802.1X/802.11 Issues

Nancy Cam-Winget, Cisco Systems
Paul Congdon, Hewlett-Packard
Jesse Walker, Intel Corporation

Agenda

- Issues with 4-way/group key handshakes
- Issues with pre-authentication

4-Way/Group Key Handshake Issues

- These
  - Represent new protocols, not simply message formats
  - Have implications for the 802.1X statement machines
  - Have expected sequencing with EAP-Success message
  - Enable unicast and multicast traffic independently via same ‘port’
- Obviously important and justifiable work
- Need to decide
  - Whether this work belongs in 802.1X or in 802.11i
  - How to resolve state machine interactions
  - Minimize impact on both 802.11i and 802.1X

4-way Handshake

- New 802.1X protocol used to:
  - establish liveness between STA and AP
  - Establish fresh PTK between STA and AP (at both 802.1X and 802.11 layers)
  - Binds management of 802.1X and 802.11 keys
- Diverges from 802.1aa
  - TGi relies on EAP-Success to trigger 4-way handshake
  - Different than current 802.1X key state machine
  - Incompatible with current 802.1aa state machines and interface

Group Key Handshake

- Relies on a successful 4-way handshake, but not clarified in the 802.1X statement machine
- Relies on unicast traffic to be protected → implies *partial* port block *or* distinct port at both STA and AP

Consensus from 802.11i ad-hoc on 4-way handshake

- Recommend that current key machines in 802.1aa are optional
  - Indicate that other key machines defined in 802.11i may be used
  - Indicate in 802.11i that 4-way handshake ‘replaces’ key machines of 802.1X and does not ‘use’ them as defined.
- Recommend and document appropriate key machine interface in 802.1aa
  - Diagram interface to key machines
  - Define variables and interface procedures
- Force opposite sequence of EAP-Success and key machine initiation in 802.1aa

Pre-authentication Issues

- These
  - 802.1X was not designed to work this way
  - have implications for the 802.1X state machines
  - potentially an additional security threats
- Obviously important and justifiable use of 802.1X
- Need to decide
  - Whether this work belongs in 802.1X or in 802.11i
  - How to resolve state machine interactions
  - Minimize impact on both 802.11i and 802.1X

Pre-authentication

- Forwarding EAPOL frames over DS:
  - Allows STA to authenticate with next AP prior to association via current AP
  - Allows an STA to authenticate with multiple APs at a time
  - Completes when the 1st message of the 4-way handshake is received by the new AP
- New paradigm for EAPOL over wired media
  - Unicast EAPOL frames on wired media
  - No concept of a ‘port’ over the DS to work with
  - Termination conditions are different than normal wired EAPOL exchanges

Ideas to address pre-authentication issues

- Define how 802.1X machines can run on wired shared media
  - Create a new concept of a ‘virtual port’ for new MAC addresses or learning events
  - Specify VLAN tagging rules for unicast EAPOL frames
- Encapsulate pre-authentication EAPOL frames differently
  - Define a new Ethertype for pre-auth EAPOL frames to skirt issues current rules
  - Establish a ‘connection’ to create a ‘virtual port’ for pre-auth converation
- Have 802.11i re-define authenticator state machines to support pre-auth using combinations of above
- Others?