IEEE 802.1X Pre-Authentication

Bernard Aboba
Microsoft

Outline

- Goals
- Conclusions
- Overview of pre-authentication
- State machine
- Threat model
- EAP requirements
- Management frame protection
- Control frame protection
- Protected negotiations
- Key activation
- Summary

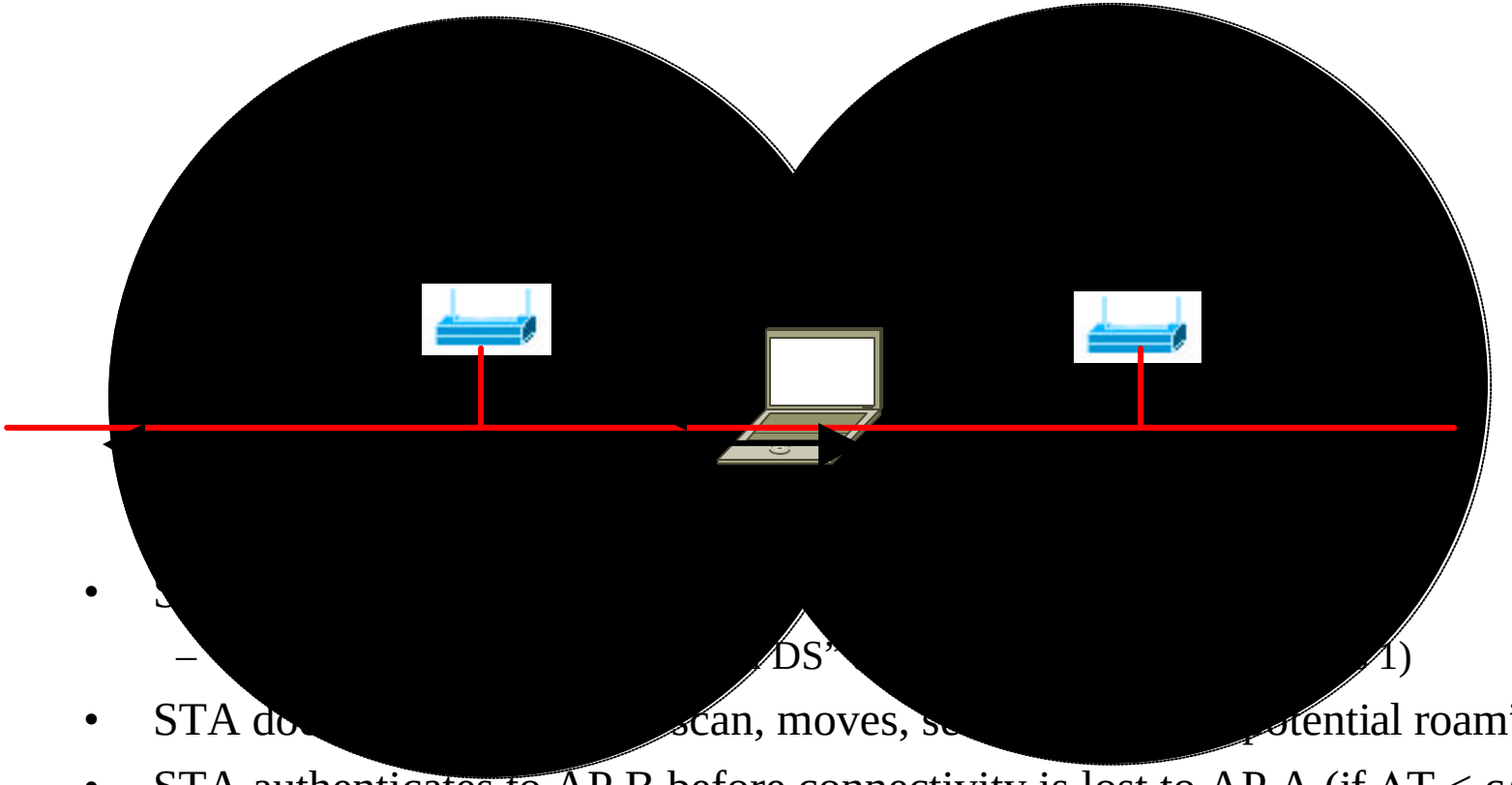
Goals

- To present a strawman threat model for IEEE 802.11 Tgi
  - Tim Moore to present detailed threat analysis on Thursday
- To understand the implications of IEEE 802.1X pre-authentication
  - Pre-authentication supported in 802.11i Draft 2.2
- To analyze solutions to potential threats
  - Protected capabilities negotiation
  - Key activation
  - Management frame authentication
  - Control frame authentication

Conclusions

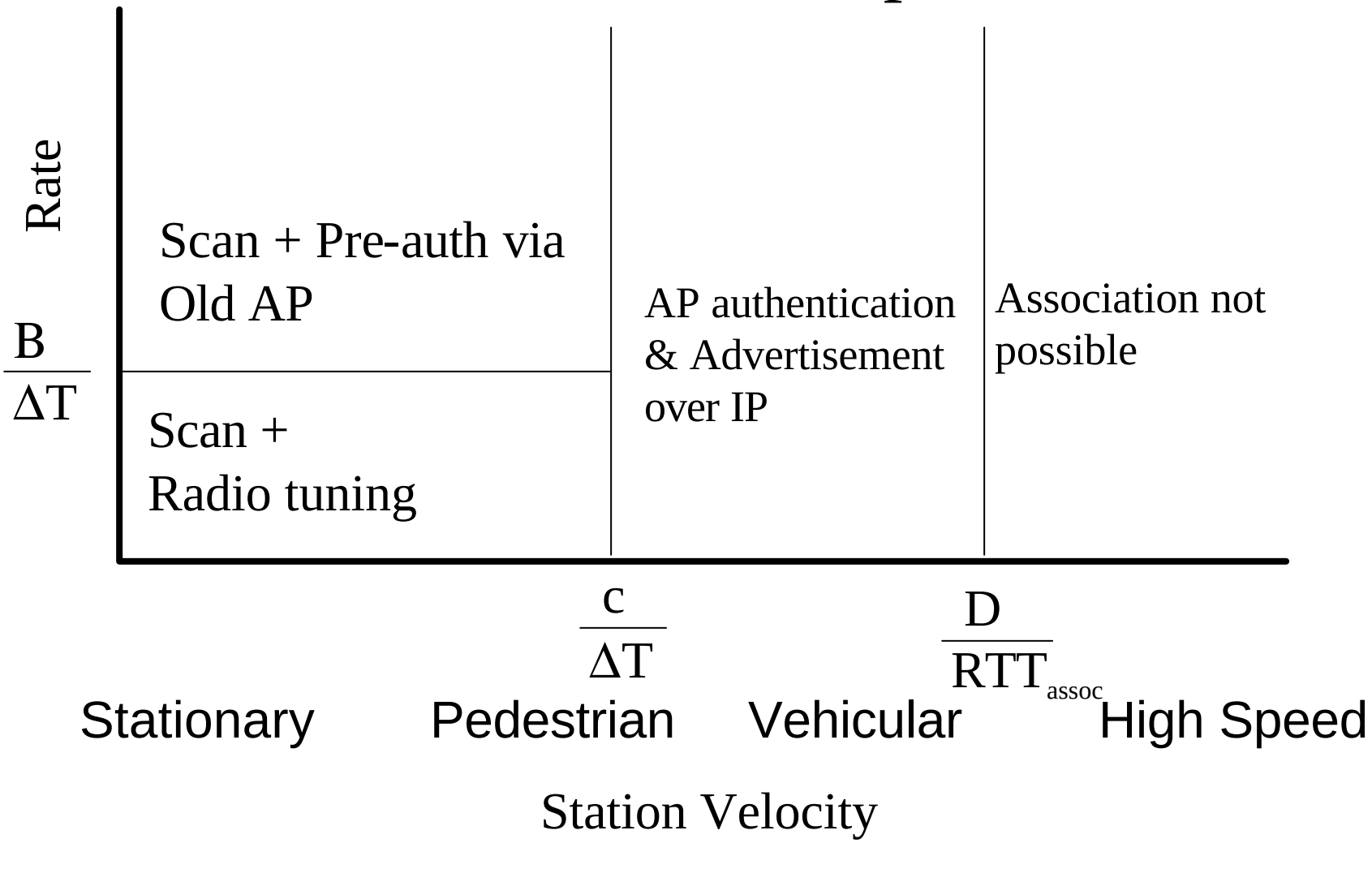
- IEEE 802.11i needs a threat model.
  - Without a threat model, you never know when you're done!
  - IEEE 802.1X could use a formal threat model too (to avoid misunderstandings).
- IEEE 802.1X pre-authentication with 802.11 introduces some new wrinkles
  - Supplicant-only initiation
  - Station authenticated to multiple Authenticators simultaneously
  - No controlled and uncontrolled ports
  - 802.11 state machine controls access, not 802.1X state machine
  - IEEE 802.1X frames have a unicast DA and may be forwarded
- IEEE 802.1X pre-authentication has substantial advantages for 802.11
  - Pre-authentication enables a station to authenticate to multiple APs, which is not possible when 802.1X occurs *after* Association.
    - Minimizes connectivity loss during roaming
  - IEEE 802.1X pre-auth makes it possible to authenticate and derive keys early on, use keys to protect as many messages as possible
  - Most management and control frames can be protected, with the exception of Beacon and Probe Request/Response

802.1X Pre-Authentication

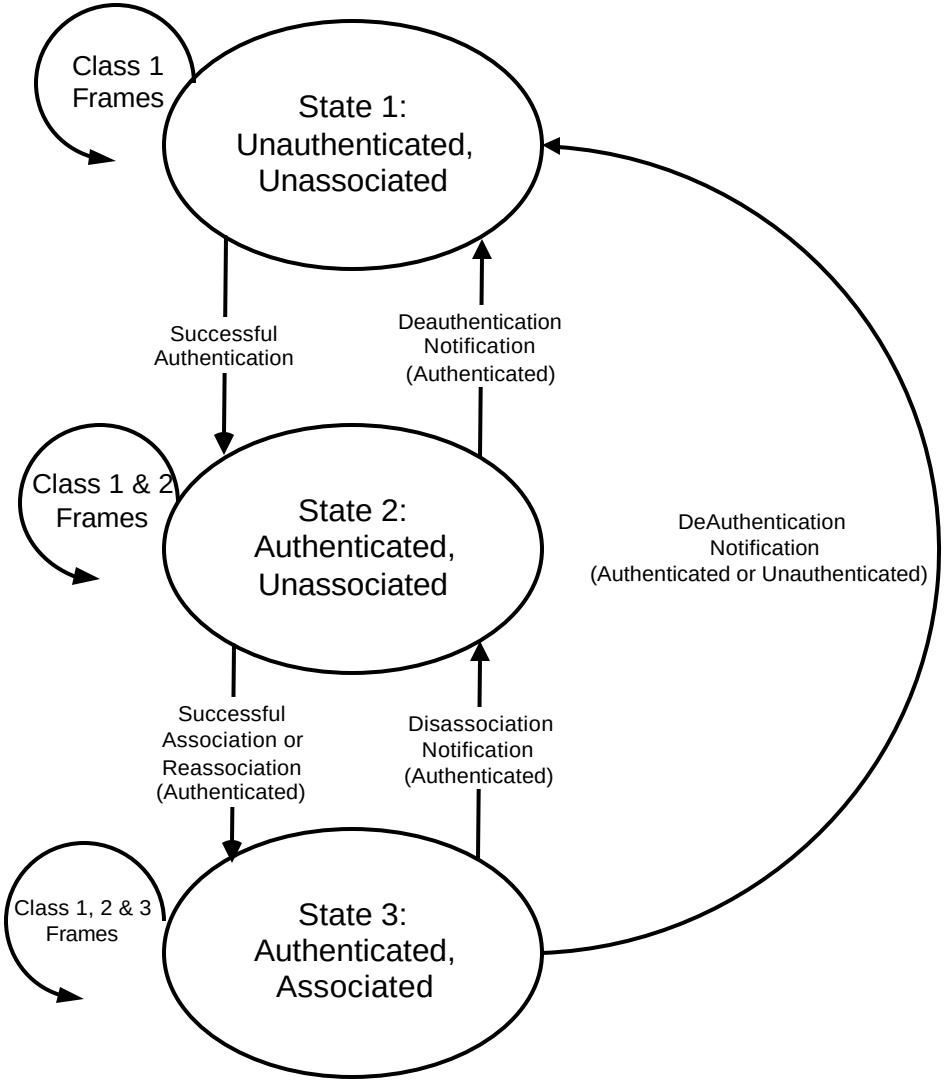


- S
  - DS" 1)
- STA do can, moves, s otential roam"
- STA authenticates to AP B before connectivity is lost to AP A (if $\Delta T < c/v$)
  - Can send unicast 802.1X data frames to AP B, forwarded by AP A
    - "From DS" or "To DS" set to true (Class 3)
  - Can tune radio to Channel 11 (if $B > r \Delta T$)
- STA reassociates to AP B

The Problem Space



State Machine



- Original 802.11 state machine can be used
- IEEE 802.1X data frames can be sent in State 1,2
  - To DS, From DS =0
  - “Unassociated pre-auth”
- IEEE 802.1X data frames can be sent in State 3
  - To DS or From DS = 1
  - “Associated Pre-auth”
- Unauthenticated Deauth can be silently discarded by STA

Pre-Authentication State Machine

- No “controlled” and “uncontrolled” ports
  - In fact, no “ports” at all!
  - Port doesn’t exist until Association/Reassociation exchange
  - RADIUS Access-Request contains no NAS-Port attribute
  - Accounting START sent after successful Association/Reassociation Response w/NAS-Port
- Supplicant initiation only
  - Supplicant authenticates to APs that it is likely to roam to
  - Since roaming decision made by STA, it also handle auth initiation
  - Unsolicited EAP-Request/Identity frames are silently discarded
- 802.11 state machine governs frame treatment
  - 802.11-1999 state machine already supports pre-authentication, no changes required
  - 802.1X “auth complete” an input to 802.11 state machine
  - Reverse of 802.1X after Association, where 802.11 events are inputs to 802.1X state machine

Strawman Threat Model for 802.11

- Snooping, modification or injection of data packets
- Impersonation of legitimate 802.11 STA or AP
- Modification of authentication or control/management messages
- Injection of forged authentication or control/management messages
- Denial of service, including resource starvation
- Disruption of security negotiations
  - Capabilities advertisement
  - Ciphersuite or authentication negotiation

802.11 EAP Method Requirements

- Question: “What role does EAP have in 802.11 security?”
- Wireless method requirements (from RFC 2284bis):
  - Mutual authentication
  - Key derivation
  - Dictionary attack resistance
  - Support for fast reconnect
    - Question: is 2.5 round trips “fast”?
  - Protected EAP conversation
- To be discussed
  - Ciphersuite negotiation?
  - Key activation?

Threats Addressed by EAP Reqmts.

- Snooping, modification or injection of data packets (802.11 ciphers)
- Impersonation of legitimate 802.11 STA or AP (802.11 ciphers)
- Modification of authentication or control/management messages
- Injection of forged authentication or control/management messages
- Denial of service, including resource starvation
- Disruption of security negotiations
  - Capabilities advertisement
  - Ciphersuite or authentication negotiation

No Mandatory Auth Method: Implications

- Interoperability
  - No guarantee that STA and AP can successfully authenticate
- Configurations without a backend server
  - Authenticator can't just implement the mandatory method; needs to support commonly deployed methods
  - Result: AP may need constant code changes to support new auth methods – what EAP was designed to prevent!
  - "Pass through" configuration is easier to implement
- IBSS authentication
  - No guarantee that two STAs can authenticate each other
- Effects on 802.1X architecture
  - Backend authentication server originally an optional component
  - Not really possible to "Colocate AS and AP"
    - In EAP, AS and client are assumed to be extensible but AP is not
  - Normative discussion of AAA attributes and protocols
    - Belongs in a non-normative Appendix, not within the main specification.

Protection of Management Frames

- Protectable
  - Association/Reassociation Request/Response, Deauthenticate, Disassociate
- Unprotectable
  - Beacon, Probe Request/Response
  - Would need to protect Beacon with multicast key; would not prevent forgery
  - Can protect contents of Beacon, Probe Response later on in order to detect forgery
- Handling of unauthenticated management frames
  - STA can discard unauthenticated Deauthenticate message
- Alternatives
  - Custom MIC
    - Requires change to key hierarchy
    - Low performance
  - TKIP/WRAP applied to MPDU
    - No change required to key hierarchy
    - High performance
    - Requires changes to ciphers

Protection of Control Frames

- Similar issues to management frame protection but fewer options
  - Control frames are higher bandwidth
  - Performance penalty of not reusing TKIP and WRAP ciphersuites is prohibitive
  - Custom MIC not a viable option
- Conclusion
  - For control frame protection, need ciphersuites operating on MPDU

Threats Addressed by Mgmt/Cntrl Protection

- Snooping, modification or injection of data packets
- Impersonation of legitimate 802.11 STA or AP
- Modification of authentication or control/management messages
- Injection of forged authentication or control/management messages
- Denial of service, including resource starvation
- Disruption of security negotiations
  - Capabilities advertisement
  - Ciphersuite or authentication negotiation

Protected Negotiations

- Ciphersuite negotiation
  - Ciphersuite negotiation needs to occur before ciphersuites are used
  - If ciphersuite used to protect management messages, then negotiation needs to occur prior to Association/Reassociation Request/Response
  - Alternatives
    - Authenticated Association/Reassociation Request/Response
      - Too late if Assoc/Reassoc protected by TKIP or WRAP ciphersuite
    - 4-way handshake
      - Early in conversation
      - Specific to 802.11
    - EAP
      - Need to create new EAP method to handle thise
      - Requires support for multiple media (PPP, 802.11, etc.)
- Authentication negotiation
  - Handled by EAP protection method

Threats Addressed by Protected Negotiation

- Snooping, modification or injection of data packets
- Impersonation of legitimate 802.11 STA or AP
- Modification of authentication or control/management messages
- Injection of forged authentication or control/management messages
- Denial of service, including resource starvation
- Disruption of security negotiations
  - Capabilities advertisement
  - Ciphersuite or authentication negotiation

Key Activation

- Determines when “FC” WEP bit can be set to true
- Alternatives
  - 4-way handshake
    - Enables “FC” WEP bit to be turned on prior to completion of EAP exchange (e.g. to cover Success/Failure frames
  - Authenticated Association/Reassociation exchange
    - “FC” WEP bit only turned on in “associated” pre-auth
    - EAP protection required
    - Used to activate keys in 802.11-1999

Summary

Threat	*Mitigation alternatives*
Authentication	*802.1X pre-authentication* 802.1X post-authentication
Protected capabilities negotiation	*4-way handshake* EAP Authenticated Association/Reassociation
Key activation	*4-way handshake* Authenticated Association/Reassociation
Management frame authentication	*Ciphers operating over MPDU* Authenticator Information Element
Control frame authentication	*Ciphers operating over MPDU*

Feedback?