LIPKEY Update

45th IETF, CAT-WG

Mike Eisler
mre@Eng.Sun.Com

July 11, 1999

Perceptions of Value of LIPKEY to General IETF Community

Is the value limited to existing applications that use GSS-API?

❑ LIPKEY is being pitched as a solution to the NFS V4-WG

❑ FTP is a potential candidate

❑ Others?

Interest in extending LIPKEY to span SSKM?

- Is this meaningful?
  - The intent of LIPKEY is work over any existing password schemes
  - SSKM assumes target knows the client’s password, whereas LIPKEY, assumes the target knows how to verify the client’s password.

Other changes for consideration

- Changes so far (from draft-ietf-cat-lipkey-00 to -01)
  - Added SPKM-3 to allow secure channel without prior knowledge of target certificate
  - Anonymous LIPKEY initiator support
- Changes planned
  - OID assignments for SPKM-3 and NULL-MAC I-ALG
  - unencumbered signature algorithm
- Changes to consider
  - stronger integrity algorithm than DES-MAC
  - others?