Information Model for Consumer-Facing Interface

draft-kumar-i2nsf-client-facing-interface-im-04

Rakesh Kumar, Anil Lohiya Juniper Networks

Dave Qi Bloomberg

Nabll Bitar, Senand Palislamovic Nokia

Liang Xia Huawei

Jaehoon Paul Jeong SKKU

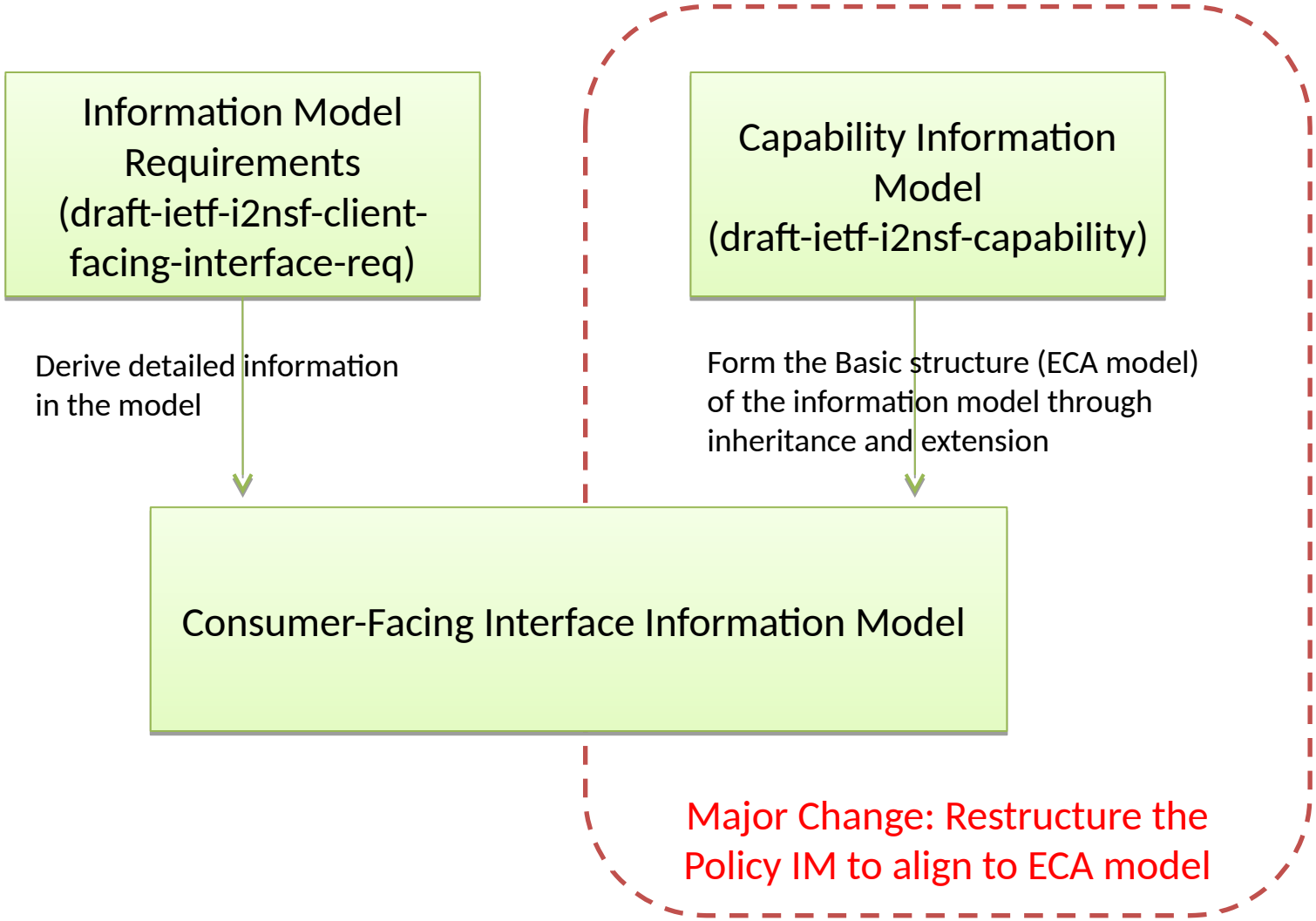
IETF-100, Singapore

Nov 14, 2017

Agenda

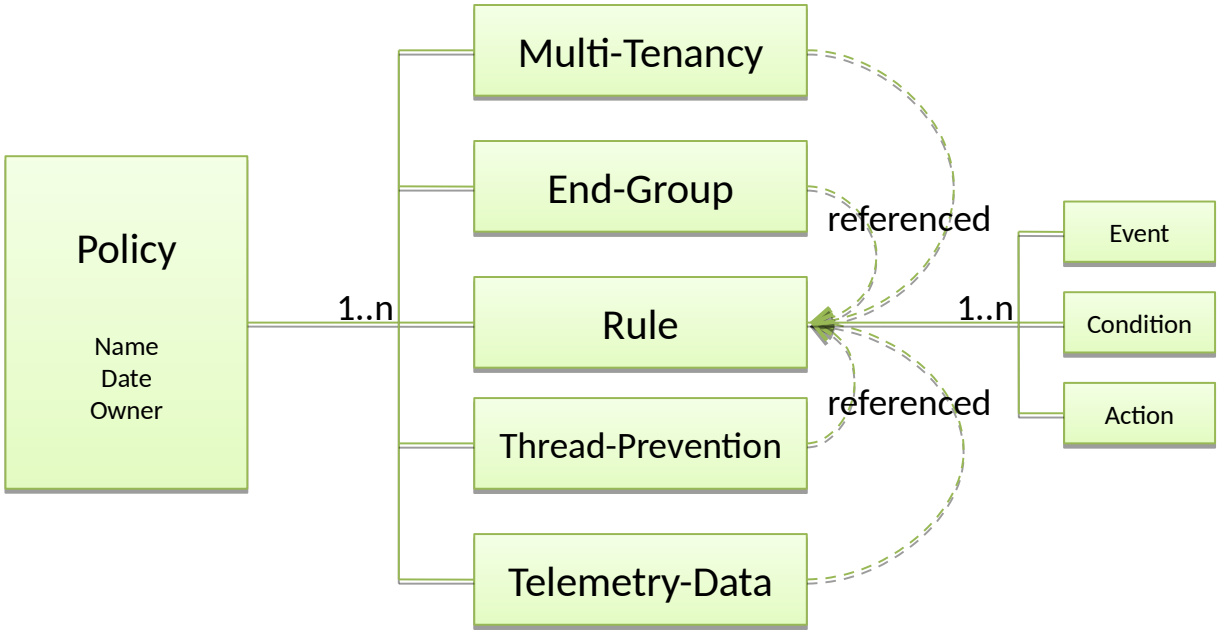
- Major Change of This Version
- Information Model Design
- Next Steps and Plan

Major Change of This Version



Information Model Design

- Information model method
  - Identify a set of managed objects (resources)
  - Relationship among these objects
  - Objects and the relationship among them define the interface.
- Basic information model structure – Policy + ECA Rules + Objects



Event Subclass

- **Name**
- **Date**
- **Event-Type:** "ADMIN-ENFORCED", "TIME-ENFORCED" or "EVENT-ENFORCED"
- **Time-Information:** "BEGIN-TIME" and "END-TIME“; recurring time
- **Event-Map-Group**
  - Name
  - Date
  - Security-Events
  - Threat-Map

Condition Subclass

- **Name**
- **Date**
- **Source:** Policy-Endpoint-Group, Threat-Feed, Custom-List, "ALL" , Telemetry-Source
- **Destination:** Policy-Endpoint-Group, Threat-Feed, Custom-List, "ALL" , Telemetry-Destination
- **Match**
- **Match-Direction:** "FORWARD" , "INVERSE" or "BOTH"
- **Exception**

Action Subclass

- **Name**
- **Date**
- **Primary-Action:** "PERMIT", "DENY", "MIRROR", "REDIRECT", "RATE-LIMIT", "TRAFFIC-CLASS", "AUTHENTICATE-SESSION", "IPS", "APP-FIREWALL", or "COLLECT"
- **Secondary-Action:** "LOG", "SYSLOG", or "SESSION-LOG"

Object Definition… (1/2)

- Managed objects possibly referenced by Rule
  - **Multi-Tenancy** object
    - **Policy-Domain, Policy-Tenant, Policy-Role, Policy-User**
    - **Authentication-Method:** Password, Token, Certificate, SSO; Mutual or not?
  - **Endpoint-Group** object (referenced by Rule Condition)
    - **Tag source** (endpoint group information source) : LDAP, Active Directory, CMDB, GeoIP Database, …
    - **User-group, Device-group, Application-group, Location-group:** Name, Date, Group-Type, Tag-Server, Group-Member, Risk-Level

Object Definition… (2/2)

- **Threat-Prevention** object (referenced by Rule Condition)
  - **Threat-Feed**: Name, Date, Feed-Type, Feed-Server, Feed-Priority
  - **Custom-List**: Name, Date, List-Type, List-Property, List-Content
  - **Malware-Scan-Group**: Name, Date, Signature-Server, File-Types, Malware-Signatures
- **Telemetry-Data** object (referenced by Rule Condition and Action)
  - **Telemetry-Data**: Name, Date, Log-Data/Syslog-Data/SNMP-Data/ sFlow-Record/NetFlow-Record, NSF-Stats
  - **Telemetry-Source**: Name, Date, Source-Type, NSF-Source, NSF-Credentials, Collection-Interval, Collection-Method, Heartbeat-Interval, QoS-Marking
  - **Telemetry-Destination**: Name, Date, Collector-Source, Collector-Credentials, Data-Encoding, Data-Transport

Net Steps and Plan

- Refine the draft to
  - Update the draft whenever the requirement draft get updated : draft-ietf-i2nsf-client-facing-interface-req
  - Align and Sync with I2NSF capability Information Model draft: draft-ietf-i2nsf-capability
  - Extend the information model to accommodate the security p olicies of the open-source security software, such as Snort and Suricata
  - Proof-of-Concept (POC) of the information model along with t he corresponding data model draft (draft-jeong-i2nsf-consumer-facing-interface-dm) through the next IETF I2NSF Hackathon Project.

- **Plan: Call for WG adoption**

Thanks!

Liang Xia (Frank)