Mandatory iSCSI Security

review of the potential methods

IPS Interim Meeting
Nashua NH, May 01 2001

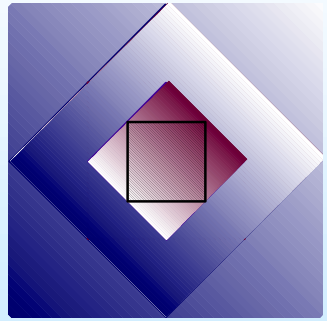
Ofer Biran

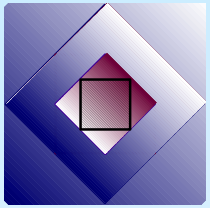
Thanks to:

Bernard Aboba, David Black,

Julian Satran, Steve Senum

IBM Research Lab in Haifa





Current draft Security MUST / MAY for Implementation:

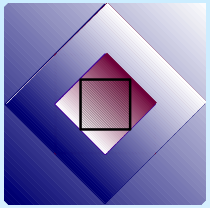
- MUST provide means of authentication and data integrity.
- MAY provide means of data privacy.
- Both can be satisfied by using IPSec.
  IPSec – ‘orthogonal’ to the iSCSI standard.
- Negotiated: Kerb5, SPKM-1,2, SRP, CHAP [TLS, proprietary]

Security Open Issues

- **Mandatory to implement** method ensures
  Implementation Interoperability

- Still might be ‘configured out’...

- e.g., in TLS, mandatory algorithm is
  `TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA`
  in CHAP: `MD5`



Selection Criteria

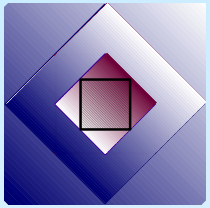
1. Suitability for the iSCSI scenarios
2. Administration
3. Standardization, existing code & implementations
4. Code complexity
5. Performance / hardware acceleration
6. Security considerations
7. Licensing

1. Suitability for the iSCSI scenarios

- Security ‘roles’:
  - Initiator
  - Target
  - iSCSI Proxy
  - iSCSI Gateway
  - iSCSI-aware firewall
- Initiators are 'users' on target systems ?
- The identity to be authenticated.

1. ...Suitability for the iSCSI scenarios

- Corporate intranet aspects, firewalls.
- Central security server appropriate ?
- iSNS requirements / interoperability.



2. Administration

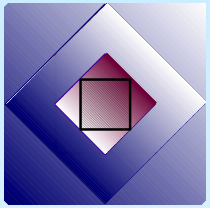
- Getting into operational state.
- Adding / removing users and service principals.
- Maintenance (passwords, certificates, security servers & databases).
- Policy.
- Authorization aspects.

2. ... Administration

- The potential methods divided to:
  - ‘User accounts on target machine’ (SRP, CHAP)
  - Security server (KERB5, CHAP/Radius, SPKM/iSNS)
  - PKI (IPSec, SPKM, TLS)

3. Standardization, existing code & implementations

- Status of formal standard
- Existing code:
  - Open source
  - Commercial libraries (GSS_API)
- Experience and acceptance
- ‘Customer base’

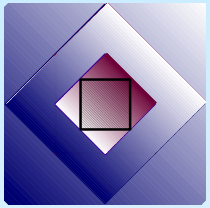


4. Code complexity

- Code size
- Programming effort
- Testing effort
  - Security server – more complex.
  - More options – more complex...

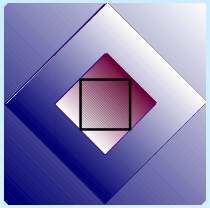
5. Performance / Hardware accelerators

- Initial Authentication – no issue
- Message authentication/integrity
- Encryption
  - not mandatory
  - Agreed – only by IPSec (or proprietary)



6. Security considerations

- Protected attacks
- Known crypto algorithm deficiencies
- Other security problems



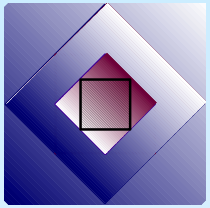
Kerberos V5

- Central KDC (AS + TGS) stores all users & services keys.
- User get credentials (TGT) from the AS, then get a ticket for each desired service.
- Service has a private key in protected file.
- Timestamps play important role.
- iSCSI login defines tokens exchange and digests based on GSS-API.

Kerberos V5

1. Suitability for the iSCSI scenarios +-
   - Excellent for Intranet scenario
   - Less suitable for Internet / crossing into Intarnet.
   - Third party (KDC) dependency.

2. Administration +
   - Some effort in initial configuration
   - Excellent for add/delete users, maintenance, Policy, Authorization aspects.



...Kerberos V5

3. Standardization, exist. Implementations +
   - Excellent experience & acceptance.
   - Large customer base.

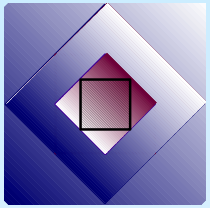
4. Code complexity +-
   - Very complex, however free & commercial GSS-API libraries exist.

5. Performance / hardware acceleration -
   - For digest: MD5 / DES based.

...Kerberos V5

6. Security considerations +-

- Crypto digest available (GSS_GetMic) (MD5 / DES issues)
- Encryption also available (GSS_Wrap) but not defined in the iSCSI draft.
- Credentials reuse & delegation.
- TGS protocol – dictionary attack (proposal to use SRP...).



SPKM-1/2 Simple Public Key Mechanism

- Based on RFC-2025 “`The Simple Public-Key GSS-API Mechanism (SPKM)`”
- SPKM-1 (random challenge), SPKM-2 (timestamp)
- iSCSI login defines token exchange:

`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`)

SPKM-1/2 Simple Public Key Mechanism

1. Suitability for the iSCSI scenarios +
   - With CA hierarchy suitable both for Intranet and Internet.
   - Proxy / real target can both play security endpoint.

2. Administration +-
   - PKI... Intranet CA + distribution of certificates. CRLs are complex.
   - Certificates can be used for authorization aspects (property fields).

... SPKM-1/2

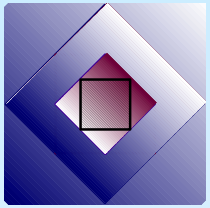
3. Standardization, exist. Implementations -
   - RFC-2025 in ‘proposed standard (since 1996)
   - NFS V4 mandates SPKM-3 which is based on SPKM (RFC-2025).
   - Very few implementations / experience.

4. Code complexity +-
   - Not complex, but lack of experience & commercial libraries.

... SPKM-1/2

5. Performance / hardware acceleration -
   - For digest: MD5 / DES based.

6. Security considerations +
   - Crypto digest available (GSS_GetMic) (MD5 issues)
   - Encryption also available (GSS_Wrap) but not defined in the iSCSI draft.
   - CRLs are problematic.



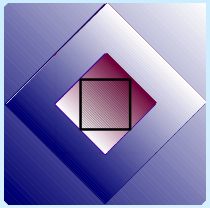
SRP

- Strong Password Authentication
- protection against both passive and active attacks.
- Server keeps password verifiers.
- Mutual authentication (the server proves the knowledge of the verifier).
- Shared key (320 bit) is constructed – no usage spec.

SRP

1. Suitability for the iSCSI scenarios
   - User/password based...
   - Machine key or user's password (?)
   - Suitable for SSPs.

2. Administration +
   - User/password DB for each target, or central security DB (with safe target connection).



...SRP

3. Standardization, existing implementations +
   - RFC-2945 in ‘proposed standard’.
   - Telnet, FTP, SSH extensions.

4. Code complexity +
   - Very simple.

5. Performance / hardware acceleration -
   - Only initial authentication (currently)

6. Security considerations +
   - Strong Password authentication. Mutual. no clear passwords saved, shared key (320 bits) is generated, can be used for MIC – no standard for this.

CHAP ([/Radius])

- Simple challenge / response scheme.
- Used for PPP authentication (defined for the PPP link layer – iSCSI defines corresponding login exchanges).
- Radius server is used on the server side – but this is optional.
- iSCSI login defines server authentication by reverse challenge / response.

CHAP ([/Radius])

1. Suitability for the iSCSI scenarios
   - User/password based...
   - Machine key or user's password (?)
   - Suitable for SSPs.
   - Target needs 'password for user' for mutual authentication.
   - Third party (Radius server) dependency.

2. Administration +
   - User/password DB for each target, or Radius security server (with safe target connection).

... CHAP ([/Radius])

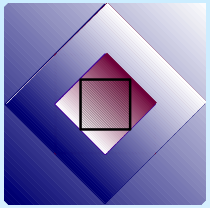
3. Standardization, exist. Implementations +
   - RFC-2945 in ‘proposed standard’.
   - Well accepted, large customer base.

4. Code complexity +
   - Very simple.

5. Performance / hardware acceleration
   - Only initial authentication.

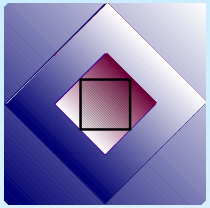
... CHAP ([/Radius])

6. Security considerations -
   - Clear password saved (on Radius server).
   - Guessing attack on the response unveil the password !
   - Target’s passwords for mutual authentication.
   - No shared key generated.



TLS

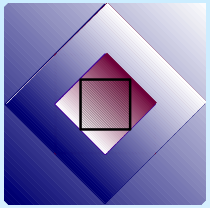
- Based on the popular SSL (99% of internet secure traffic ?)
- Public key & certificate scheme.
- Handshake phase – authentication, session key generated and integrity / encryption algorithms negotiated.
- Has its own framing (record layer) – doesn’t preserve message boundaries.
- Otherwise convenient API control.



TLS

1. Suitability for the iSCSI scenarios +
   - With CA hierarchy suitable both for Intranet and Internet.
   - Proxy / real target can both play security endpoint.

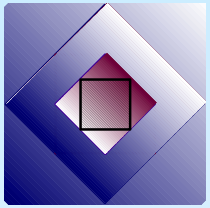
2. Administration +-
   - PKI... Intranet CA + distribution of certificates. CRLs are complex.
   - Certificates can be used for authorization aspects (property fields).



...TLS

3. Standardization, exis implementations +
   - **THE** Internet de-facto security.

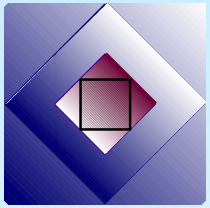
4. Code complexity +-
   - Complex, but many commercial libraries.



...TLS

5. Performance / hardware acceleration -
   - Hardware accelarators exists, not 1Gbs
   - Record layer fragmentation breaks iSCSI steering and synchronization.

6. Security considerations +
   - CRLs are problematic.



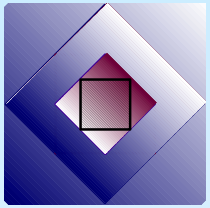
IPSec

- Security at the IP level.
- Transport mode for host to host.
- Tunnel mode between routers (VPNs).
- AH – IP header authentication.
- ECP – encryption of the payload (& auth)
- SA generated by IKE (or KINK...)
  - Manual keying or certificate based.
  - Main mode for authentication, keying material and protection of quick modes.
  - Quick modes for generating specific Sas.
- Complex policy rules for handling packets.
- Cannot be negotiated in iSCSI level.

IPSec

1. Suitability for the iSCSI scenarios +-
   - Security on the (ext-)Initiator – firewall segment.
   - Suitable for ‘iSCSI aware firewall’.
   - The only acceptable solution for encryption.
   - Fragmentation of IKE cert payloads (filters).

2. Administration -
   - PKI... Intranet CA + distribution of certificates.
   - Or – manual keys setting – not scalable.
   - CRLs are complex.
   - Complex policy.



... *IPSec*

3. Standardization, exist. Implementations +
   - IPSec, IH,ECP,ISAKMP, DOI, IKE
   - Well accepted, growing usage.

4. Code complexity +-
   - Very complex, IP Stack.

... IPSec

5. Performance / hardware acceleration +
   - Available hardware with excellent encryption/integrity performance.

6. Security considerations +
   - Issue of binding the identity authenticated during IKE SA with iSCSI.
   - Awareness of iSCSI implementation of the underlying IPSec protection. Would iSCSI / IPSec be orthogonal (only the administrator knows).
   - Credential reuse. (+)
   - CRLs are problematic.

	iSCSI Scena.	Admin	Std. & Impl.	Code Comp.	Perf. HW	Secur
Kerb5	+-	+	+	+-	-	+-
SPKM	+	+-	-	-	-	+
SRP		+	+	+	-	+
CHAP		+	+	+		-
TLS	+	+-	+	+-	-	+
IPSec	+-	-	+	+-	+	+

Recommendation

1. MUST implement E-E Authentication
   - Kerberos - Third party, non-intranet
   - SPKM - standard, code complexity
   - CHAP – Security, mutual auth.
   - TLS – record layer
   - SRP with defined digests

2. MUST (?SHOULD) implement IPSec ?unless… system where IPSec must be provided by other component.

… MUST IPSec

- Retrieving IKE identities / certs should be possible.
- Require IPSec/IKE administrative interface ?
- Restricting IPSec (Tunnel / ESP) ?
- Defining the IKE / SA rules in the iSCSI standard ? (iSCSI login in lower level – or iSCSI ‘login’ standard on 2 levels)