NETCONF Access Control

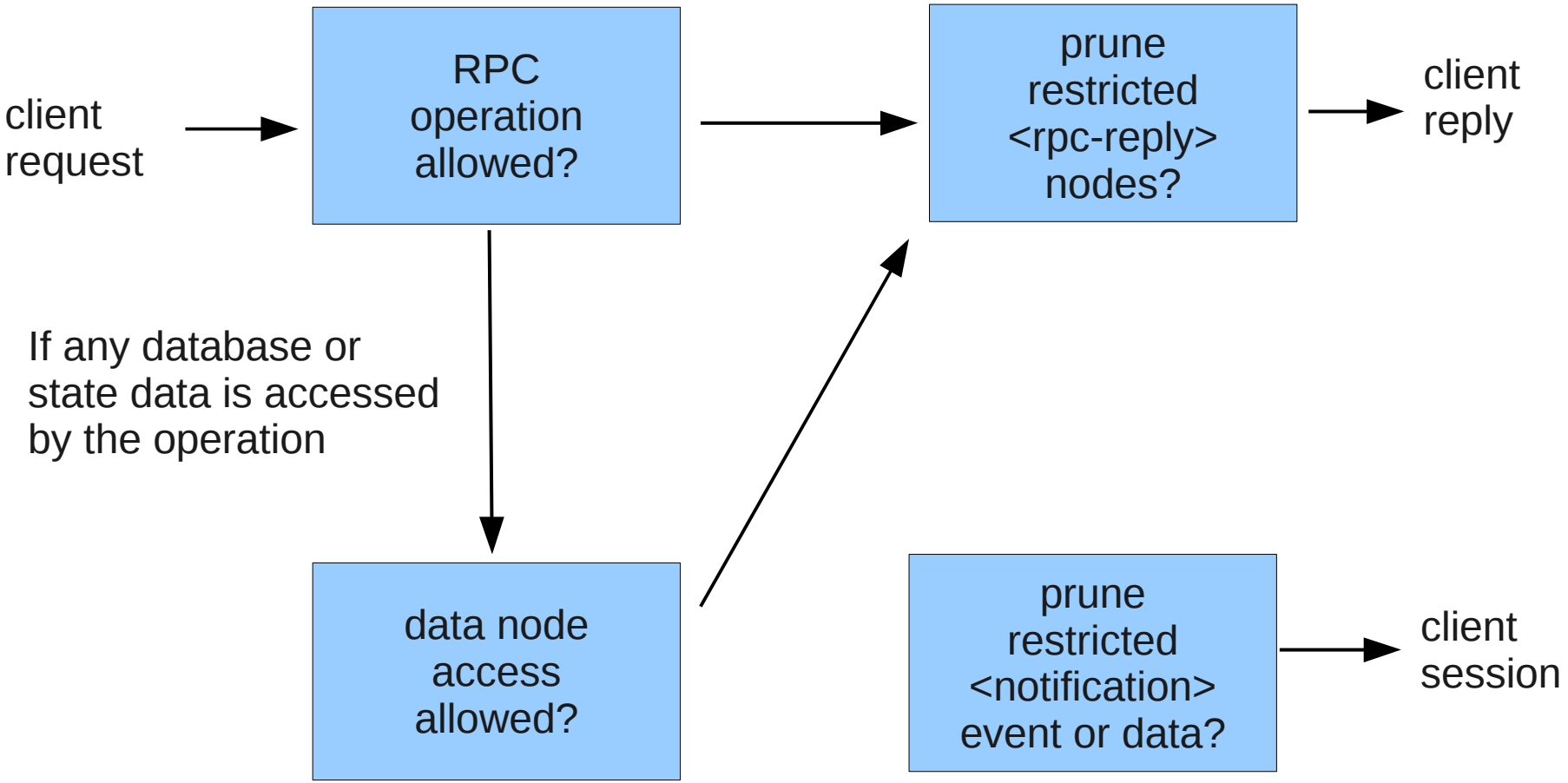
draft-bierman-netconf-access-control-01
IETF 77, March 2010

Andy Bierman
andyb@iwl.com

Agenda

- Why does NETCONF need a standard access control model (ACM)?
- What are the functional requirements for a standard ACM for NETCONF?
- Extra Slides (if time permits):
  - What is 'nacm:secure', and why is content tagging important for configuration?
  - What is in nacm.yang?

Conceptual Model



Need for a standard ACM (1)

- Operators will benefit from a standard way to control access to NETCONF content, based on the user associated with the NETCONF session.

Need for a standard ACM (2)

- Without a standard ACM, every NETCONF user is a 'root' user:
  - NETCONF has only 1 login sequence.
  - SNMP has the concept of 2 user classes built in (public and private community string).
  - Some CLIs have the concept of an extra login step to get to 'configuration mode'.

Need for a standard ACM (3)

- NETCONF allows unlimited operations and actions to be added to the protocol:
  - The likelihood that every user should have access to everything is even lower than SNMP.
  - Specialized configuration for access control will increase the complexity of new module deployment.

Need for a standard ACM (4)

- The threat of XML data injection attacks in NETCONF needs to be addessed:
  - There is a known SSH end-of-message attack that can be used to truncate an <rpc> request and insert one or more new <rpc> requests into the data stream.
  - Access control can be used to constrain the scope of this attack by limiting the commands and data that an attacker can reach.

Consensus Check

- Should the IETF develop a standard solution for session authorization to configurable subsets of all NETCONF operations and content?
  - a) yes
  - b) no

NACM Requirements (1)

- Protocol Control Points
  1) <rpc> operation requested.
  2) Server contents that can be returned for a <get> request. This includes all configuration database contents, plus read-only non-configuration data.
  3) <notification> event type to be sent.

NACM Requirements (2)

- Non-control points:
  - The <rpc-reply> contents for an arbitrary RPC that does not access the conceptual <get> content:
    - If the client can invoke the operation, it can receive any reply for that operation.
  - The <notification> contents for an arbitrary notification event:
    - If the client is authorized to receive the event type, it can receive any possible content for that event type.

NACM Requirements (3)

- Simplicity:
  - Localized cost:
    - Simple tasks must be easy to configure, or require no configuration at all.
    - Simple mechanisms should not require any special knowledge, like XPath.
    - Complex tasks should be possible using additional, optional-to-use, mechanisms.
  - Familiar set of permissions:
    - read, write, exec

NACM Requirements (4)

- Database Access:
  - The same access control rules apply to all standard databases:
    - Must be applied to <candidate>, <running>, and <startup>.
    - External <url> databases are not subject to access control enforcement by the server.
    - Managing credentials for external databases (using other protocols) is outside the scope of NACM.

NACM Requirements (5)

- Users and Groups:
  - The server must obtain a user name string from the transport layer somehow.
  - A user may be a member of zero or more groups.
  - A group contains zero or more users.
  - An access control rule applies to one or more groups.

NACM Requirements (6)

- Superuser Access:
  - The server should support the concept of a superuser (root) account that can bypass all access control enforcement:
    - Needed for secure initial bootstrap of NACM configuration.
    - Needed if the NACM configuration (or the implementation) is broken and all users are locked out.

NACM Requirements (7)

- On/off switch:
  - It should be possible to enable and disable access control enforcement without deleting or altering any access control rules that are configured.

NACM Requirements (8)

- Separate configurable default modes for each permission:
  - read-default
  - write-default
  - exec-default
- These defaults are applied when there is no appropriate access control rule found for the requested user/operation/data.

NACM Requirements (9)

- Identifying security holes:
  - Data modeler knows which conceptual data is a security risk, according to IETF security consideration guidelines.
  - Operators need to learn of this data and configure the proprietary ACM to block access to it.
  - A machine-readable statement could be used to help YANG tools identity sensitive data that should not be accessed by default.

NACM Requirements (10)

- Data shadowing and leakage:
  - The server should treat 'pointer' data nodes as if the user requested access to the 'pointed-at' data node.
  - Only identifiable for YANG leafref types.
  - Key leaf values returned in instance-identifiers may leak sensitive information. The data modeler should be aware of this when using i-i data nodes.

NACM Requirements (11)

- Monitoring and Errors:
  - Counters to indicate when a write or exec request was denied should be maintained.
  - An 'access-denied' error is generated for denied write and exec requests.
  - A denied read request causes the unauthorized data to be silently omitted, instead of an 'access-denied' error.

Consensus Check

- Do you generally agree with these requirements for NETCONF access control?
  - a) yes
  - b) no

Extra Slides

- The nacm:secure and nacm:very-secure YANG language extensions
- Brief overview of nacm.yang contents
- Free client and server implementation of nacm.yang available at http://yuma.iwl.com/
  - called yuma-nacm, not nacm

YANG Extensions for NACM

- nacm:secure
  - Instead of using the default rule, deny requests for write or exec access.
  - Use the default rule (read-default) for read operations.
- nacm:very-secure
  - Instead of using the default rule, deny all access.
- These extensions only apply if no ACL is found for the specific request.

nacm.yang (1)

- Groups are identified with YANG identities:
  - in case an operator wants to attach semantics to a specific group name.
  - no standard semantics for 3 example groups included (admin, monitor, guest).
- Global boolean controls:
  - enable-nacm
  - read-default
  - write-default
  - exec-default

nacm.yang (2)

- Simple access control rules are provided:
  - <module-rule>
    - access to an entire YANG module.
  - <rpc-rule>
    - access to a specific RPC operation.
  - <data-rule>
    - access to a subset of all conceptual data nodes, available for a <get> operation.
  - <notification-rule>
    - access to a specific notification event type.

nacm.yang (3)

- NACM access control rule common fields:
  - <rule-name>
    - arbitrary name for user-ordered list insertion.
  - <allowed-rights>
    - bits containing zero or more permissions granted by this rule.
  - <allowed-group>
    - leaf-list of all the group names that are affected by this rule.
  - <comment>
    - user comment to store along with this rule.

nacm.yang (4)

- Open issues:
  - More complex data rules and wildcard mechanisms?
  - What to do about <copy-config> leaving out unauthorized data?
    - Should backup/restore only be done by a user with full access, or should the server violate the NETCONF operation and pretend the unauthorized data was not removed?
  - Is an <access-denied> notification event needed?