

IPsec and Application Security

Sam Hartman

Massachusetts Institute of Technology

IETF 66

July 11, 2006

Application Security using IPsec

- Goals of IPsec
- Goals of Applications
- Challenges to Application Security

Goals of IPsec

- Provide system security solution.
- Single security policy
- Both endpoints must agree to bypass or protect traffic.

Goals of Application Security

- Easy configuration based on knowledge of what the application does.
- Different endpoints may have different policies: one requires confidentiality while one supports it
- Mobility, NAT

Challenges to Application security with IPsec

- Selecting Traffic
- Protection barrier and SPD selection functions
- Optionally protecting traffic
- Getting information about peers to the application