Security Policy

IETF-109

Sarah Heiner
Sarah.Heiner@jhuapl.edu
240-592-3704
Overview

- BPSec represents security operations as extension blocks in a bundle

- The lifecycle of an extension block is:
  - A series of events
  - Finite and unchanging

- The reaction to these events can make or break end-to-end security
  - Consistent reactions to events enable end-to-end security
  - Inconsistent reactions to events disable end-to-end security

- There is value in documenting these events and possible reactions to the events
Interoperability Enabled by Security Policy

Syntactic Interoperability

- **Enabled by:**
  - Security protocols
  - Cipher suites

- **Required to:**
  - Parse/decode network information
  - Generate cryptographic material

Semantic Interoperability

- **Policy required to process security services**

- **Enabled by:**
  - Security policy
  - Actions associated with policy

- **Required to:**
  - Provide coherent, consistent reactions to security events
  - Process security services

BPSEC establishes a security context
Defining Security Policy

- Security policy is the set of configurable reactions for a security operation event
  - Consistent behavior in response to security events
  - Context necessary for processing security
  - Identification of required security operation(s)

- Consistent behavior requires coherent action in response to events
Security Operation Lifecycle

Security operation events are universal policy points
Proposed Action

- The security operation lifecycle is a series of events which are finite and unchanging
- Propose documenting this lifecycle for BPSeq
- Provide a common language which enables the discussion and definition of policy among different BPSeq implementations