EAP-EKE Update
draft-sheffer-emu-eap-eke

Scott Fluhrer, Yaron Sheffer, Hannes Tschofenig, Glen Zorn
IETF-75, Stockholm
EKE: Reminder

- EKE = Encrypted Key Exchange
  - Bellovin and Merritt 1992
- The first strong password authentication protocol
  - Memorizable (=short) passwords
  - Trust requires *only* the password, e.g. no certificates
  - Resists online and offline dictionary attacks
- US patent due to expire late 2011
- Several variants in the original paper
  - The one we use is not formally proven, but believed secure
The Protocol

**Server**

ID, crypto proposal →

E(Password, $g^{xa}$) →

Prot(K, Challenge$_a$ || Challenge$_b$), Auth →

**Peer**

← ID, crypto selection

← E(Password, $g^{xb}$), Prot(K, Challenge$_b$)

← Prot(K, Challenge$_a$), Auth

Where K is the D-H shared secret, $g^{xa \cdot xb} \mod p$
Implementation

- A team of students from Tel Aviv University added EAP-EKE to FreeRADIUS and wpa_supplicant

- Another team is adding it to StrongSwan (IKEv2)
Changes in -02

- Minor tweaks following the implementation
- Added integrity protection to encrypted nonce payloads
  - Original paper mentions integrity protection to counter “cut-and-paste” attacks
- Added an “extraction step” per HKDF
  - draft-krawczyk-hkdf-00
- Eliminated protected failures
Thank You!