iSCSI Security Requirements:
What MUST be done?

David L. Black (EMC)

IP Storage WG co-chair

A Procedural Note

- Security is too important to leave to the security wizards …
  - Can't do a comprehensive security tutorial here
  - But we will try to explain everything
- Please ask if you don't understand something
  - Interrupt if necessary, but with some courtesy

Security Property Definitions

Authentication	Who or what are you? Prove it!
Authorization	What are you allowed to do?
Access Control	Authorization of access
Integrity (Cryptographic)	Has this data been tampered with?
Confidentiality (or ***Privacy***)	Has this data been disclosed?
Non-Repudiation	Can someone prove that you did X?

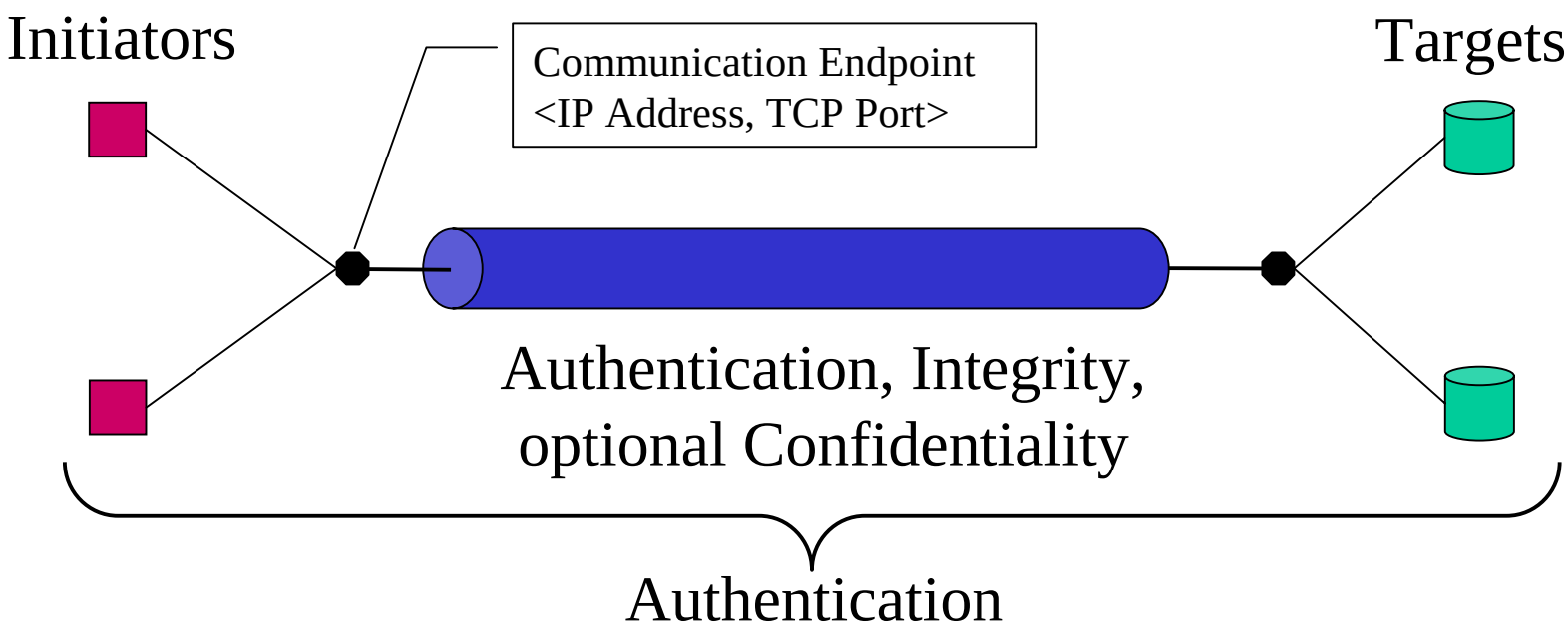
iSCSI Security Requirements

- Threat environment: public network
  - Crackers and script kiddies
- Authentication: MUST implement
  - Mutual - Initiator to Target and v.v.
- Cryptographic integrity: MUST implement
  - Secure hash - checksum or CRC is not sufficient
  - MUST counter regeneration and replay threats
- Confidentiality (encryption) - MUST specify
  - May be OPTIONAL to implement

iSCSI Security Concerns

- Authorization and Access Control
  - SCSI access controls: above iSCSI level
  - iSCSI control: allow/disallow connections
    - Specification of this (e.g. ACL interface) NOT required
- Security algorithm and protocol selection
  - At least one "MUST implement" in each case
- Security Usage: can be configurable/negotiable
  - Dynamic mechanisms MUST be secure against impersonation and man-in-the-middle threats

Two Domains of Security



- Integrity and Confidentiality are assumed behind endpoints, Authentication may not be.
  - WWW security often has a similar structure
    - SSL/TLS server authentication + client password

Authentication Coordination

- Authentication identities
  - Secure connection (e.g., X.509 cert.)
  - In-band authentication
- Are both needed?
  - If used in same direction, how are they related?
- WWW example (SSL/TLS):
  - Server identity from SSL/TLS must match URL
  - Client usually uses an inband identity and password
    - Client certificates are rarely used

Auth. Coordination Comments

- WWW-like structure
  - Initiator checks Target secure conn. identity
    - Need that identity information as part of Discovery
  - Inband Initiator authentication to Target (e.g., ACL)
- Single-level identity structure
  - Both secure connection identities checked
- "Send Targets" implications
  - Targets use same secure conn. identity as "iscsi"
  - Else have to return target secure identity information