

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

- Assumptions
 - 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 Hierarchy = full security policy specification

Cookie Ladder Diagram

Cookies CONTROLLER	MESSAGE	MEMBER
in Cookie Mode		
	!<--Request to Join without Cookie Info---!	
<Gen Cookie Rsp> !	!	
	!-----Cookie Download----->!	
	!	! <Process CD>
	!<----Request to Join with Cookie Info----!	
<Process RTJ> !	!	
	!-----Key Download----->!	
	!	! <Process KD>
	!<-----Notification - Ack/Failure-----!	
<Process Notif> !	!	
	!<=====SHARED KEYED GROUP SESSION=====>!	