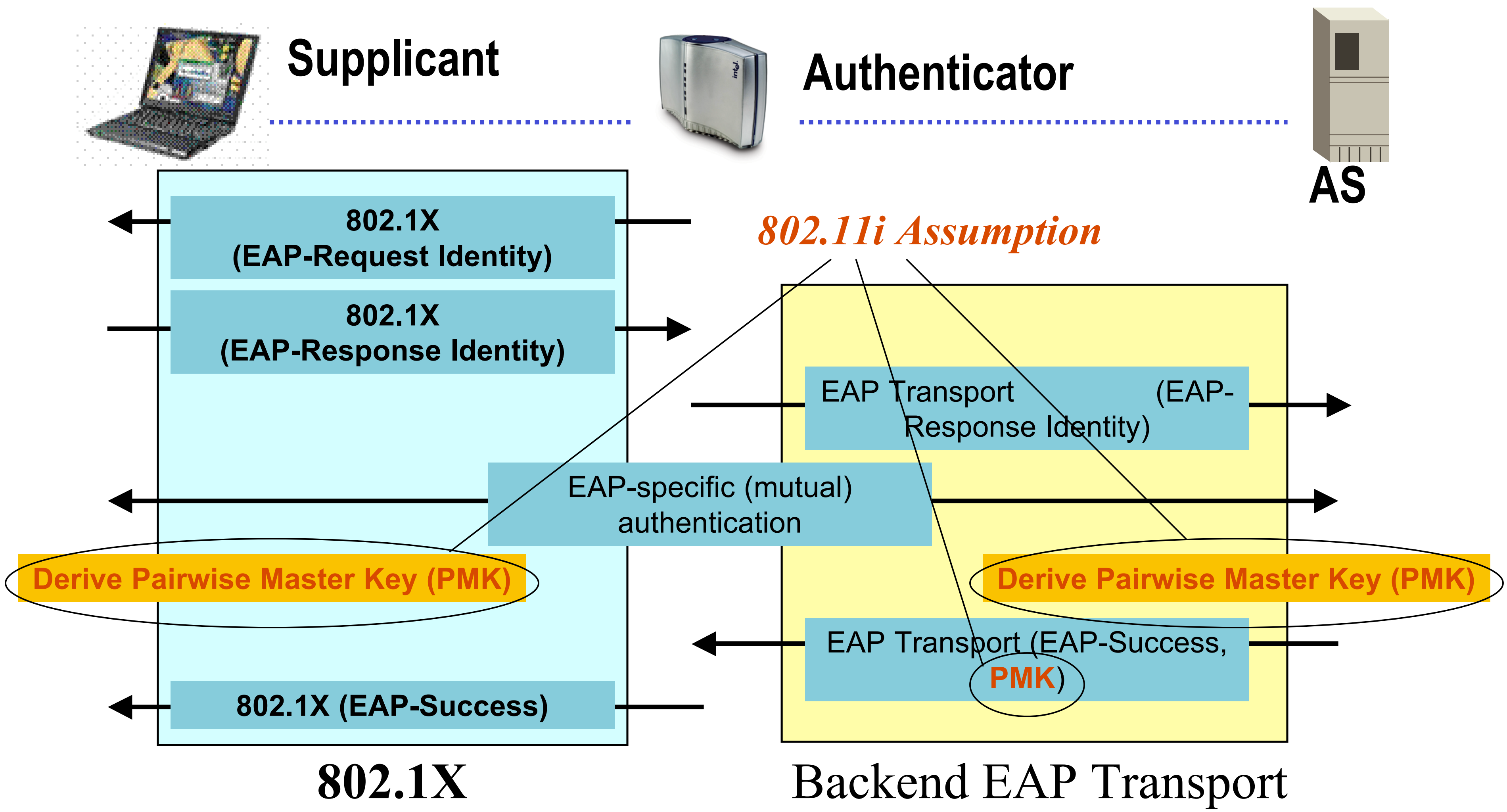
Authentication Server

EAP Method (e.g., EAP-TLS)	
EAP	
802.1X (EAPOL)	Backend EAP Transport

EAPOL = ***EAP*** Transport ***O***ver ***L***AN

802.1X messages sent as data messages in its own Ethertype

802.1X Message Flow



802.1X Message Flow Discussion

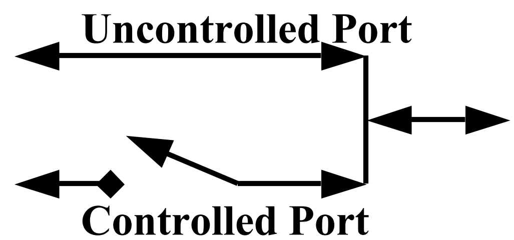
- **Authenticator is only a proxy in 802.1X architecture**
- **Since 802.1X communicates via data messages, authentication based on it can occur only after 802.11 association**
  - Increases service disruption time for AP-to-AP transitions
- **The session identifier function delegated to EAP method**
- **All 802.1X messages subject to attack when LAN type = 802.11**
  - In 802.11, Supplicant and Authenticator rely on 4-Way Handshake completion rather than Success message

802.1X Ports

Before Authentication:

802.1X Traffic

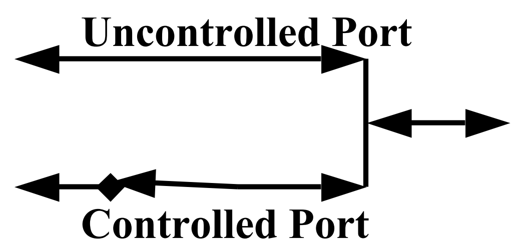
Non-802.1X Traffic (Blocked)



After Authentication:

802.1X Traffic

Non-802.1X Traffic (Unblocked)



802.1X Port Discussion

- **802.1X defines controlled and uncontrolled port only for Authenticator**
  - Model assumes the Supplicant system will not be attacked, an invalid assumption for 802.11i
- **802.11i implementations must provide controlled and uncontrolled ports for Supplicant as well**
  - Do not deliver any traffic received before keys are in place
- **Under 802.11i**
  - Controlled port is closed on association or disassociation
  - Opened when SME signals 4-Way Handshake succeeds

Scaling

- Deployment experience with 802.11i shows that 802.1X scales gracefully and with no performance degradation to WLANs consisting of 10s of thousands of Access Points
- This is sufficient for the largest enterprise campuses

802.1X Summary

- **802.11i meets its central constraint, reuse of RADIUS authentication database, by relying on 802.1X framework**
  - This delegates definition of authentication methods to IETF
- **802.1X not an ideal framework**
  - All messages can be forged
  - No cryptographically useful session identifiers
  - 802.1X model based on Unilateral instead of Mutual Authentication
  - 802.1X based on always connected model
- **802.11i design and deployment guidance mitigates the problems 802.1X causes**
- **802.1X authentication meets the performance expectations of the largest enterprises**

EAP Description

- **EAP Concepts**
- **EAP Design Goals**
- **EAP Operation**
- **EAP Keying**

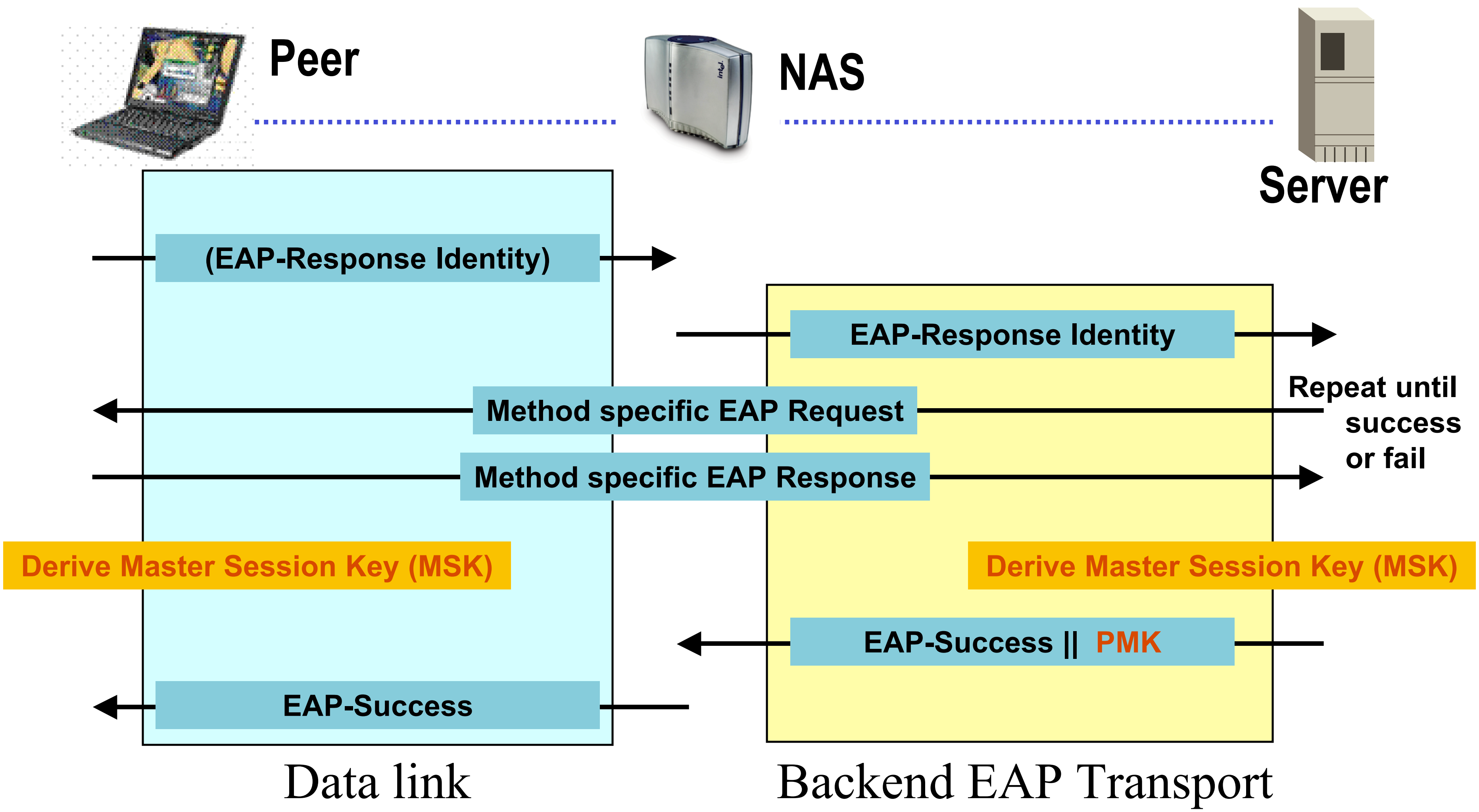
EAP Concepts

- **EAP – Extensible Authentication Protocol, RFC 3748**
- **EAP Server – coincides with 802.1X notion of an Authentication Server**
- **NAS – for Network Access Server, coinciding with 802.1X notion of Authenticator**
- **EAP Peer – coincides with 802.1X notion of Supplicant**
- **Master Session Key (MSK) – key constructed by EAP method between Server and Peer**
- **AAA Key – Key derived by Server and Peer and exported by the Server to the NAS**
  - The 802.11i PMK = 1st 32 octets of the AAA Key
- **EAP Request/Response – EAP Protocol messages**

EAP Design Goals

- **Carry existing authentication methods directly over a data link**
  - EAP a transport for authentication methods, not an authentication method itself
  - EAP is a “plug-in” framework for authentication methods
- **Allow easy deployment of new authentication methods**
  - Change only the Server and Peer, not the NAS
- **EAP independent of the transport used between the NAS and the Server**
  - Support multiple back-ends, including RADIUS, Diameter, LDAP, COPS, and others

EAP Operation



EAP Operation

- **EAP Authentication initiated by an EAP-Response/Identity message**
  - Gives a hint to the Peer's identity
- **Except for first and last messages, All EAP exchanges occur as Request/Response transactions initiated by the Server**
  - EAP a "stop-and-wait" protocol
  - EAP Server does not "advance" to "next" Request message until Peer responds to previous
  - This affords Server with some protection against denial-of-service attacks
- **Server tells Peer which authentication method to use in its first Request message**
  - Peer breaks off communication if this is unacceptable (e.g., unsupported, or disallowed by policy)
- **Method operates over sequence of Request/Response pairs until success or failure**
- **Server sends EAP-Success Message if method succeeds**
- **Server and Peer generate an MSK if method succeeds**

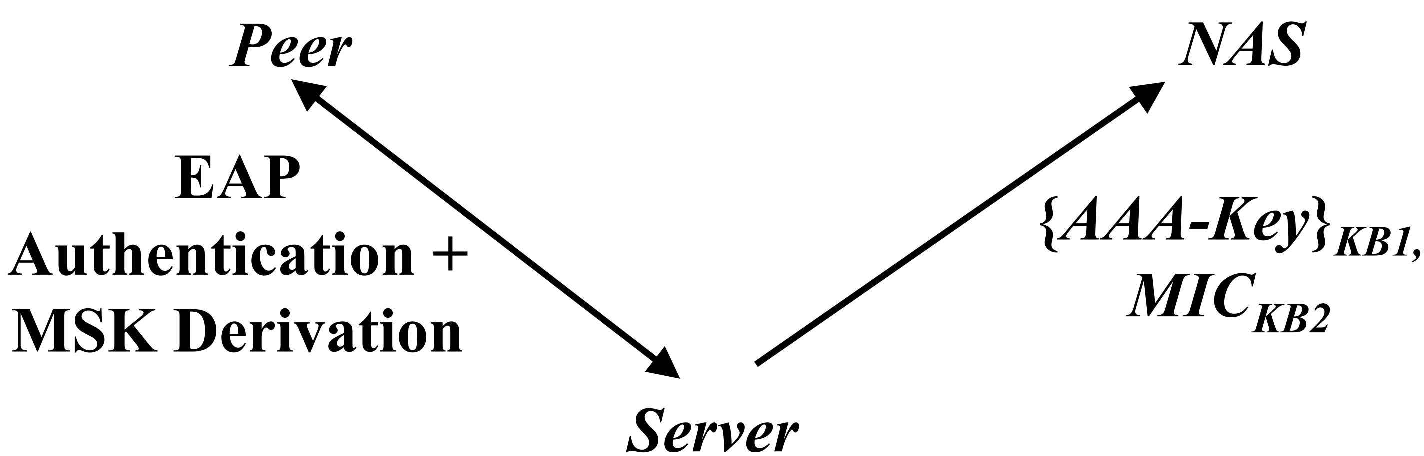
EAP Operation Discussion

- **EAP well-matched to 802.11i's central goal**
  - EAP evolved from work to extend RADIUS to support new authentication methods
- **EAP well-matched to 802.11's economics**
  - Off-load "expensive" authentication from ubiquitous commodity devices (access points) to capable server machines
  - Centralizes authentication and authorization decision, reducing enterprise management costs
- **EAP operation is unprotected**
  - No defense for the EAP-Success message in particular
  - EAP relies on authentication methods to defend themselves from attack
  - EAP depends on authentication method to provide a strong notion of a session
- **AAA Key is unbound to Peer, NAS**

EAP Keying, Abstractly

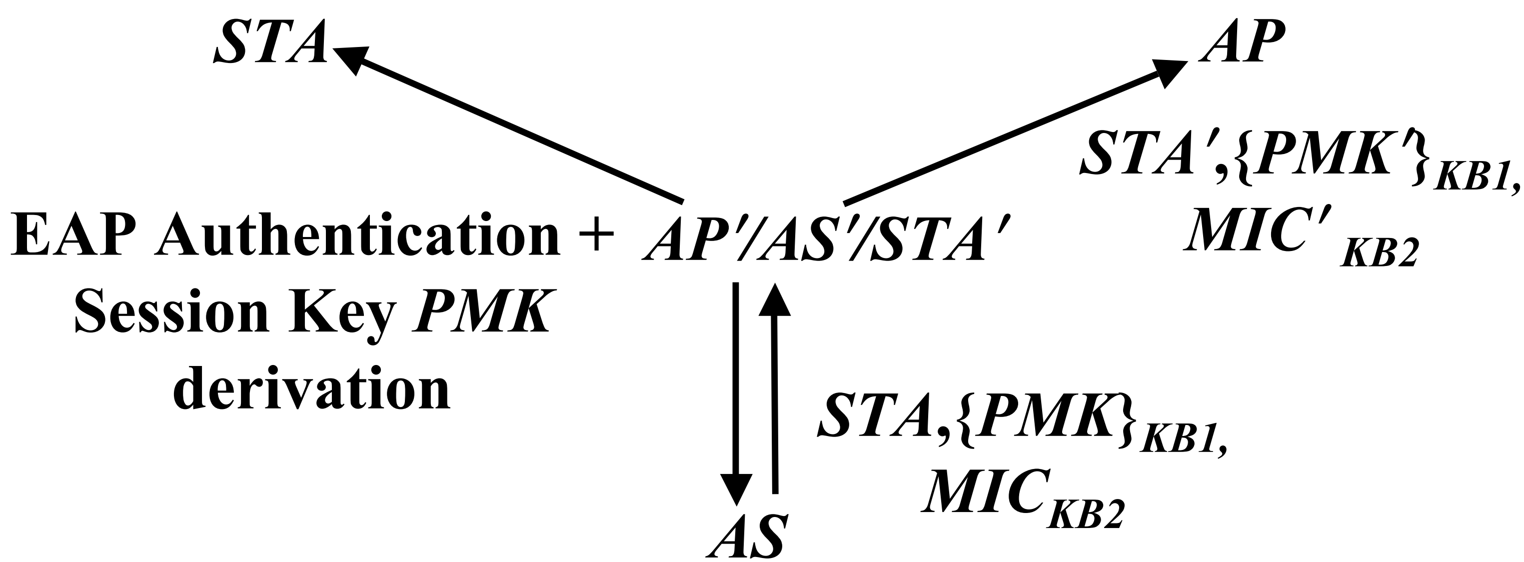
Goal: **Establish session key *AAA-Key* between *Peer* and *NAS***

Technique: **Use on-line trusted 3rd party *Server* as an intermediary**

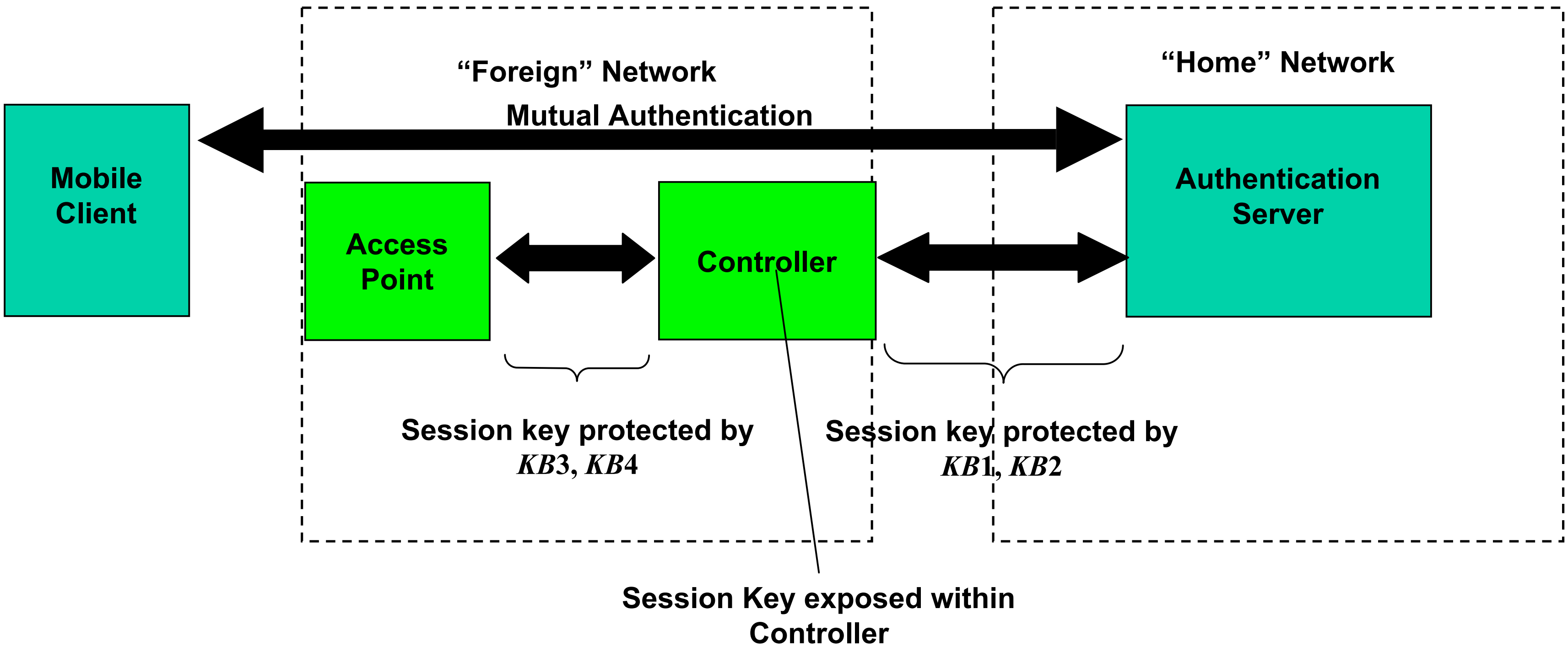


When Does This Work?

- No mutual authentication ⇒ MITM attack between STA, AS feasible
- No end-to-end data authentication key ⇒ MITM attack between AP, AS feasible
- No end-to-end key encryption key ⇒ PMK theft feasible
- PMK timeliness depends on correct AS implementation



The Operator's Dilemma



Many proposed operator architectures explicitly violate 802.11i assumptions

- Enables Rogue Access Point to capture Mobile Client

802.11i Deployment Requirements

- EAP method must provide mutual authentication
- Backend must protect AAA-Key end-to-end between AS and AP
  - AS must be known to the AP
  - AP must be known to the AS
  - AS and AP must share end-to-end keys
- These requirements can be met in enterprise deployments
- These requirements are problematic for symmetric key based authentication in the operator space

Is This a Problem?

- **Enterprise is the 802.11i design center**
- **Enterprise will not deploy 802.11 at all unless it can reuse its existing RADIUS authentication database**
- **Enterprise can obtain reasonable assurance when reusing its RADIUS authentication database via EAP deployed according to 802.11i guidelines**

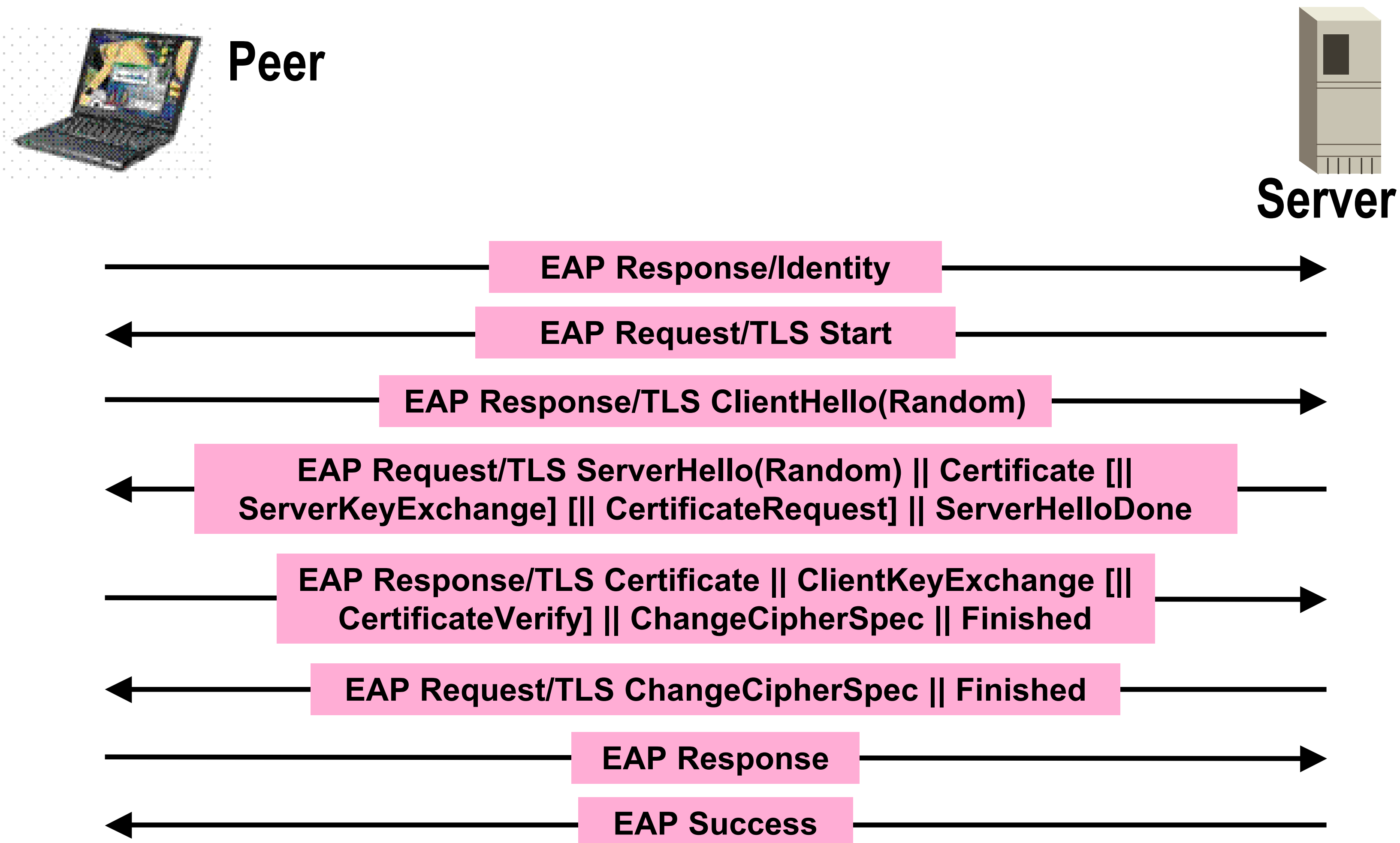
EAP Summary

- **EAP is not an ideal solution from a security perspective**
  - EAP message unprotected
  - EAP relies on authentication method to provide a notion of a session
  - Most important, EAP fails to define adequate key binding
- **Deployment guidelines limit the mischief possible due to lack of key binding**
  - These guidelines are reasonable for the enterprise, which is the 802.11i design center
- **EAP allows 802.11i to meet its central design goal, viz., reusing enterprise RADIUS databases for 802.11i authentication, to enable enterprise deployment**
  - Enterprises said explicitly they will not deploy 802.11 if they are forced to discard this investment in favor of a new authentication scheme
- **EAP appears to give the best tradeoff possible between security correctness and imperatives from the market**

EAP-TLS Description

- **EAP-TLS = RFC 2716**
- **EAP-TLS Overview**
- **EAP-TLS Discussion**

EAP-TLS Overview



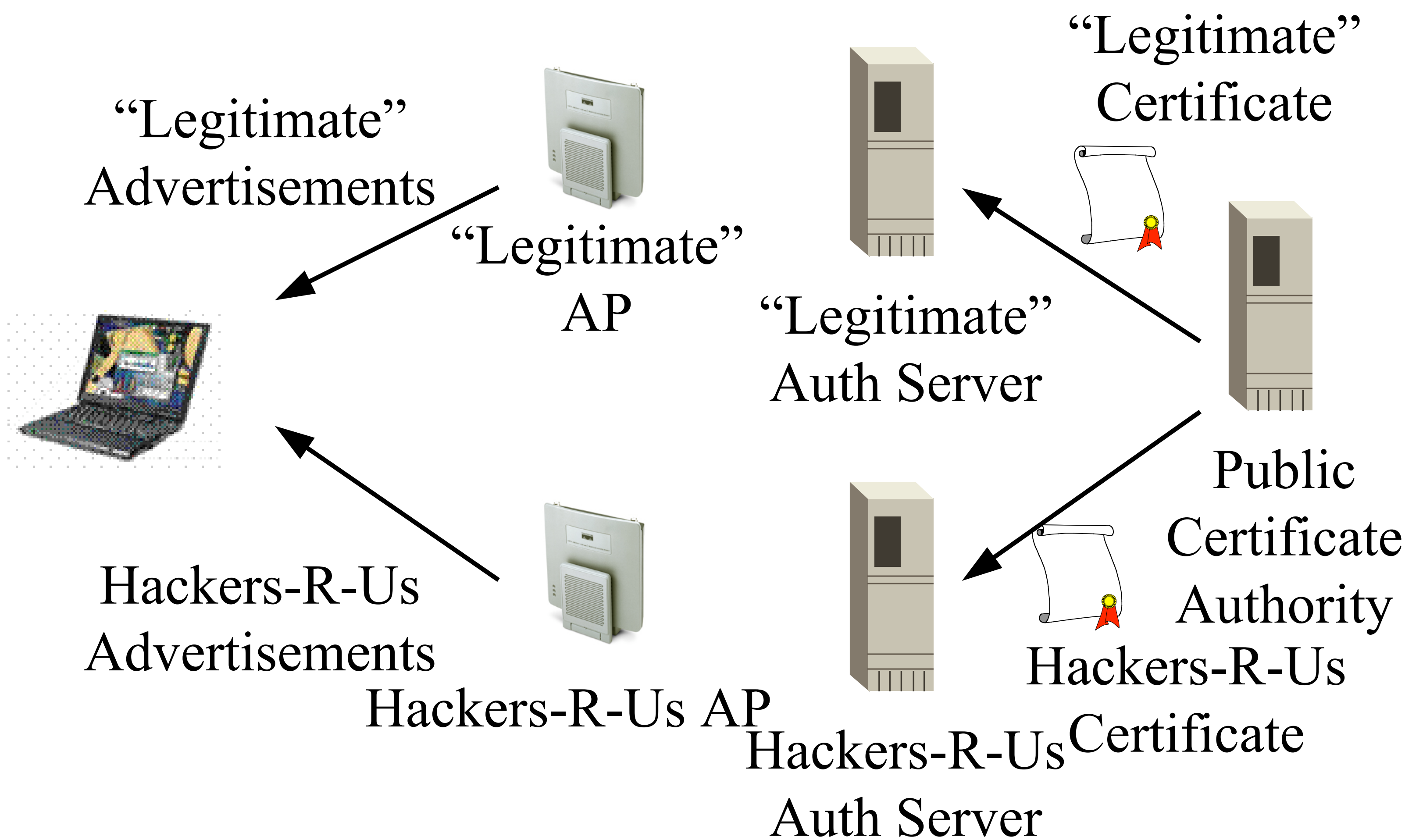
EAP-TLS Discussion (1)

- **EAP-TLS borrows the session establishment handshake from TLS (RFC 2246 = "Standardized SSL")**
- **X.509 certificate based model**
  - Works well ***if*** the enterprise has deployed infrastructure for X.509 certificates
- **Supports both mutual and bilateral authentication**
  - Because of e-commerce, enterprises know how to provision Server Certificate, even when they haven't deployed PKI
- **EAP-TLS protects itself from direct attack**
  - Can defeat MITM
  - Strong notion of a session
- **Generates a strong MSK**
  - With a strong AAA-Key and hence PMK

EAP-TLS Discussion (2)

- **To be secure, must avoid the e-commerce certificate model**
  - Server certificate must be provisioned on Client
  - N.B. This appears to be true of ***all*** uses of digital certificates with 802.11
- **To be secure, Client must break off association if it cannot contact the CRL server**
  - Or else Access Point becomes its Judge, Jury, and Executioner
- **Certificate and CRL download can be a performance problem**
- **Most important, not directly applicable to enterprises with RADIUS databases that are not X.509 based**

The E-commerce Model and 802.11



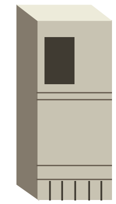
PEAP Description

- PEAP Overview
- PEAP Discussion

PEAP Overview

Wireless Station

AP



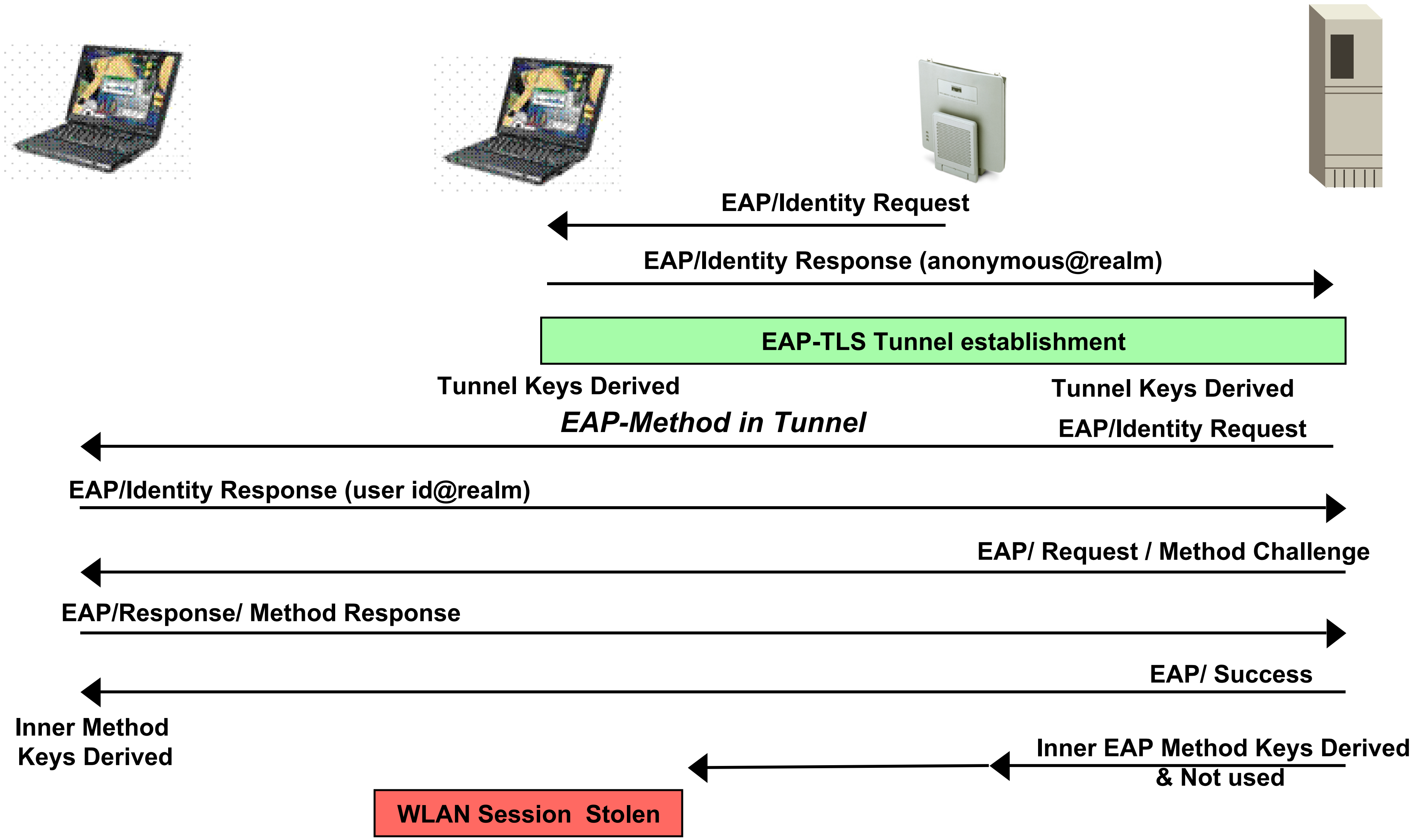
Authentication Server

Step 1: Use EAP-TLS to authenticate AS to Station

Step 2: Use TLS key to protect the channel between Station, AS

Step 3: Use Legacy method protected by TLS key to authenticate Station to AS

PEAPv1 Man-in-Middle Attack



PEAP Discussion

- **For legacy methods that produce session keys, their use with PEAPv2 is no worse than in native environment**
  - PEAPv2 protects against MITM attacks by binding the EAP-TLS MSK to the legacy method session key
- **For legacy methods that do not produce session keys (e.g., SecurID), PEAPv2 appears to offer better security than native environment**
- **PEAPv2 + legacy method finally achieves 802.11i goal of meeting market requirement**

RADIUS and Diameter (1)

- **The EAP transport in the back-end is outside of 802.11i scope and is not part of the standard**
- **Since the authentication architecture was adopted to meet market dictates to reuse RADIUS databases, it easily accommodates RADIUS**
  - And Diameter, since Diameter is the "next generation RADIUS"
- **RADIUS is not required by 802.11i**
  - Implementations exist using LDAP, COPS, and proprietary protocols as the back-end transport
  - The EAP transport to implement is strictly a business decision

RADIUS and Diameter (2)

- **RADIUS communication between the AP and the AS can be secured in two ways**
  - Manual keying
  - IKEv2
- **Diameter and COPS communication between the AP and the AS is secure via TLS**

Authentication Coda: 802.11i PSK

- **Consumers and small businesses unwilling to deploy Authentication Servers**
- **802.11i defines Pre-Shared Key (PSK) mode of operation**
  - User configures PSK on STA and AP
  - Instead of authenticating, STA and AP use PSK with the 4-Way Handshake to establish a secure link
- **Security is only as good as the PSK allows**
- **Access control decision is at PSK configuration time instead of run-time**

Part IV:
On-going Work

Selected On-going Work

- 802.11r
- 802.11s
- 802.11w
- EAP Keying Draft
- Operator Experiments and EAP-SIM

802.11r

- **Deployment experience shows that AP-to-AP transitions cost ≥ 200 msec with 802.11i**
  - Authentication is after reassociation
  - Almost all of the cost is authentication
- **Introduction of VoIP Wi-Fi handsets expected to overwhelm AS with frequent (re-)authentication requests**
- **802.11r established to address performance problems introduced by AP-to-AP transitions**

802.11s

- **How to build an 802.11 Mesh?**
- **Mesh-specific security problems:**
  - How do you identify mesh nodes that are authorized to route?
  - How do you establish a secure link between routing nodes?
  - How do you secure routing advertisements?
  - There is not necessarily an outside link to a centralized AS
- **802.11s established to address 802.11 mesh architecture, including security issues**

802.11w

- **802.11i only protects data frames**
- **802.11 has many control frames that need forgery and/or confidentiality protection as well**
  - 802.11e QoS negotiations
  - 802.11k radio resource measurements
  - 802.11u control frames
  - Disassociation, deauthenticate frames
- **802.11w established to address these problems**

EAP Keying Draft

- draft-ietf-keying-04-txt
- Documents how EAP keying works
- Attempts to address the key binding issues left open by the original design
- Work remains

Adapting 802.11i to Operator Space

- **Operators are attempting to roll out 802.11 service**
  - Lack of a viable business model still the largest roadblock
- **Trying to adapt 802.11i to their needs**
- **Using EAP-SIM for authentication**
- **When used with VoIP handsets, security appears no worse than in 3GPP networks**
- **Major security concerns about this architecture when used with data**

Summary

- **802.11i target = commercial grade security**
- **802.11i provides security as good (or as poor) as the PMK delivered to it**
  - Addresses all known issues with WEP
- **802.11i is backward compatible with WEP, and forward compatible with all existing and planned amendments**
  - Backward compatibility a practical necessity for any network protocol
  - Forward compatibility a necessity to avoid market dead-end
- **802.11i is extensible to other ciphersuites and authenticated key management methods**
- **802.11i uses 802.1X as its authentication framework, but this can be replaced (see prior bullet)**
- **802.1X/EAP/PEAP trades off security to meet the market imperative to support legacy RADIUS authentication**
  - Worldwide the market has said very explicitly that it will not procure solutions that don’t permit legacy authentication reuse

Backup

References

- IEEE Std 802.11i, July 2004
- IEEE 802.1X-Rev Draft 10.0, June 2004
- RFC 3748, “Extensible Authentication Protocol”, June 2004
- RFC 2716, “PPP EAP TLS Authentication Protocol”, October 1999
- RFC 3610, “Counter with CBC-MAC (CCM),” September 2003