Implementation Challenges of Channel Binding

Sam Hartman
IETF 83

Goal

- Implement draft-ietf-emu-chbind for TTLS
- Peer: EAP library from WPA Supplicant
- EAP Server: Freeradius 3.x

Protocol for TTLS

- TTLS carries AVPs from the Diameter namespace
- Channel binding requires an AVP in the tunnel for request and response
- So, pick a diameter AVP, right?

Diameter meets RADIUS

- A lot of people use RADIUS-based EAP servers even for TTLS.
- RADIUS servers don't know what to do with diameter AVP.
- So, they throw away the entire access request

Trying a RADIUS VSA

- If we use a RADIUS VSA to carry the channel binding AVP, we can represent that in Diameter.
- RADIUS servers should understand VSAs.
- Sadly, unknown VSAs inside TTLS apparently also cause discards.
- Squat on a standard RADIUS AVP?

The Joys of Success

- EAP Success is so simple.
- EAP servers are delighted to send it at the first signs things go well—fewer round trips!
- But wait, I wanted to finish off channel binding.

To Take Away

- Implementation challenges will add significant constraints to how channel binding is added to existing methods.
- Secure negotiation is even harder.

Acknowledgments

- Kevin Wasserman
- Margaret Wasserman
- Alan DeKok