

A History of 802.11 Security

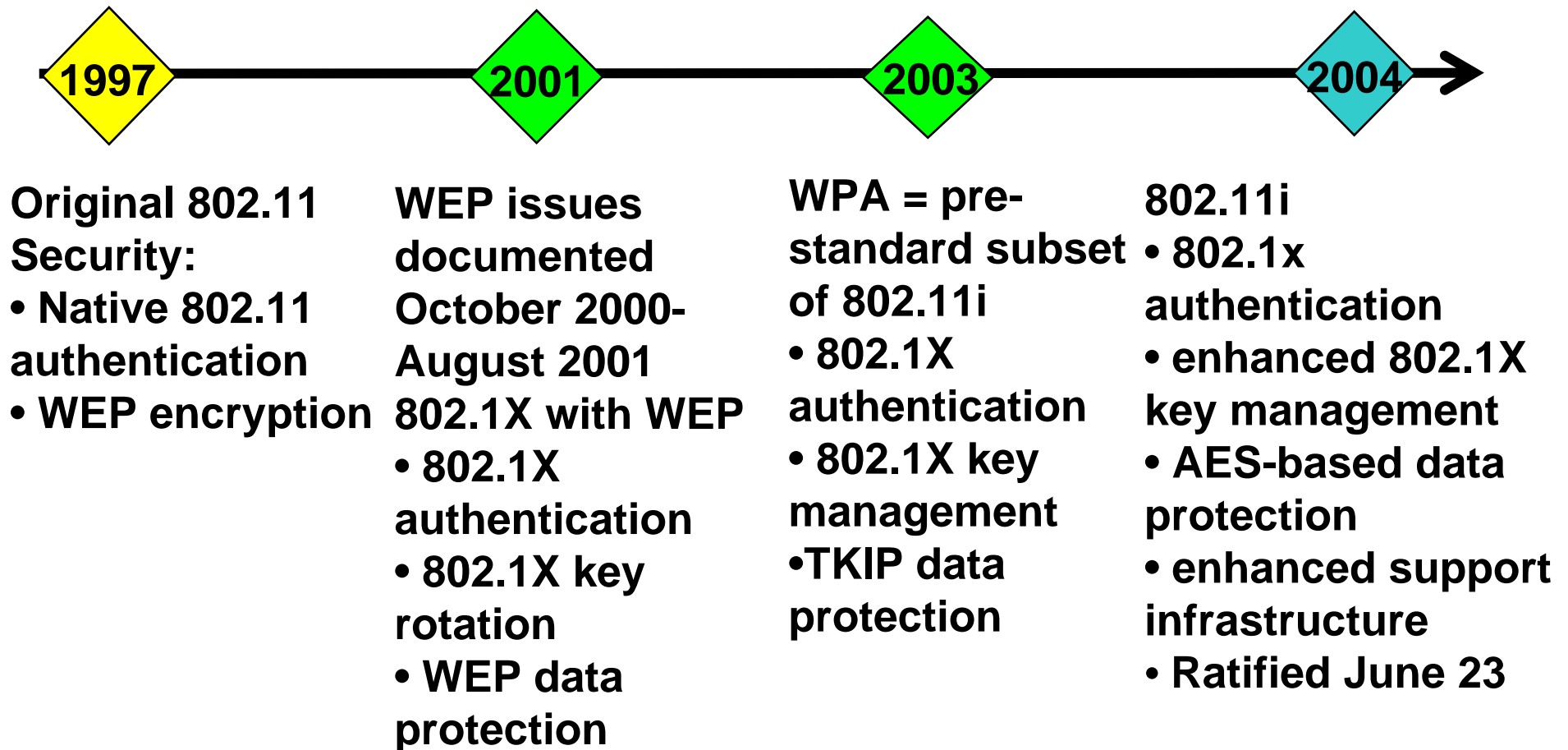
Jesse Walker
Communications Technology Lab
Intel Corporation
jesse.walker@intel.com

Goal and Agenda

- Goal:
 - What is 802.11i, and where did it come from?
- Agenda
 - In the beginning ...
 - Constraints and requirements
 - Architecture
 - Data protection
 - Discovery, authentication, and keying
 - Evaluation

In the beginning ...

Chronology of Events



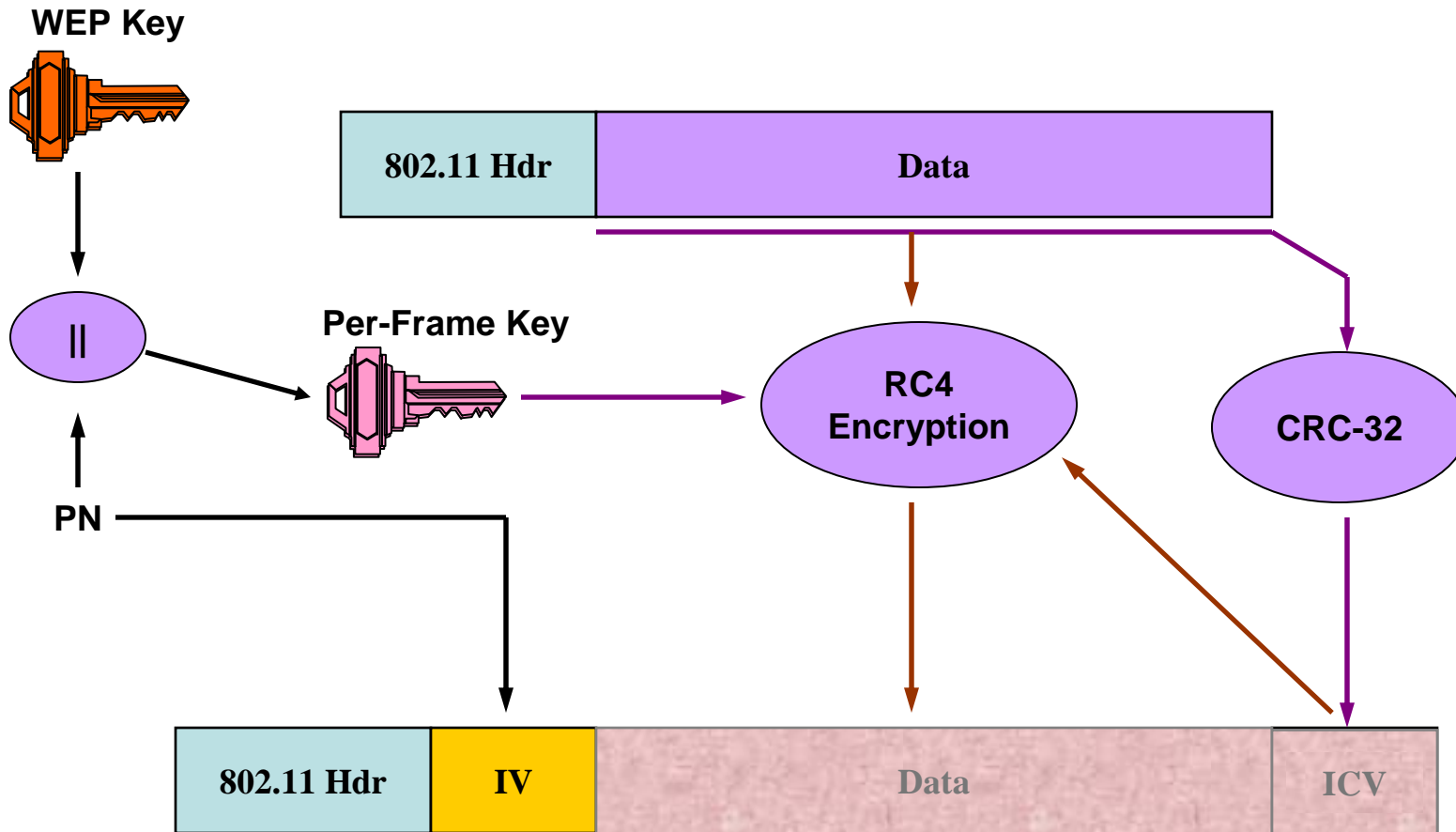
In the beginning ...

WEP: What is it?

- IEEE Std 802.11-1997 (802.11a) defined **Wired Equivalent Privacy** (WEP)
 - Unchanged in ISO/IEC 8802-11:1999
- WEP's Goals:
 - Create the privacy achieved by a wired network
 - Simulate physical access control by denying access to unauthenticated stations

In the beginning ...

WEP Description



In the beginning ...

WEP Analysis

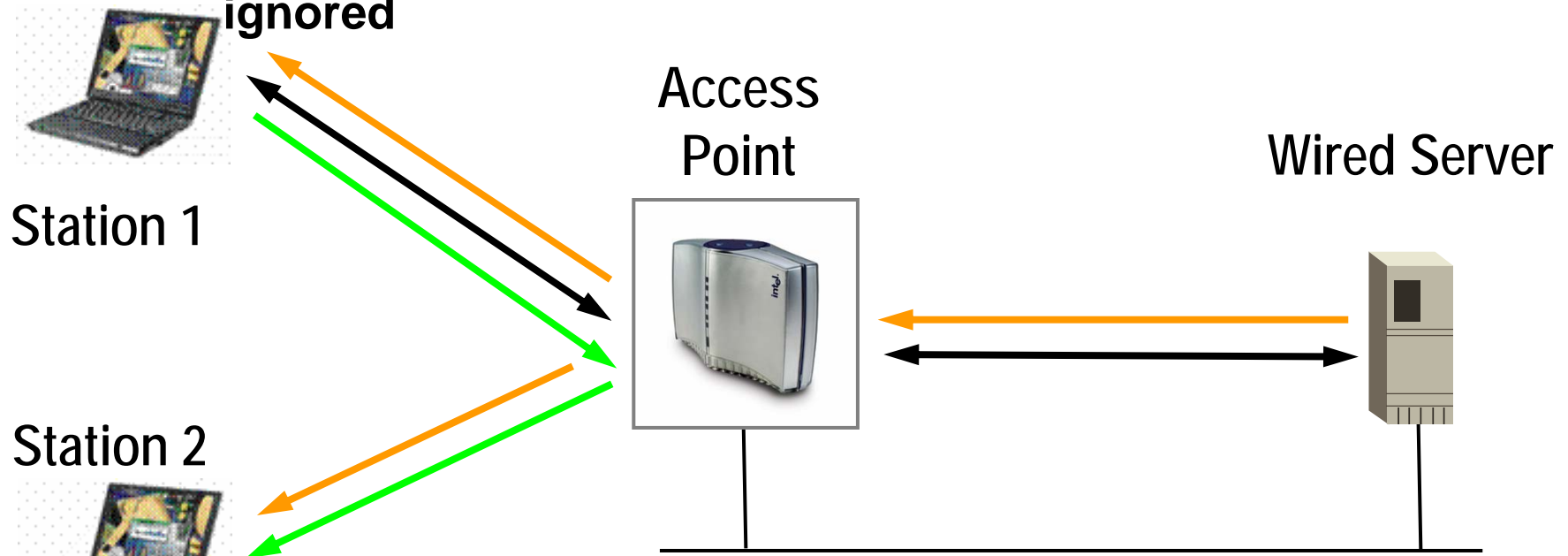
- Attacks against WEP published before the ink was dry
 - Walker, “Unsafe at any Key Size” , IEEE 802.11 doc. 00-362, October 2000
 - Arbaugh, “An inductive Chosen Plaintext Attack against WEP”, IEEE 802.11 doc. 01-230, May 2001
 - Borisov, Goldberg, Wagner, “The insecurity of 802.11”, Proceedings of International Conference on Mobile Computing and Networking, July 2001
 - Fluhrer, Mantin, Shamir, “Weaknesses in the key schedule algorithm of RC4”, Proceedings of 4th Annual Workshop of Selected Areas of Cryptography, August 2001
- 802.11 instituted remediation in November 2000
 - Specification of a replacement for WEP became a TGe work item

Protection Requirements

- Migration path or compatibility with WEP-only equipment
- Never send or receive unprotected data frames
- Message origin authenticity — prevent forgeries
- Sequence frames — prevent replays
- Don't reuse keys – a key establishment protocol needed
- Avoid complexity: avoid rekeying — 48 bit frame sequence space
- Protect source and destination addresses – prevent header forgeries
- Use one cryptographic primitive for both confidentiality and integrity – minimize implementation cost
- Interoperate with proposed quality of service (QoS) enhancements (IEEE 802.11 TGe) – don't compromise performance

Design Constraints

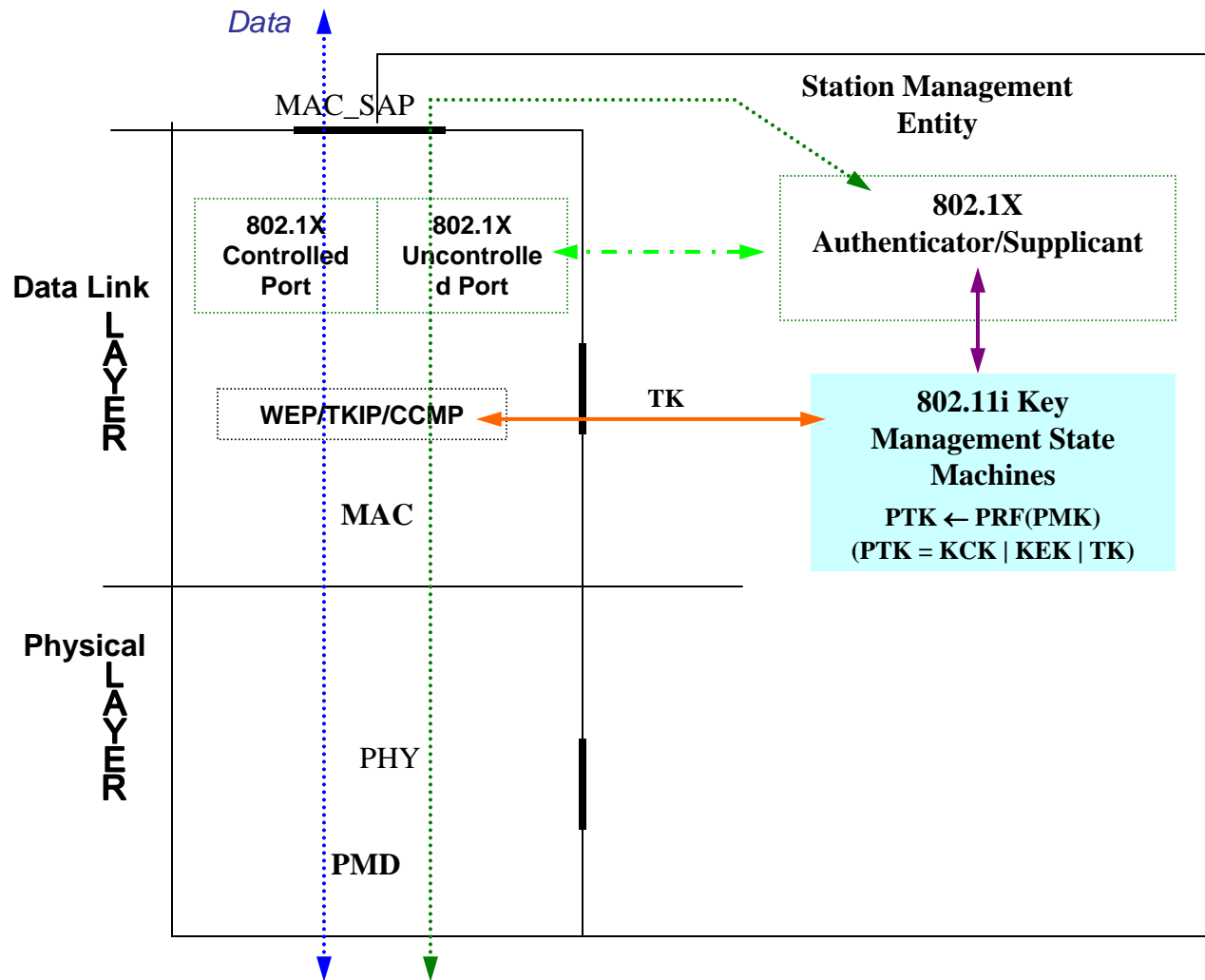
Constraint 3: Multicast integral to modern networking (ARP, UPnP, Active Directory, SLP, ...) and cannot be ignored



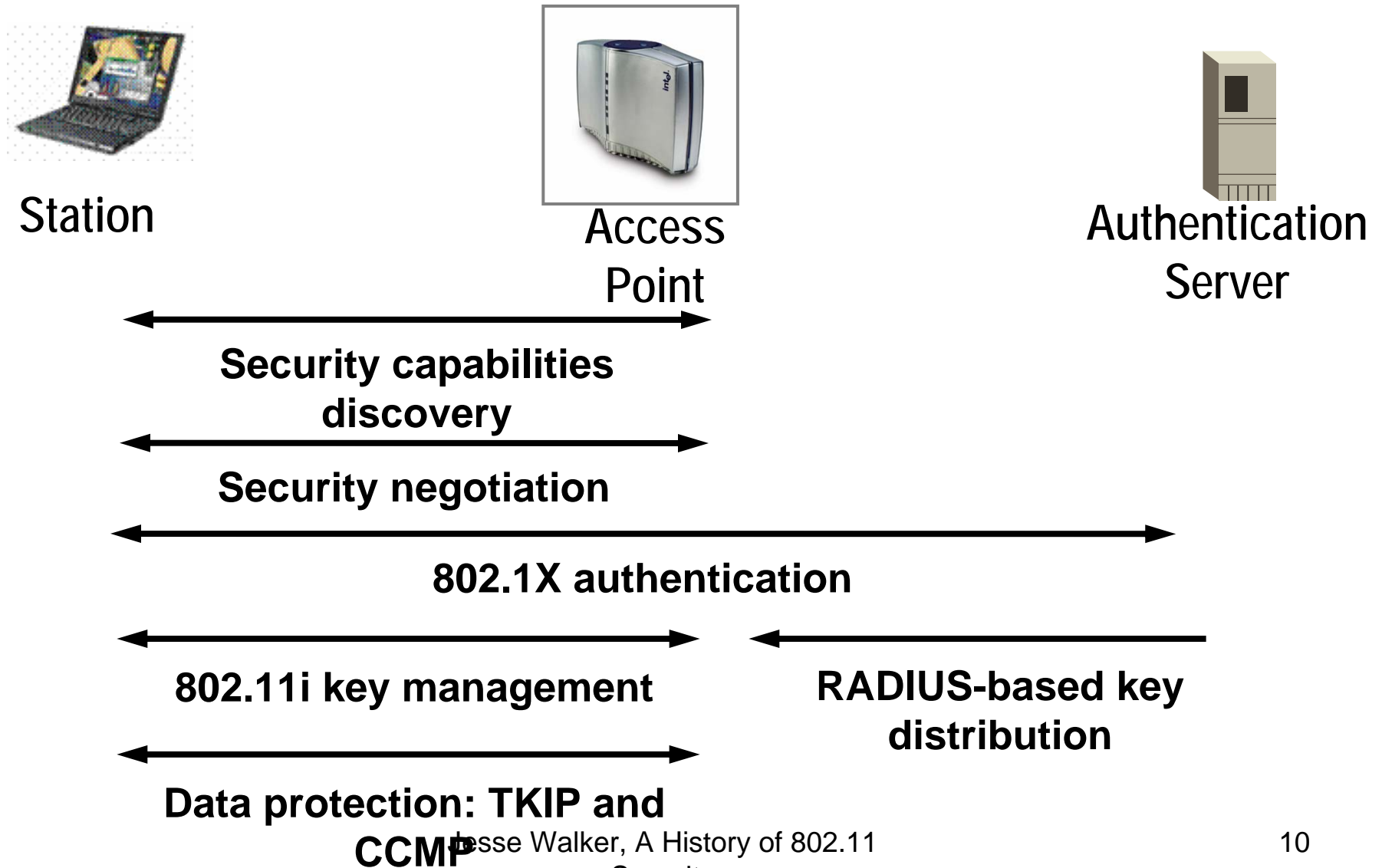
Constraint 1: All messages flow through access point; 1st generation AP MIPS budget = 4 Million instructions/sec

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

802.11i Architecture



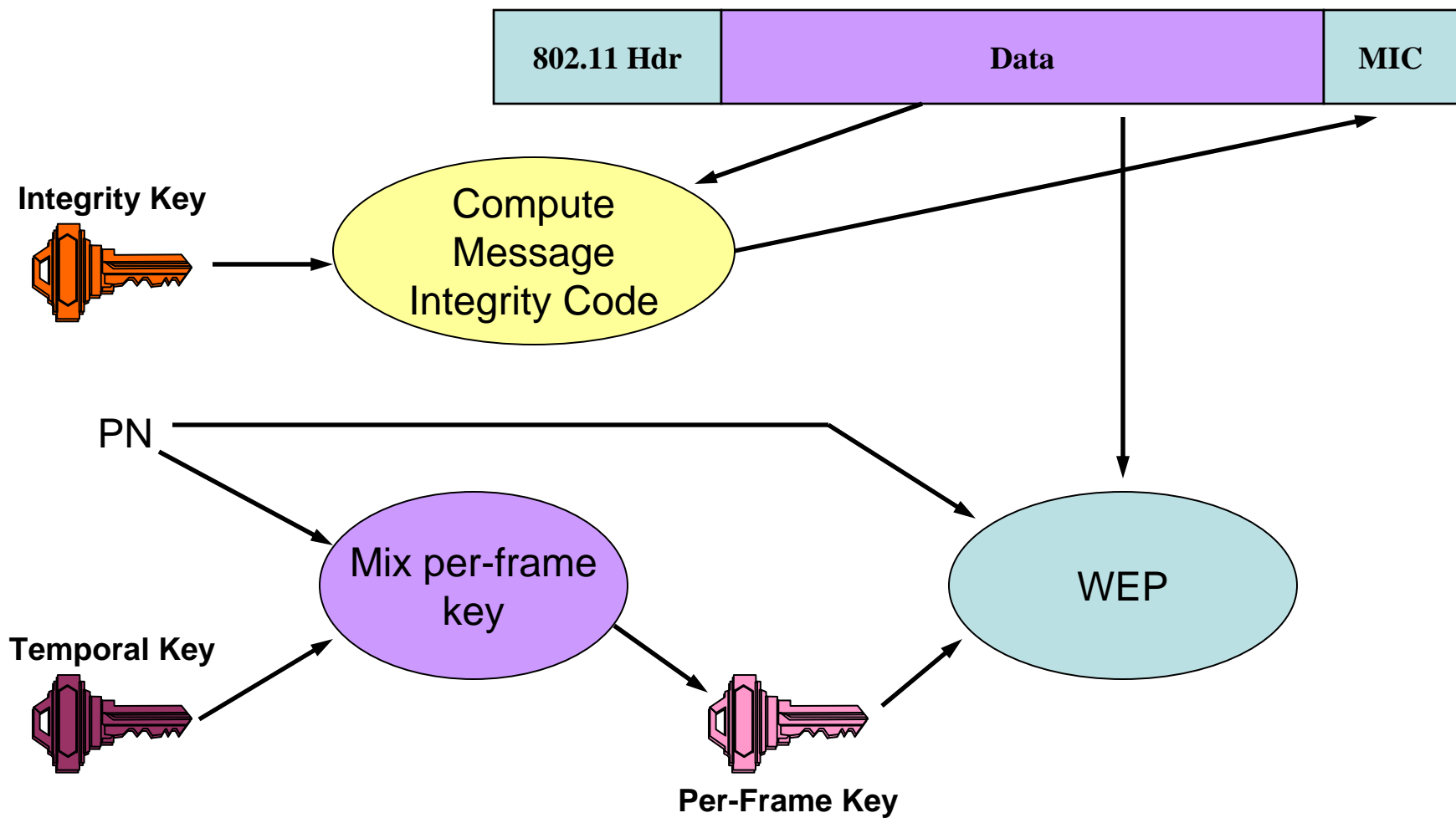
802.11i Phases



TKIP Overview

- Legacy hardware addressed second
 - I never believed it was feasible
- TKIP: *Temporal Key Integrity Protocol*
 - Conform to 1st generation access point MIP budget: 4 Million Instructions/sec
 - o Must reuse existing WEP hardware
 - Special purpose Message Integrity Code – costs 5 instructions/byte \approx 3.5 M instructions/sec, and protects source, destination addresses (Ferguson, “A MAC-implementable MIC for 802.11”, November 2001)
 - Prevent Replay: WEP IV extended to 48 bits, used as a packet sequence space (Stanley, 802.11 doc. 02-006)
 - New Per-frame key constructed using a cryptographic hash (Whiting/Rivest, 802.11 doc 02-282, May 2002) – costs 200 instructions/frame \approx 300K instructions/sec
- Designed to permit migration to new hardware

TKIP Overview

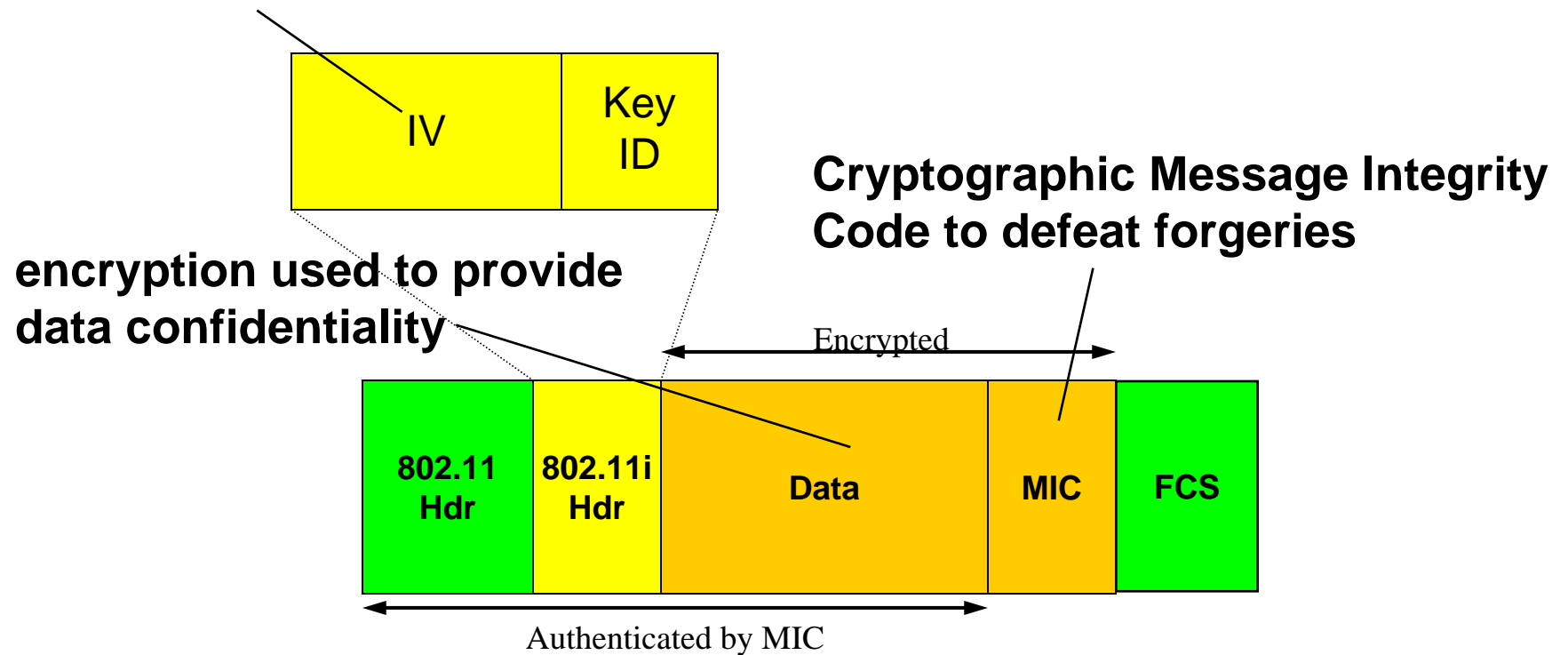


AES CCMP

- Long term problem addressed first
 - Backward compatibility always hard(er)
- All new protocol with few concessions to WEP
- First attempt: protocol based on AES-OCB (Walker, 802.11 doc. 01-018)
 - OCB = Rogaway's Offset Code Book mode
 - Costs about 20 instruction/byte in software \approx 15 M instr/sec
 - Removed in July 2003 due to IPR issues
- Second attempt: similar protocol based on AES-CCM (Ferguson-Housley-Whiting, 802.11 doc. 02-001)
 - Prevent replay – Frame sequence number enforcement
 - Provide confidentiality – AES in Counter mode
 - Provide forgery protection through CBC-MAC
 - Costs about 40 instructions/byte in software \approx 30 M instr/sec
 - Replaced AES-OCB in July 2003
- Requires new AP hardware
 - CPU Budget of 1st generation AP: 4 M Instructions/sec
 - RC4 off-load hardware doesn't do AES or CCMP

Frame Format

IV used as frame sequence space to defeat replay



Authentication Overview

- Authentication, not WEP flaws, led to new security work in 802.11
 - Original authentication was 802.11 specific
 - Enterprise market refused to deploy WLANs if legacy RADIUS authentication could not be reused
- Candidate solutions considered
 - 802.1X (Aboba, Halasz, Zorn, 2000)
 - Kerberos/GSSAPI (Beach, Walker 802.11 doc. 00-292)
- 802.1X adopted in November 2000
 - Business, not technical decision, drove selection

Discovery, authentication, and keying

IEEE 802.1X Layering



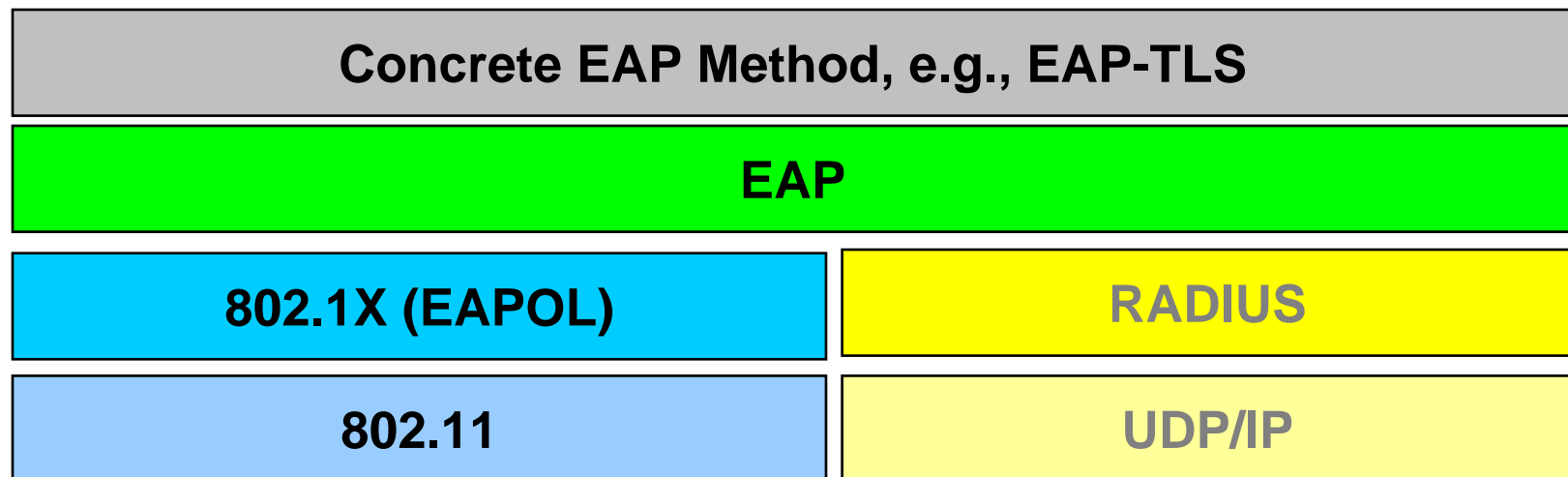
Wireless
Station



Access
Point

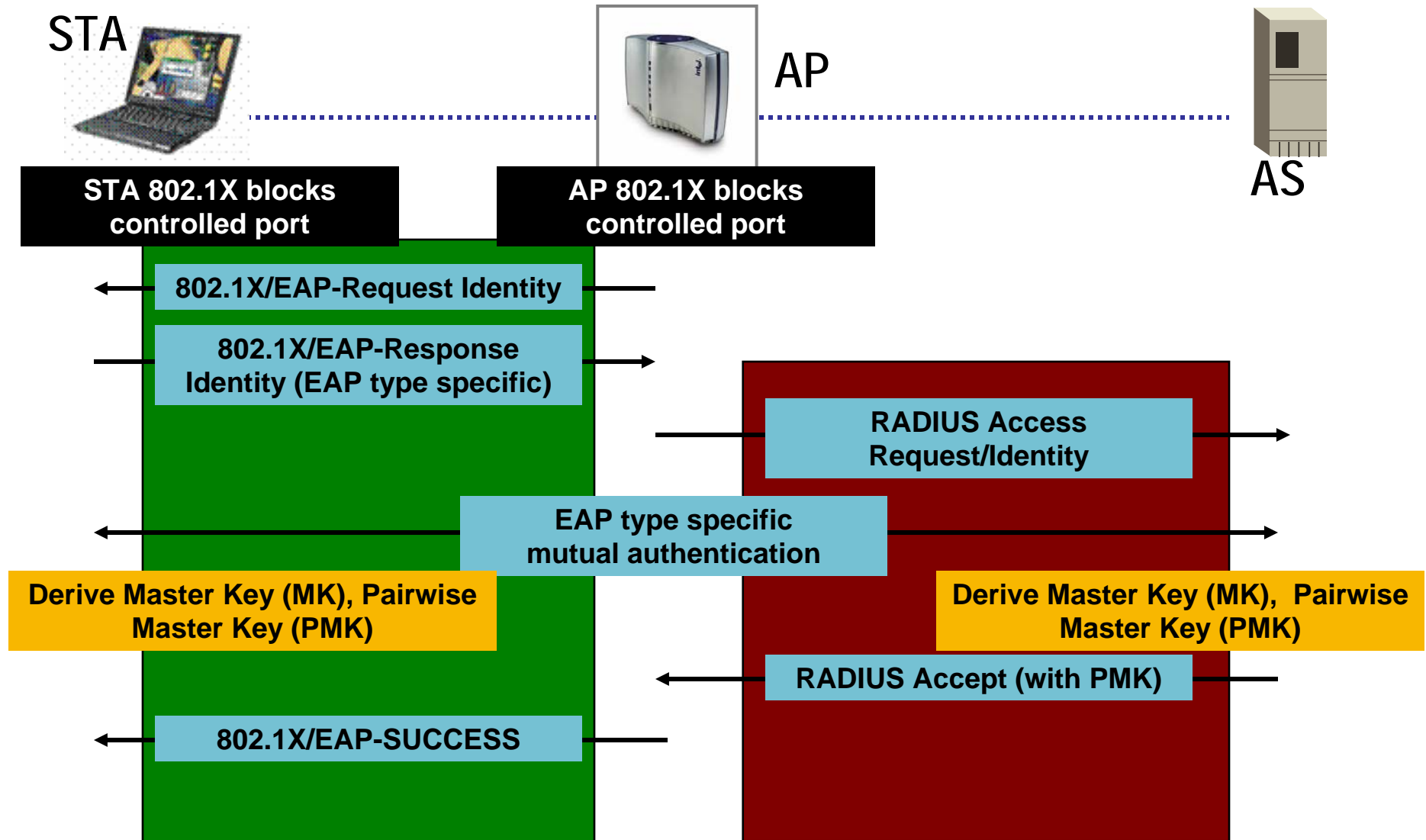


Authentication
Server



Discovery, authentication, and keying

Authentication Overview



802.1X

Jesse Walker, A History of 802.11 Security

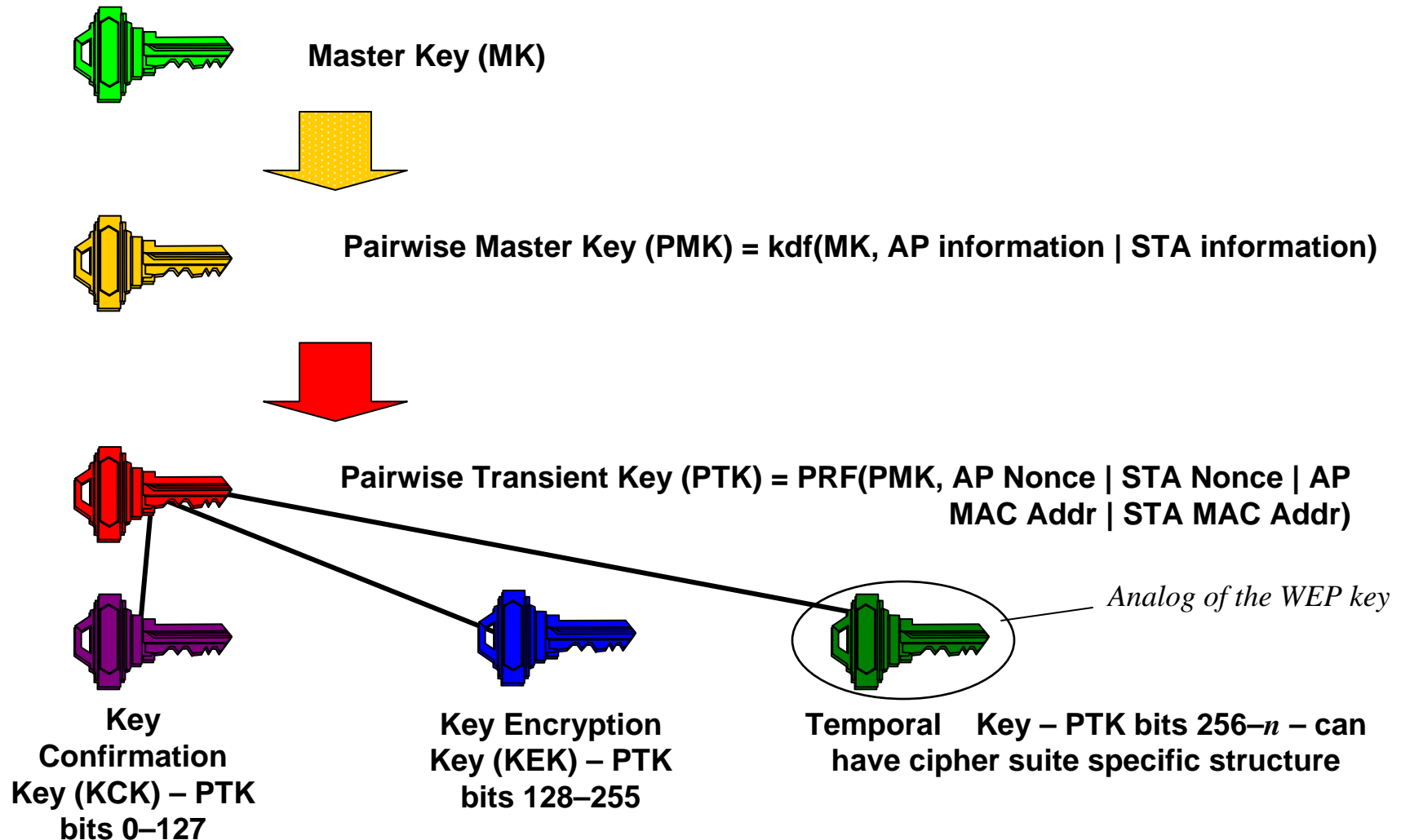
RADIUS

Keying Overview

- Requirements:
 - Prevent WEP's key reuse (guarantee fresh keys)
 - Synchronize key usage
 - Verify liveness and proof of possession
 - Bind key to STA and AP
- Candidate solutions considered
 - Authenticated Key Exchange (Cam-Winget, Housley, Walker, 802.11 doc. 01-573, November 2001)
 - 802.1X keying (Moore, November 2001)
- 802.1X adopted in November 2001
- Deficiencies of each redesign noted in January, February, March, May of 2001
- "Final" design completed in May 2002 (Moore, 02-298)

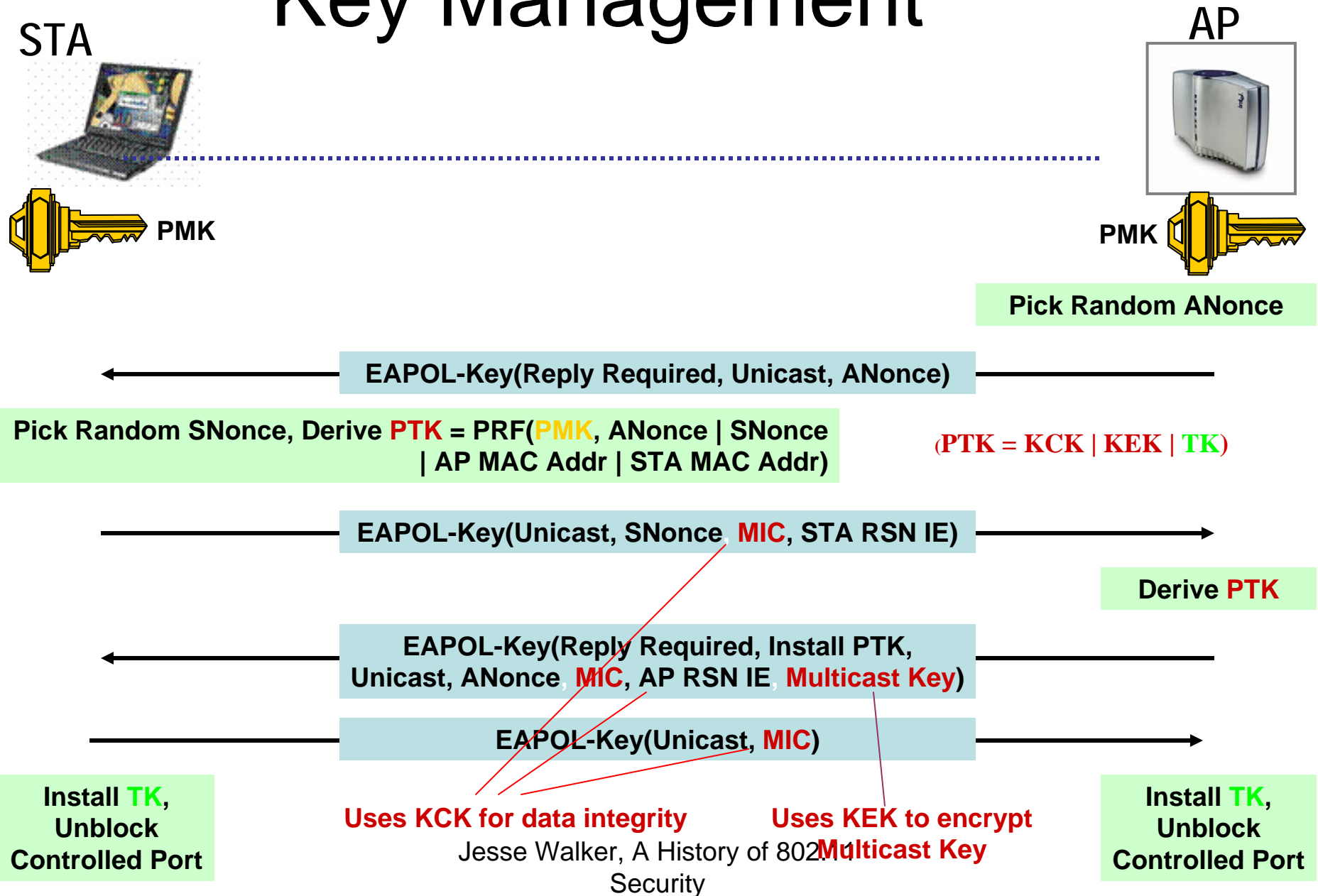
Discovery, authentication, and keying

802.11i Key Hierarchy



Discovery, authentication, and keying

Key Management



Discovery Overview

- Requirements:
 - Advertise AP capabilities
 - Negotiate session capabilities
- Candidate solutions considered
 - No significant differences between any of the proposals
 - Authenticated Key Exchange (Cam-Winget, Housley, Walker, 802.11 doc. 01-573, November 2001)
 - 802.1X keying (Moore, November 2001)
- Approach in 802.1X keying proposal adopted in November 2001

Discovery, authentication, and keying

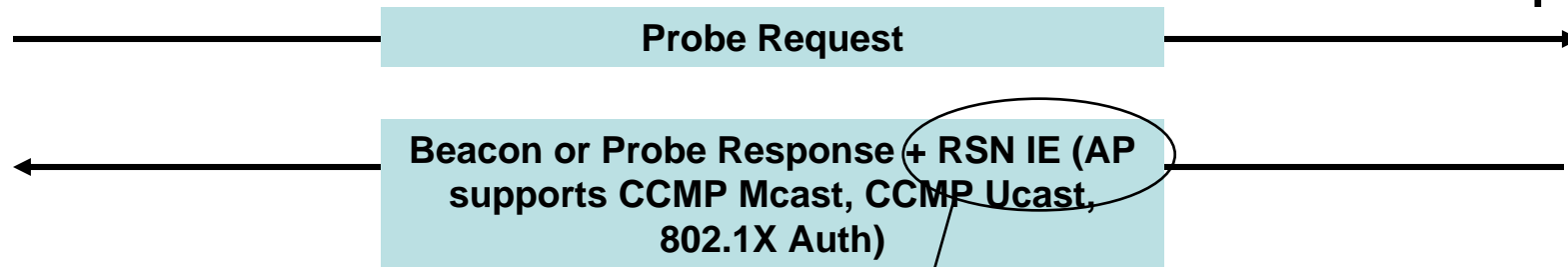
Discovery



Station



Access Point



Advertises WLAN security policy

Discovery, authentication, and keying

Capabilities Negotiation

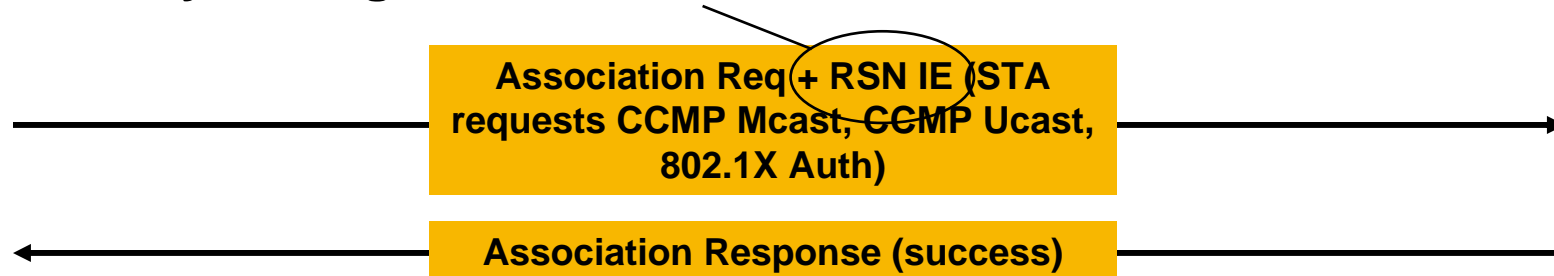


Station



Access
Point

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



How did we do?

- 802.11i is a horse defined by committee
- AES-CCMP believed to be a solid design
 - But limited by reuse of WEP key name space
- TKIP meets the requirements for a good standard – everyone is unhappy
- Authentication scheme well-tuned to the enterprise
- Key “works” if deployed correctly
 - STA, AP binding to session key missing
 - No distinction made between key separation, peer liveness functions
- 802.11i already a market success
 - All vendors have embraced it
 - Wi-Fi Alliance certifies it as WPA and WPA2
 - 275K devices implementing 802.11i ship each day

Remaining Issues

- Broadcast vulnerable to insider attack
 - But Boneh, Dufree, and Franklin (EUROCRYPT '01) showed better solutions unlikely without auxiliary assumptions, e.g., TESLA
- Defense against interference attacks – research
- How do I enable the)*#!% security? – WFA attempting to define “Easy Setup”
- Key binding – IETF EAP Keying work
- Protection for Management frames – 802.11w

Feedback?

