EMU BOF

EAP-TLS Experiment Report

RFC 2716

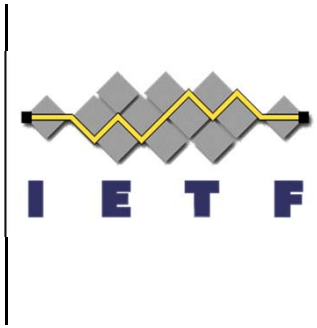
Bernard Aboba

Microsoft

Thursday, November 10, 2005

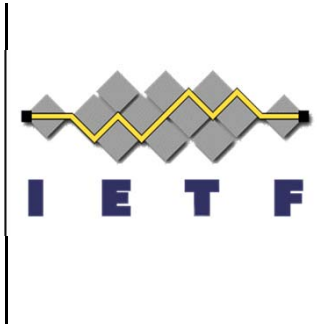
IETF 64, Vancouver, CA

History of RFC 2716



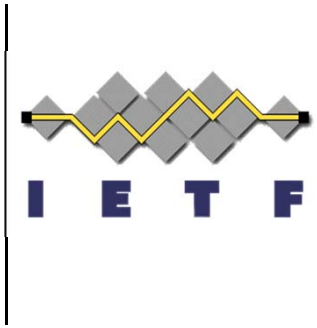
- Goal: support for certificate-based mutual authentication within EAP over PPP
- -00 draft submitted to PPPEXT WG in October 1997
- http://www.watersprings.org/pub/id/draft-ietf-pppext-eaptls-00.txt
- Experimental RFC published in October 1999
- Why Experimental?
  - No previous EAP method had supported mutual authentication or key derivation
  - Few existing certificate or smartcard deployments

Basics of EAP-TLS



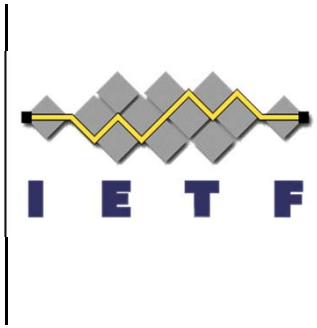
- EAP Type Code 13
- Server certificate REQUIRED (Section 3.1)
  - “If the EAP server is not resuming a previously established session, then it MUST include a TLS server_certificate handshake message, and a server_hello_done handshake message MUST be the last handshake message encapsulated in this EAP-Request packet.”
- Client certificate RECOMMENDED (Section 3.1)
  - “The certificate_request message is included when the server desires the client to authenticate itself via public key. While the EAP server SHOULD require client authentication, this is not a requirement, since it may be possible that the server will require that the peer authenticate via some other means... If the EAP server sent a certificate_request message in the preceding EAP-Request packet, then the peer MUST send, in addition, certificate and certificate_verify handshake messages.”
  - Client authentication can be postponed until later to enable privacy support

Subsequent Events



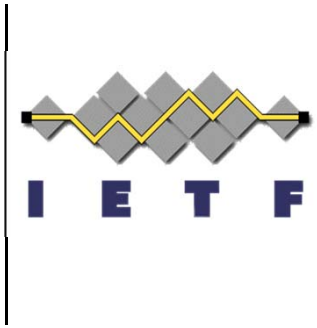
- EAP evolution
  - Expanded lower layer support (RFC 3748)
    - IEEE 802: IEEE 802.1X, IEEE 802.11i, IEEE 802.16e
    - VPNs: PPTP, L2TP, IKEv2
- Improvements in certificate/smartcard support
- Regulatory mandates
  - FIPS 140-2
  - HIPAA

Evaluating the EAP-TLS Experiment



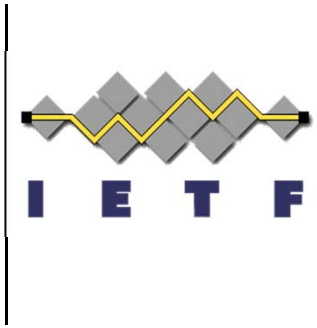
- Security analyses
- Implementations
- Certification programs
- Deployments

Security Analyses



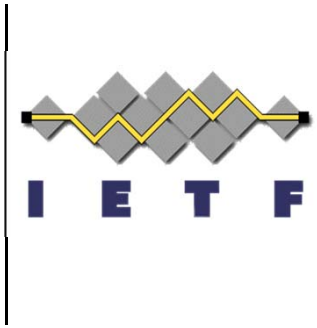
- Arbaugh & Mishra (2002)
  - http://www.cs.umd.edu/~waa/1x.pdf
  - Found issues in EAP state machine that could lead to bypass of EAP-TLS server authentication
  - Issues fixed in RFC 3748 & 4137
- He, Sundararajan, Datta, Derek & Mitchell
  - “A Modular Correctness Proof of IEEE 802.11i and TLS”
    - Proof of security of EAP-TLS stand-alone and when used with IEEE 802.11i

EAP-TLS Implementations



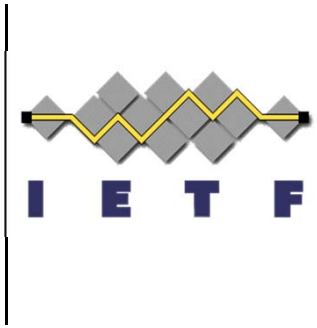
- Peer
  - Windows 2000, XP, CE
  - XSupplicant
  - Meetinghouse AEGIS
  - Funk Odyssey
  - Cisco ACU
  - Devicescape
  - Wire1X
- Server
  - Windows 2000, Windows 2003 Server
  - pppd
  - FreeRADIUS
  - OpenRADIUS
  - RADIATOR
  - Cisco ACS
  - Funk Odyssey, Steel-Belted RADIUS
  - Meetinghouse AEGIS
  - Interlink
- Toolkits
  - Matrix SSL
  - Certicom
- Decode/debug
  - Ethereal
  - Netmon
- Test Suites
  - Qacafe

Certification Programs



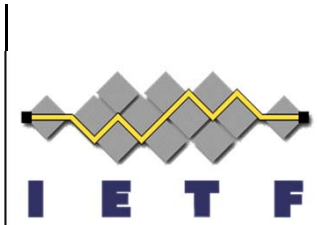
- WFA EAP Certification program
  - EAP-TLS interoperability testing included within WPA certification program, April 2003
  - Expanded EAP certification program launched in April 2005
  - http://www.wi-fi.org/membersonly/getfile.asp?f=WFA_Security_Ext_EAP_04_12_05_overview_media.pd
- FIPS 140-2 compliance
  - FIPS compliant EAP-TLS implementations now shipping
    - Restriction on allowable ciphersuites, key strength, etc.
- Vendor certification programs
  - Thousands of engineers trained in installing, debugging, maintaining EAP-TLS

Deployments



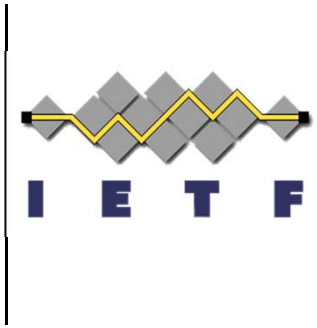
- Surveys indicate that ~10% of all EAP deployments are using EAP-TLS
  - Among customers who have deployed certificates, EAP-TLS usage is much higher
- Popular in security conscious environments
  - Government/military
  - Financial institutions
  - Medical
  - Engineering
- Regulatory mandates play an important role
  - FIPS 140-2
  - HIPAA
- Customers frequently deploy smartcards along with EAP-TLS

Summary



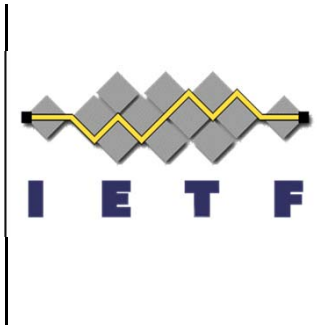
- EAP-TLS has been widely implemented and deployed.
- EAP-TLS interoperability has been demonstrated in multiple distinct implementations.
- EAP-TLS certification and testing programs are in place.
- Recommendation: The experiment has been a success.

Possible Next Steps



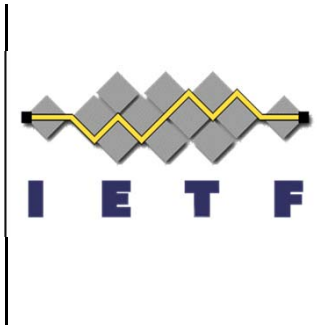
- Document the existing protocol in a Draft Standard
- “Improve” the protocol in a Proposed Standard

Draft Standard Approach



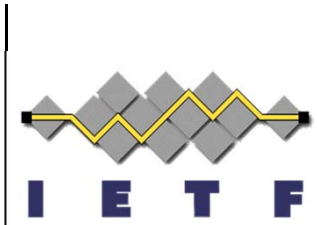
- Leverage WFA certification testing
  - Identify interoperability problems and clarify specification
  - Remove features that have not been shown to interoperate in two distinct implementations
  - No feature additions beyond what is in RFC 2716
- Issue RFC2716bis as Proposed Standard
- Move document to Draft Standard ASAP with minimal changes

Proposed Standard Approach



- Add features that would be “nice to have”
- Required work
  - Redo the “proof of security”
  - Revise test suites
  - Upgrade certification programs
  - Rewrite documentation, deployment guides
  - Revise implementations
  - Collect interoperability data on revised implementations
- Problems
  - Unlikely the above work will actually get done
  - Possible introduction of security vulnerabilities and interoperability issues
  - Potential for IPR disclosures encumbering the revised protocol
  - Existing implementations unlikely to upgrade
  - Possible disruption of pending deployments
  - “Nice to have” features may not supported within certification programs

Recommendation



- Draft Standard approach preferred
  - EAP-TLS is a mature, stable protocol
    - 6 years since publication of RFC 2716
    - Many distinct, interoperable implementations
    - Proof of security available
  - Stability more important than new features at this point
    - Major deployments in progress
    - Costs of protocol revision outweigh the benefits
    - New features, if needed, can be introduced in a new EAP method

Feedback?