# Amending 1X

The devils in the details for P802.1af

Mick Seaman
mick_seaman@ieee.org

# Amending .1X

- The goal
- The current state of .1X
- Treading cautiously
- A possible structure with .1af
- Summary & conclusions

# The goal (1)

.1X/EAP supports

- 'Naked' Ethernet operation
- .11i
- MACsec/802.3 (or other)
- Potentially other 'keyed' media/scenarios

sharing architectural concepts, infrastructure support, and many management operations.

# The goal (2)

EAP used/usable in all cases to provide authentication.

- ‘Token’ of authentication is PMK for ‘keyed’ cases i.e. .11i and MACsec
- .11i specifies derivation of session keys from PMK
- New .1X clauses derive MACsec SAKs from PMK(s)
  - CAK = PMK for point-to-point
  - CAK derived/shared using transitive PMKs for groups
  - KSP derives SAKs using succession of CAKs.

# The goal (3)

Controlled/Uncontrolled Port ‘Y’ common to all cases.

- Used by common PAE
- Fully specified (somewhere at least)

Asymmetric and symmetric communication specified i.e. devices that naturally have Supplicant/ Authenticator roles and devices that don’t fully covered.

.

# The current state of .1X (1)

Many traces of its history

- Role of keys/PMK as a token of Auth. almost hidden
  - Not mentionned until clause 6.7 bullet (a)
  - Describes authorization as a state of communication
- Almost entirely authorization of secure physical wire
  - Restrictions to physical characteristics in many places
  - Integrity not mentioned in body of standard at all
  - Confidentiality mentioned once (non-goal)

# The current state of .1X (2)

- Controlled/uncontrolled port ‘Y’ not an entity
  - No physical instantiation specified, a property of a port?
  - Thus hard to write text saying use (a), (b), or (c) to realize

  - No ‘upper’ interfaces
  - Therefore no MAC_Operational status for Uctrld./Ctrld. Port
  - Thus theoretically does not support MAC Service i/f.
  - Thus does not support current 802.1 protocol machines (e.g. RSTP state machines)

  - Can’t precisely locate ‘Y’ function in a complex i/f stack (.11i solves its own problem, as does MACsec, leaves ‘naked’ case unsolved)

# The current state of .1X (3)

- Supplicant PAE state machine very end station specific
  - Not surprising, matches .1X target scenario
  - Assumes, e.g., that supplicant is AUTHENTICATED when PortValid, coupling authentication directly to communication, rather to a key that can facilitate communication

    (In other words authorization is synchronous with communication)
  - Unclear whether other ‘keyed media’ should redefine this machine entirely (as per .11i) case by case, or reinterpret machine, or whether a new general machine is needed

# Treading cautiously

- Absolutely no intention of changing or even appearing to change conformance requirements for .11i
- Not interested in changing requirements for ‘naked’ Ethernet, although clarification may be desirable

# A possible structure (1)

- Clarify that .1X is defines PbNAC, common architecture for implementing control, framework for authentication/authorization inc master key distribution, EAPOL for EAP transport
  - Remove/clarify restriction to ‘physical access’ and p2p
- Clause 6 Ctrl./Uctrl. Port is architecture for PbNAC
  - Clarify that ‘Y’ function is implemented in a number of ways .11i, ‘naked’ Ethernet/media, 802.1AE MACsec, other (?)
  - Be explicit about PAEs role in acquiring master key & about relationship of keying to protection of access to Port
- Profile Cl. 9 parameters to clarify which apply to ‘naked’ Ethernet, which to .11i (do any apply to .11i?)
- Add new clause for ‘naked’ and ‘1X above’ implementations, so Cl. 6 is ‘clean’, specify interfaces/MAC status etc., relate to existing Cl. 8 PAE machine

# A possible structure (2)

- Reference .1AE for implementation of ‘Y’ function for MACsec
  - And for relationship of 1af to 1AE
- Define key hierarchy for .1AE/.1af
- Add new clause for PAE machines for .1af
- Add clause to derive/distribute group CAK from pair-wise PMKs
- Add clause for KSP (updated version w.r.t 1af D0.1)
- Profile Cl. 9 parameters to clarify which apply to .1AE
- Add mgmt clauses for KSP & group key derivation

# Summary & conclusions

- .1X currently obscure about the things we value it for
  - Very understandably, given its development history
  - PMK distribution very much an after thought
  - .11i largely glued on as ‘forget this, look there’
- Can be straightened out, mainly as an editorial exercise
  - Without risk to existing implementations!!
  - Making it much cleaner to add in .1af
- New PAE machines needed for .1af
  - Decouple master key acquisition as auth. token from use
  - Support continued connectivity as master key changes