EAP and AAA Update

Bernard Aboba
Microsoft
http://www.drizzle.com/~aboba/IEEE
NIST 802.11 Security Workshop
Fairfax, Virginia
December 4-5, 2002

Outline

- EAP
  - Secrets of RFC 2284
  - EAP methods: taking inventory
- AAA
  - Secrets of RFCs 2548, 2685-2689, 3162
  - AAA: taking inventory

Secrets of RFC 2284

- IEEE 802.1X state machine is not the EAP state machine
- EAP is a peer-to-peer protocol
- Identity is optional
- “Pass through” is optional
- EAP can be terminated on the AP
- EAP assumes a mandatory to implement method

IEEE 802.1X State Machine is Not the EAP State Machine

- Why?
  - IEEE 802.1X “authenticated” state does not imply that the Supplicant has successfully authenticated the Authenticator
    - If EAP mutual auth has not completed successfully, “authenticated” state could be reached via Success spoofing (University of Maryland)
- How to avoid being bitten
  - Check whether EAP method has returned “Success” to EAP layer prior to accepting unprotected Success indications (RFC 2284 bis)
  - Implement EAP state machine, above 802.1X/aa state machine
  - Understand the EAP/802.1aa/802.11 interlock
    - It’s different for pre-authentication and post-authentication!

EAP is a Peer to Peer Protocol

- Why?
  - PPP is a Peer to Peer protocol!
- Authentication can occur in one direction… then reverse!
  - So a “Supplicant”/Peer can request reversal, by sending an EAP Request to an “Authenticator”.
- Bad assumptions
  - STA == “Supplicant”, AP == “Authenticator”
- When bad assumptions will bite you
  - Adhoc
  - Device-Device authentication
- How to avoid being bitten
  - Implement both Supplicant and Authenticator, at least for adhoc operation

Identity is Optional

- Why?
  - It says so in RFC 2284!
- But, but…
  - IEEE 802.1X says Identity Request is always the first packet sent!
    - Uh, not necessarily: read IEEE 802.1aa D4!
    - Access Point can send another EAP Request as the first packet, can be set via MIB variable
    - Example: AP could send EAP TLS-Start as first packet
  - How can you *not* send an Identity Request first?
    - When you know what method you want to use
    - When you desire Identity Protection
    - When Identity is determined by other means: MAC Address, etc.
    - When authentication terminates on the AP/NAS
- When bad assumptions will bite you
  - When authenticating via certificates without AAA
- How to avoid being bitten
  - Implement IEEE 802.1aa state machine and revised MIB

Pass Through is Optional

- Why?
  - It says so in RFC 2284… and IEEE 802.1X
- But, but…
  - How can EAP work without pass through?
    - If the AP implements a mandatory to implement method
    - If the mandatory to implement method is negotiated
    - If the AP can authenticate locally without “pass through”
    - Example: EAP TLS (RFC 2716)
  - Isn’t pass through all or nothing?
    - Who says?
    - AP can authenticate local users via some methods (e.g. mandatory to implement) and pass through other methods and users
    - Ascend terminal servers did this (not with EAP) back in 1994

EAP Can Be Terminated on the AP

- First discussed in ROAMOPS WG in 1997
  - "Certificated-Based Roaming", http://www.drizzle.com/~aboba/IEEE/
- Scenario
  - STA has a STA cert chaining to trusted root
  - AP has an AP cert chaining to trusted root
  - Authentication occurs via EAP TLS (RFC 2716) or equivalent
- AAA
  - No authentication/authorization required (if STA cert provides implicit authorization)
  - No key transport from AAA server to AP
  - Can do accounting only, if the billed party is ok with that
- Handoff
  - Don't want to do full TLS handshake on every roam
  - APs need to do "pre-emptive handoff" (U of Maryland)
  - STA does "session resume" on roam
- Computational requirements
  - Modest, assuming pre-emptive handoff and session continuation

EAP Assumes A Mandatory to Implement Method

- Why?
  - RFC 2284 has a mandatory to implement method: EAP MD5
  - Without a mandatory to implement method, interoperability cannot be guaranteed
  - Without a mandatory to implement method, the security of IEEE 802.11i cannot be analyzed
  - Existence of a mandatory to implement method enables optional identity, optional pass through, etc.
- But, but…
  - EAP MD5 isn’t useful for IEEE 802.11i
  - We couldn’t agree on a mandatory method
  - My AP has {too little CPU, NVRAM, etc.} to implement a mandatory method

EAP Method Inventory

Allocated EAP Type#’s

Type	Description	Reference	Implemented?	Spec Available?
1	Identity	[RFC2284]	Yes	RFC 2284
2	Notification	[RFC2284]	Yes	RFC 2284
3	NAK (Response only)	[RFC2284]	Yes	RFC 2284
4	MD5-Challenge	[RFC2284]	Yes	RFC 2284
5	One Time Password (OTP)	[RFC2284]	No	RFC 2284
6	Generic Token Card	[RFC2284]	No	RFC 2284
7			No	No
8			No	No
9	RSA Public Key Authentication	[Whelan]	No	Expired
10	DSS Unilateral	[Nace]	Yes	I-D?
11	KEA	[Nace]	Yes	I-D?
12	KEA-Validate	[Nace]	Yes	I-D?
13	EAP-TLS	[Aboba]	Yes	RFC 2716
14	Defender Token (AXENT)	[Roselli]	Yes	No
15	Windows 2000 EAP	[Asnes]	?	No
16	Arcot Systems EAP	[Jerdonek]	?	No
17	EAP-Cisco Wireless	[Norman]	Yes	No
18	Nokia IP smart card auth	[Haverinen]	?	No
19	SRP-SHA1 Part 1	[Carlson]	Yes	I-D
20	SRP-SHA1 Part 2	[Carlson]	No	I-D
21	EAP-TTLS	[Funk]	Yes	I-D
22	Remote Access Service	[Fields]	?	No
23	UMTS Auth and Key agreement	[Haverinen]	?	?
24	EAP-3Com Wireless	[Young]	Yes	No
25	PEAP	[Palekar]	Yes	I-D
26	MS-EAP-Authentication	[Palekar]	Yes	No
27	Mutual auth w/key exchange (MAKE)	[Berrendonner]	?	No
28	CRYPTOCard	[Webb]	Yes	No
29	EAP-MSCHAP-V2	[Potter]	?	I-D
30	DynamID	[Merlin]	?	No
•	Rob EAP	[Ullah]	?	No
•	SecurID EAP	[Josefsson]	Yes	I-D
•	EAP TLV	[Palekar]	Yes	I-D
•	SentriNet	[Kelleher]	Yes	No
•	Actiontec Wireless	[Chang]	?	No
•	Congent Systems Biometric	[Xiong]	?	No

Some Observations

- Rate of Method Type allocation is increasing
  - 36 Type values allocated since March 1998
  - 4 Type values allocated in the last 3 months
  - Serious problems possible in 4-5 years
- Two Method Type values allocated to the same Method
  - EAP SRP-SHA1 Parts 1 and 2
  - Two EAP MS-CHAPv2 (don’t ask)
- Most allocations are for vendor-specific use with no specification
- Not all allocated Method Types are used
  - At least 5 of the allocated types have not been implemented (~15 percent!)

EAP Methods: Taking Inventory

- Certificate authentication
  - EAP TLS
  - EAP IKE (expired)
- Cellular authentication (3G)
  - EAP SIM (IPR statement)
    - http://www.ietf.org/ietf/IPR/NOKIA-draft-haverinen-pppext-eap-sim.txt
  - EAP AKA
- Password-based methods
  - EAP MS-CHAPv2 (two variants, don't ask…)
  - EAP SRP (multiple IPR statements)
    - Soon to be a major motion picture:
      - http://www1.ietf.org/mail-archive/working-groups/ipr-wg/current/msg00249.html
    - http://www.ietf.org/ietf/IPR/LUCENT-SRP
    - http://www.ietf.org/ietf/IPR/WU-SR P
    - http://www.ietf.org/ietf/IPR/PHOENIX-SRP-RFC2945.txt

EAP Methods: (cont'd)

- Legacy
  - "Legacy" methods (one-way auth without key derivation)
    - EAP MD5
    - One Time Password (OTP)
    - Generic Token Card (GTC)
    - EAP RSA Public Key Authentication (IPR statement)
      - http://www.ietf.org/ietf/IPR/pppext-eaprsa
  - Hardware token cards
    - EAP SECURID
    - AXENT Defender token
    - Many, many more...
  - Tunneling protocols
    - EAP TTLS
    - PEAP (IPR statement)
      - http://www.ietf.org/ietf/IPR/MICROSOFT-PEAP.txt

Where Are We?

- IETF understands certificate authentication
  - IKE: Identity protection, DH key exchange, etc.
  - TLS: Identity protection (not by default), DH as an option, etc.
- Pre-shared key authentication needs work
  - IKE Main Mode
    - Identity protection, DH key generation, but… pre-shared key tied to IP address
    - Dynamic IP addresses require group pre-shared keys??
    - 802.11: Not a good idea to tie MAC address to pre-shared key
  - IKE Aggressive Mode
    - DH key generation, pre-shared key tied to ID payload
    - No identity protection?
    - Some folks (Europeans) really want Identity protection
  - IKEv2: XAUTH, PIC, CRACK, HYBRID…
    - A petri-dish for vulnerabilities, including man-in-the-middle attacks
    - “Thou Shalt Not Touch the IKE” – Steve Bellovin
- Password based auth is an IPR minefield
  - SRP: Repeat after me: “I’m not a lawyer…”
  - EKE patents don’t expire for a long while
  - Tunneling methods have their own set of issues (Russ will discuss)
  - But there may be “rough equivalents”… (e.g. SSH)

What We Need

- More thought
- More unencumbered algorithms
- More attention to pre-shared keys and passwords
  - Handling them badly doesn’t make them go away
- More attention to certificate profiles and provisioning
  - http://www.drizzle.com/~aboba/CPW/

Secrets of RFC 2865-2869, 3162

- RADIUS can run over IPsec
- Vulnerabilities
  - PAP: Pandora's Authentication Protocol
  - RADIUS accounting is not confidential
  - RFC 2548 key wrap can be improved
  - See http://www.drizzle.com/~aboba/IEEE for links to RADIUS security analyses

RADIUS Can Run Over IPsec

- RADIUS over IPsec described in:
  - RADIUS over IPv6 (RFC 3162)
  - Draft-chiba-radius-dynamic-authorization-05.txt
- Benefits
  - Replay protection
  - Confidentiality
  - Additional flexibility in configuration (IDs instead of IP addresses)
  - Credible ciphers: no more “hiding” algorithms, just 3DES, AES, etc.
- How would it work?
  - IKE MM with pre-shared key: AP w/static address
  - IKE AM with pre-shared key: AP w/dynamic address
  - IKE MM with certs: AP w/dynamic address, built-in cert or enrollment protocol support
    - Caveat: hard to do per-application certificate policies with IKE

Can RADIUS/IPsec Be Implemented?

- Footprint isn’t too bad
  - IKE w/pre-shared keys (no certs) can be as small as 200 KB footprint
  - IKE, 3DES, IPsec has been implemented on iSCSI HBAs at modest prices (running at 1 Gbps line rate!)
- CPU consumption isn’t too bad
  - Average session time of 10 minutes = 6 sessions/hour/”port”
  - 100 simultaneous users at peak: 600 sessions/hour
  - Assume 6KB/RADIUS traffic/session
  - RADIUS traffic: 3600 KB/hour = 1000 bytes/second
  - 3DES (140 cycles/byte) * 1000 bytes/second = 140,000 cycles/second

Pandora's Authentication Protocol (PAP)

- Isn't PAP unsupported in EAP?
  - We didn't allocate a Type to it, shouted down people who wanted it, and then…
  - Oh no! It's supported within EAP TTLS!
- If I don't use EAP TTLS, does this affect me?
  - Yes, if a NAS doing PAP has the same RADIUS shared secret as an 802.11 AP
- What can happen if I use PAP with promiscuous RADIUS shared secrets?
  - PAP passwords are "hidden" with a stream cipher derived from the RADIUS shared secret + the Request Authenticator (128 bits)
  - Opens RADIUS up to "known plaintext attack"
  - Request authentication should be "temporally and globally unique" in RFC 2865, but…
  - RADIUS clients often call RAND(), may have low boot entropy…
  - RADIUS servers don't check for RA repetition
  - Sound familiar? Welcome to WEPville…

RADIUS Accounting Is Not Confidential

- RADIUS accounting packets are integrity protected and authenticated, not confidential
  - 802.11 user's location can be determined by snooping the wire between AP and RADIUS accounting server
  - NAS-IP-Address, NAS-Identifier, User-Name attributes allow an attacker to determine user location in real time
- In RFC 2866, Request and Response Authenticator fields are both MICs
  - No nonce in the RA
- No source of "liveness"…
  - Except the RADIUS "Session-ID" attribute
  - Which is checked by the backend billing server, *not* the RADIUS accounting server
  - Billing server check needed due to failover

RFC 2548 Key Wrap Could Be Better

- Uses MD5 for “hiding” the MPPE-Key attributes, just like RFC 2865
  - Why not HMAC-SHA1?
- “Salt” was added to protect against known plaintext attack, but…
  - It was put at the end!
  - If MD5 keystream is compromised via PAP “known plaintext” then Salt (sent in the clear) can be used to continue the keystream,
  - Result: 802.11i key is compromised too.
- Need a standardized “key wrap” algorithm

AAA: Taking Inventory

- RADIUS
  - Supports EAP: RFC 2869bis, draft-congdon-radius-8021x-20.txt
  - Widespread commercial support, demonstrated interoperability
  - Server initiated messages
    - Draft-chiba-radius-dyamic-authorization-05.txt
  - New applications via new “NAS-Port-Type”
  - Hop-by-hop security
    - RADIUS: integrity protection and authentication
    - IPsec: replay protection, integrity, authentication and confidentiality
  - Object security
    - Kerberos attribute protection
    - Needed for roaming w/untrusted proxies (see RFC 2607)
  - Accounting
    - Unreliable: UDP w/no defined retransmission or failover behavior
    - Replay protection in the billing server

AAA: Taking Inventory (cont'd)

- Diameter
  - Supports EAP: draft-ietf-aaa-eap-00.txt
  - No 802.1X support yet
  - Some limited interop testing, APIs, open source implementation in progress
  - Server initiated messages
  - New applications via new "Diameter Application"
  - Transmission-layer security
    - TLS or IPsec: we couldn't make up our minds?
  - Object security
    - CMS Security Application (not rev'd since IETF 53)
  - Accounting
    - Reliable: TCP/SCTP w/standardized retransmission, failover and load balancing
    - Replay protection built into the protocol, two different ways!

Where Are We?

- Poor understanding of proper RADIUS “hygene”
  - Use of RAND() vs. cryptographic random number generation of Request Authenticators
  - PAP support in EAP TTLS: say it ain’t so!
  - Shared secret reuse
- Proprietary keying attributes commonly used despite known flaws
- Vendor community not embracing RADIUS over IPsec

What We Need

- PAP back in the box
- An RFC on RADIUS security practices
- RADIUS over IPsec deployment
- Standard RADIUS keying attributes
- Diameter as a viable AAA protocol (long term)
  - Prerequisites:
    - Multiple interoperable implementations
    - CMS object security
    - EAP application
    - Support for draft-congdon-radius-802x

Feedback?