IETF/IEEE 802.11i Liason Report

Bernard Aboba
Microsoft
http://www.drizzle.com/~aboba/IEEE

NIST 802.11 Security Workshop
Fairfax, Virginia
December 4-5, 2002

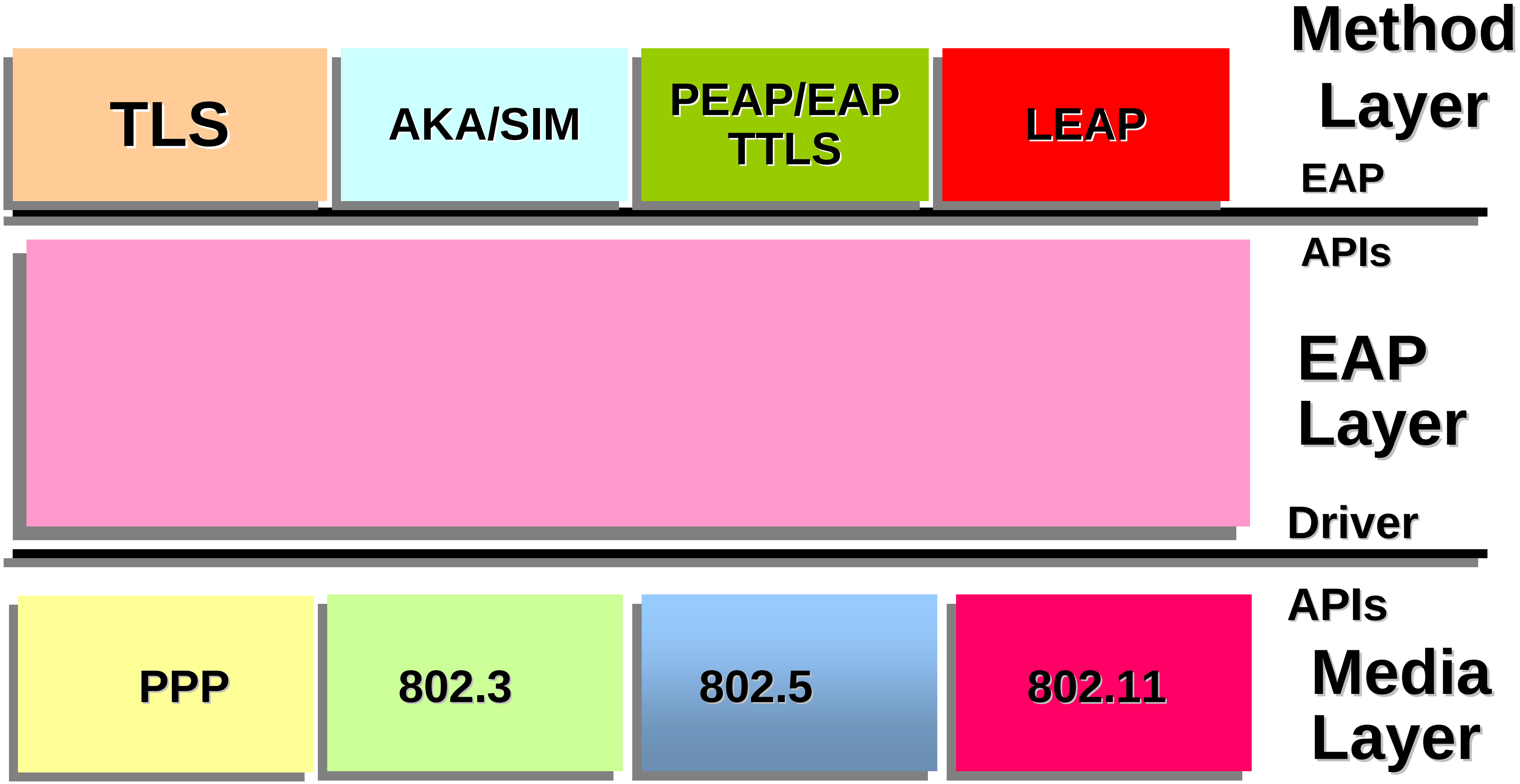
Outline

- Dependencies
- Liason relationships
- Document status
- Timeline
- Roadmap

IEEE 802.11i Dependencies

- IEEE 802.11i security needs to be analyzed as a system
- IEEE 802.11i architecture includes components developed in IETF
- Dependencies:
  - EAP (RFC 2284bis)
  - EAP keying framework
  - EAP methods
  - Authentication, Authorization and Accounting
    - RADIUS (RFC 2869bis)
    - Diameter EAP
- 802.11 Liason letter: http://www.ietf.org/IESG/LIAISON/ieee802.11.txt

EAP Architecture



Method Layer

TLS

AKA/SIM

PEAP/EAP TTLS

LEAP

EAP APIs

EAP Layer

Driver APIs

PPP

802.3

802.5

802.11

Media Layer

Division of Responsibilities

- Encapsulation (IEEE)
  - IEEE 802.1aa defines the encapsulation of EAP on wired media
  - IEEE 802.11i defines the encapsulation of EAP on 802.11 WLANs
- Authentication mechanisms (IETF)
  - RFC 2284 defines no authentication methods of interest to IEEE 802.11i (EAP MD5, OTP, GTC)
  - IEEE 802.11 has requested IETF development of authentication methods relevant to IEEE 802.11i
- State Machines (IETF, IEEE)
  - IEEE 802.1aa defines state machine for wired media
  - IEEE 802.11i defines state machine for WLAN
  - EAP state machine defines operation of EAP protocol
- Key management (IETF, IEEE)
  - IETF defines key management framework
  - IETF develops key management protocols
  - IEEE defines key hierarchy for IEEE 802.11i ciphersuites
- AAA (IETF, IEEE)
  - IETF develops AAA protocols (RADIUS, Diameter)
  - IEEE 802.1aa defines usage guidelines for existing RADIUS attributes
  - IEEE 802.11f defines new IEEE vendor-specific attributes

IETF/IEEE 802.11 Liason Status

- IEEE 802.11
  - Liason letter: http://www.ietf.org/IESG/LIAISON/ieee802.11.txt
  - Dependencies: EAP key framework, AAA keying attributes, EAP methods
  - IEEE 802.11i schedule: completion expected Winter 2003?
- IEEE 802.1aa (IEEE 802.1X revision)
  - Informal liason between IEEE 802.1aa and IETF Bridge and EAP WGs
  - Provides IETF access to IEEE 802.1aa work in progress and cross-publication of MIB and AAA documents
  - IEEE 802.1 TG: Tony Jeffree, Paul Congdon
  - IETF WGs: Les Bell (Bridge WG), Bernard Aboba (AAA, EAP WGs)
  - Dependencies: RFC 2869bis, draft-congdon-radius-8021x, RFC 2284bis, 802.1X MIB
  - IEEE 802.1aa schedule: completion expected Spring 2003
  - Status:
    - EAP WG: http://www.drizzle.com/~aboba/EAP/eapissues.html
    - IETF draft tracker: https://datatracker.ietf.org/public/pidtracker.cgi

IETF/3GPP Liason Status (WLAN Related)

- 3GPP/IETF Liason
  - – Formal liason agreement (RFC 3131)
  - – IESG Liason: Thomas Narten
  - – 3GPP Liason: Stephen Hayes
  - – WLAN Dependencies: Diameter, EAP AKA
  - – 3GPP Milestones & Status: http://www.3gpp.org/TB/Other/IETF.htm
  - – AAA WG Status: http://www.drizzle.com/~aboba/AAA/issues.html

Relevant IETF RFCs

- Proposed Standard
  - RFC 2284 (EAP)
  - RFC 2486 (NAI)
  - RFC 2865 (RADIUS Authentication)
  - RFC 3162 (RADIUS and IPv6)
- Experimental
  - EAP TLS (RFC 2716)
- Informational
  - RFC 2548 (Microsoft RADIUS attributes)
  - RFC 2607 (RADIUS Roaming)
  - RFC 2866 (Accounting)
  - RFC 2867 (Tunnel Accounting)
  - RFC 2868 (Tunnel Authentication)
  - RFC 2869 (RADIUS/EAP)

IETF Working Group Work Items

- Proposed Standard
  - EAP WG (http://www.ietf.org/html.charters/eap-charter.html)
    - RFC 2284bis
      - http://www.drizzle.com/~aboba/EAP/draft-ietf-pppext-rfc2284bis-08.txt
  - AAA WG (http://www.ietf.org/html.charters/aaa-charter.html)
    - Base: http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-15.txt (IESG Review)
    - Transport: http://www.ietf.org/internet-drafts/draft-ietf-aaa-transport-08.txt (IESG Review)
    - NASREQ: http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-10.txt (AAA WG last call)
    - MIP: http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-mobileip-13.txt (IESG Review)
    - EAP: http://www.ietf.org/internet-drafts/draft-ietf-aaa-eap-00.txt
    - CMS: http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-cms-sec-04.txt
  - PKIX WG
    - WLAN Certificate extensions
      - http://www.ietf.org/internet-drafts/draft-ietf-pkix-wlan-extns-02.txt

Individual Submissions

- IEEE 802.1aa dependencies
  - RFC 2869bis: Draft-aboba-radius-rfc2869bis
  - IEEE 802.1aa Appendix D: Draft-congdon-radius-8021x
- EAP Keying Framework
  - Draft-aboba-pppext-key-problem-03.txt
- EAP methods
  - EAP SIM
  - EAP AKA
  - EAP SRP
  - EAP GSS
  - PEAP
  - EAP TTLS
  - EAP MAKE
- EAP extensions
  - EAP TLV
    - Acknowledged & protected success/failure
    - Language negotiation
    - Cryptographic binding
    - Ciphersuite negotiation
    - MIPv6/802.11 fast handoff
- References:
  - http://www.drizzle.com/~aboba/IEEE/

Security Claims Plan

- Goal: Enable customers to evaluate claims against security requirements
- Plan
  - Define security claims in RFC 2284bis-08 (and in IEEE 802.11i?)
  - EAP method specifications to detail security claims in Security Considerations and provide proof
- Gotchas
  - Method specifications with invalid claims
  - Methods with non-published algorithms (EAP SIM)
  - Methods which enable multiple algorithms to be selected (EAP GSS)
  - Methods with undisclosed encumberence (EAP SRP)

Security Claims

Mechanism
Target Media
Mutual auth
Dictionary attack resistance
Key derivation
Key Strength
MiTM vulnerability
Fast reconnect
IPR Status
Protection

- Method negotiation
- Ciphersuite negotiation
- Success/Failure indication
- Identity hiding
- Method data
- EAP header

EAP WG Timeline

- RFC 2284bis: 1Q03
  - RFC 2284bis-08 strawman available now
- RFC 2869bis: 1Q03
- EAP State machine: 2Q03
- EAP keying framework: 2Q03
- Revised Liason letters from 3GPP and IEEE 802.11: ASAP
- Not in EAP WG charter
  - EAP method solicitation and evaluation
  - EAP “extensions”

AAA WG Timeline

- Diameter “first wave”: 1Q03
  - Base
  - Transport
  - MIPv4
  - NASREQ
- Diameter “second wave”: 1Q04
  - EAP
  - CMS
- Not in AAA WG charter
  - Credit control
  - Multimedia
  - MIPv6/AAA

Roadmap Issues

- EAP Method requirements
  - Influenced by IEEE 802.11, 3GPP Liason process
    - Scenarios
    - Requirements
  - Updated liason letters forthcoming?
  - Requirements document needed?
- EAP method solicitation and evaluation (TBD)
  - Audience
  - Format
  - Schedule
  - Judges
  - Suggestions based on NIST experience?
- EAP Extensions
  - Are they needed? If so, which ones?
  - How to avoid “kitchen sink syndrome”?

Feedback?