ION 4.0.2 BPSec Policy Release Notes

Overview of BPSec Policy

BPSec Policy allows network operators to indicate required security operations for bundles as well as configure reactions to certain security events. Policy is configured using the bpsecadmin ION administrative tool and is implemented for Bundle Protocol Version 7 only.

While the expression of BPSec policy is complete in this release, certain options are not operationally supported due to the current capabilities of the ION BPSec implementation. Notably only a subset of certain security event actions are supported (as noted below), not all blocks are supported as security targets, and ION does not currently implement the default security context being standardized in the IETF.

Highlights of BPSec Policy

- The bpsecadmin utility has been updated to
    - Support an initialization command, '1', which **must** be called to start the bpsecadmin utility as part of ION startup.
    - Accept all BPSec policy statements (policy rules, event sets, events, and associated processing actions) using a JSON syntax.
    - Persist all BPSec policy objects to the ION SDR for persistent storage when added by a user, and to remove these items from the SDR when removed by a user.
    - Co-exist with heritage BIB/BCB rules so as to not break existing scripts.
        - When both BPSec policy and legacy BIB/BCB policy co-exist, BPSec policy rules will be used instead of BIB/BCB legacy policy.
- The ION BPSec Implementation has been updated to
    - Initialize BPSec policy objects from the SDR at system startup
    - Apply policy rules to blocks when creating, receiving, or delivering bundles.
    - Apply supported policy actions at defined security events.
- The BPSec Policy engine supports:
    - Policy Rules associated with named event sets.
    - Named Security Policy Event Sets
    - Security Policy Events
- Supported Optional Processing Actions:
    - Remove security operation.
    - Remove security operation target.
    - Remove all security target operations.
    - Report with reason code.
    - Fail bundle forwarding.

- Added support for issuing the following reason codes associated with BPSec:
    - Missing Security Service
    - Unknown Security Service
    - Unexpected Security Service
    - Failed Security Service
    - Conflicting Security Services

ION Modifications

File	Status	Summary
Makefile.am	Modified	
bpv7/doc/pod5/bpsecrc.pod	Modified	Updated to include security policy command syntax.
bpv7/library/bpP.h	Modified	Added security reason codes.
bpv7/library/bpsec.c	Modified	Corrected the eidsMatch function for wildcard matching. Wildcard character now functions as * (matching 0 or more).
bpv7/library/ext/bpsec/bcb.c	Modified	Handling of security policy rules added. Corrected encryption/decryption of the payload block for policy rules. BCB written to SDR when attached.
bpv7/library/ext/bpsec/bib.c	Modified	Handling of security policy rules added. Added support for the application of integrity over the primary and payload blocks. BIB written to SDR when attached.
bpv7/library/ext/bpsec/ bpsec_policy.*	Created	Established the BPSec policy engine. Implementation of processing actions.
bpv7/library/ext/bpsec/ bpsec_policy_event.*	Created	Implementation of security operation events which are persisted to the SDR.
bpv7/library/ext/bpsec/ bpsec_policy_eventset.*	Created	Implementation of security policy event sets and associated red-black tree.
bpv7/library/ext/bpsec/ bpsec_policy_rule.*	Created	Implementation of security policy rules including persistence and searching functionality.
bpv7/library/ext/bpsec/bpsec_util.c	Modified	bpsec_serializeASB updated to use ASB context flags and serialize security context parameter data. ZCO bug fix.
bpv7/library/ext/bpextensions.c	Modified	Added processOnDequeue callback for quality of service block (extension block).
bpv7/library/ext/bpq/bpq.c	Modified	Added qos_processOnDequeue function.

bpv7/library/libbpP.c	Modified	Auto-init the bpsec policy engine on startup of the node.
bpv7/utils/bpsecadmin.c	Modified	Acceptance and handling of security policy commands.
bpv7/utils/jsmn.h	Added	JSON parsing utility.
doc/bpsec_policy_info.pdf	Created	Documentation of configuration options for BPSec policy.
ici/include/ionsec.h	Modified	Added security policy rules and event sets to the security database as well as in shared memory.
ici/include/radix.h	Created	Custom implementation of a radix tree.
ici/library/ionsec.c	Modified	Added support for security policy in shared memory.
ici/library/platform.c	Modified	Modified the findToken function to support JSON commands.
ici/library/radix.c	Created	Custom implementation of a radix tree.
ici/library/radixP.h	Created	Custom implementation of a radix tree.
tests/nm-unit/utils/radix_gen.*	Created	Generate a radix tree for testing.
tests/nm-unit/utils/radix_pt.*	Created	Radix tree performance test with Lyst data for comparison.
tests/nm-unit/utils/radix_pt/dotest	Created	Test script for radix tree performance.
tests/nm-unit/utils/radix_ut.*	Created	Radix tree unit tests.

Included Utilities

jsmn, a minimal JSON parser, has been added to the BPv7 utilities to support JSON policy commands handled by bpsecadmin.

jsmn is an open source utility distributed under MIT license.

Testing

The BPSec Policy implementation has been tested for the nominal path, including handling the Security Source, Verifier, and Acceptor roles for bib-integrity and Security Source and Acceptor roles for bcb-confidentiality.

Known Issues

The following are known or potential issues with this release.

- JSON processing for bpsecadmin has not been thoroughly tested – it is possible that malformed JSON input could cause problems.
- The BPSec implementation is not feature complete:
    - Encryption with a BCB is only supported over the bundle payload.
    - Other combinations have not been fully tested.
- This release is only tested with the ION NULL cipher suite.
- The following policy actions are not supported
    - Request storage of a bundle that should not be forwarded.
    - Override target block processing control flags
    - Override security block processing control flags.
- The IETF DTNWG default security context is not implemented in ION and, therefore, parameters related to this security context are not supported.

Contact

BPSec Policy was implemented by The Johns Hopkins University Applied Physics Laboratory for the ION 4.0.2 release.

Ed Birrane
Edward.Birrane@jhuapl.edu

Sarah Heiner
Sarah.Heiner@jhuapl.edu