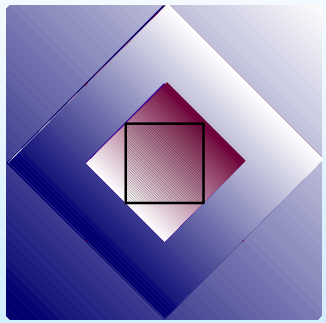
iSCSI Security Issues

IPS IETF-50 meeting
Mar 19 2001

Ofer Biran
Julian Satran

IBM Research Lab in Haifa

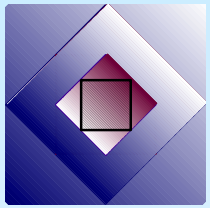


03 – 05 draft changes

- Security MUST / MAY (next page...)
- AuthMethod instead InitAuth TargetAuth (mutual - AuthMethod specific).
- Auth - KRB5, SRP, (proprietary)
  Digests – CRC_, KRB5_ (GSS_getMIC)
- Detailed negotiation examples.

Security MUST / MAY for Implementation

- MUST provide means of authentication and data integrity.
- MAY provide means of data privacy.
- Both can be satisfied by using IPSEC.
  IPSEC – orthogonal to the iSCSI standard.

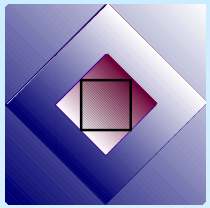


Security Open Issues

- Additional authentication methods
  (KRB5, SRP,... PublicKey , RADIUS)

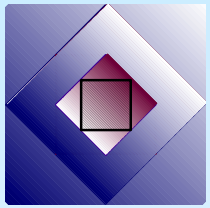
- Make one mandatory ? (e.g., in TLS `TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA` is mandatory)

- SRP digest (based on 320 bits shared key)



*Additional authentication methods (KRB5, SRP,...**PublicKey**)*

- Based on RFC-2025 “`The Simple Public-Key GSS-API Mechanism (SPKM)`”
- SPKM-1 (random challenge), SPKM-2 (timestamp)
- `SPKM-REQ` gss_init_sec_context()
  `SPKM-REP-TI` gss_accept_sec_context()
  `SPKM-REP-IT` gss_init_sec_context()
- Digest by GSS_GetMIC() similar to KRB5 (here: `md5WithRSA`,`DES-MAC`,`md5-DES-CBC`)



*Additional authentication methods (KRB5, SRP,...**RADIUS**)*

- Password based challenge / response used in PPP CHAP.
- RADIUS compatible, so the authenticator can compose query for RADIUS server.