Some Additional Capabilities for Extensible Tunneled Authentication

Dan Harkins

Certificate-less Password Auth

- Server-side certificate authentication may not always be possible
  - The little checkbox is there for a reason, and it is used!
  - When it's not we don't want to use PAP!
- Use tunnel method:
  - Phase 1 is a TLS ciphersuite for anonymous D-H.
  - Phase 2 is an EAP method that supports mutual authentication using a password that is resistant to dictionary attack– EAP-pwd or EAP-EKE.
- Why not just use the phase 2 EAP method by itself (outside the tunneled method)?
  - Tunneled method has channel bindings and a way to pass arbitrary stuff back and forth between client and authenticator. These EAP methods don't.

Provisioning another Credential

- Tunnel method has the concept of a PAC for subsequent fast(er) authentication
  - How does one get this PAC?
  - Ask for one after going through the whole tunnel method the first time (see previous slide).
- If I only had a cert… (I'd do EAP-TLS)
  - Authenticate, even if there's no trusted root or path for validation (see previous slide).
  - Issue PKCS#10-ish request, get PCKS#7-ish response.
  - Et voilà!