Password Authenticated Key Exchange Selection Criteria

draft-sheffer-ipsecme-pake-criteria-01

Yaron Sheffer, IETF-77

Introduction

- Password auth is a new IKEv2 mode, just like certificate- or PSK-authentication

- We will talk about the criteria, not how they apply to any specific solution alternatives

- Security criteria
- IPR criteria
- Other criteria

Lots of Options

- SPSK
- EKE
- SPEKE
- SPAKE (no kidding)
- SRP
- AugPAKE

- And many more…

- We will not go into any particular one here

Security Criteria

- Good security "best practices"
  - Crypto agility
- Protocol has been known/analyzed for some time, available to researchers
- Thorough professional analysis
  - Preferably published
  - Of the latest protocol version
- Proven security is a very nice property

- More important than all other criteria
  - High impact if a vulnerability is discovered late

IPR Criteria

- IANAL
- IETF does have a lawyer, but…

- Unencumbered is best
  - But very hard to prove
  - This is each participant's responsibility
  - Spurious IPR statements
- Rare cases where the IPR situation is clear
- Freely licensed technology

- Compromise here?

Other Criteria

- Specification (e.g. in standards) as opposed to description in an academic paper
- Existing integration with IKE
- Sharing of algorithms and DH groups with IKE
- Performance (round trips, exponentiations)
- Future scalability: elliptic curves
- Implementation simplicity (FWIW)