Updates to the GSAKMP Spec.

Presented by
Hugh Harney

SPARTA, Inc.
(410) 872-1515 x203
hh@sparta.com

GSAKMP Software: http://www.isso.sparta.com/gsakmp

Agenda

- Security Considerations
- Cookies

Security Considerations

- Assumtions
  - Operating System good
  - Software Assurance
  - Good key generation
  - Random Randoms
- Diffie-Hellman = IKEv2
- Reliance on other Protocols
  - We rely on none
    - We stole from them, with attribution
      - » ISAKMP structure
      - » IKE nonces
- DoS (Cookies only offer some help)
- Trust Heirarchy = full security policy specification

Cookie Ladder Diagram