EAP Method Update (EMU)

IETF 67- San Diego
November 6, 2006

Joe Salowey
(jsalowey@cisco.com)

Agenda

- Administrative
  - Note takers, blue sheets, agenda, documents
- RFC2716bis (EAP-TLS)
  - Bernard Aboba
- GPSK
  - Charles Clancy, Hannes Tschofenig
- Password Based Mechanism
  - Charles Clancy, Joe Salowey
- Enhanced EAP-TLS
  - Joe Salowey

Current WG Drafts

- EAP-TLS
  - draft-simon-emu-rfc2716bis-04.txt
  - Close to ready for WG last call
- GPSK
  - draft-ietf-emu-eap-gpsk-00.txt

Enhanced TLS Based Mechanism

- “Enhanced functionality to enable a TLS-based EAP method to support authentication methods beyond certificates, channel bindings and other optional functions required in RFC 4017. So as to enable RFC 2716bis to focus solely on clarifications to the existing protocol, this effort will be handled in a separate document. Depending on an analysis of the behavior of existing implementations, it is possible that this effort may be able to use the existing EAP-TLS type code, or it may need to be handled via assignment of a new EAP Type Code.”

Enhanced TLS

- New Type Code (and Name)
  - Perhaps one for each ciphersuite class
- Channel Binding
- Protected Result Indications
- How?
  - TLS Extension?
  - Tunneling?

Password Based Mechanism

- “A mechanism meeting RFC 3748 and RFC 4017 requirements that makes use of existing password databases such as AAA databases. The implementation should strive to be usable in resource constrained environments.”
- Forming design team
  - Message sent to EMU list