MSEC Area 3 – Policy

(draft-irtf-smug-polreq-00.txt)

Presented by Patrick McDaniel

pdmcdan@eecs.umich.edu

IETF MSEC BOF

San Diego, CA

December 12, 2000

Problem

- How do we create, distribute, and enforce a session (security) policy?
- Policy is "... a statement of the entirety of security relevant parameters used to implement the group."
  - who are the entities allowed to participate,
  - which mechanisms will be used to achieve mission critical goals
- Policy (from framework document)
  - Creation, Translation, Representation

Group vs. Peer Policy

- Similar objectives
  - Distribution of context defining policy
  - Collaboration/use of existing work
- Differences
  - Describes more dynamic, complex context
  - Local policies – participant requirements
  - More complex auth/access control models
  - N-party negotiation

Requirements

- Creation and translation
  - Flexible policy infrastructures (creation)
  - Synchronized, unambiguous policy (translation)
- Representation
  - Unambiguous, succinct, clear
  - Support a useful range of policies
  - Flexibility in integrating new policies
  - Support for existing infrastructures and approaches (PFWG, SPS, IPSec)

Building Blocks

- Policy system can be defined my these areas:
  - Identification
  - Mechanism
  - Authorization
  - Access Control
  - Verification
- ASN.1 structure (example: GSAKMP)

Documents

- Multicast Security Policy, P. McDaniel and H. Harney and P. Dinsmore and A. Prakash. June 2000.

  draft-irtf-smug-mcast-policy-00.txt

- Multicast Security Policy Requirements and Building Blocks, P. McDaniel, H. Harney, A. Colegrove, A. Prakash, and P. Dinsmore. November 2000.

  draft-irtf-smug-polreq-00.txt

A session (security) policy is …

- "… a statement of the entirety of security relevant parameters and facilities used to implement the group."
  - how security directs group behavior,
  - who are the entities allowed to participate,
  - which mechanisms will be used to achieve mission critical goals
- Note: not restricted to electronically distributed statements