Endpoint Compliance Profile

SACM WG Virtual Interim Meeting

03/09/16

Agenda

- Overview
- Solutions update
- Alignment with SACM
- Next steps

Overview

- ECP[1] provides an extensible framework for collecting, communicating, and evaluating endpoint information

- Consists of IETF NEA protocols and complementary TCG TNC interfaces and protocols

- Currently utilizes ISO Software Identification (SWID) [2] tags to reduce the security exposure of a network by confirming all network-connected endpoints are:
  - Known and authorized
  - Running applications that are known and authorized
  - Running applications that are patched and up-to-date
  - Applications with known vulnerabilities can be located and patched

[1] https://datatracker.ietf.org/doc/draft-haynes-sacm-ecp/

[2] http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670

Solutions update

- NEA PA-TNC, PB-TNC, PT-TLS were already in the IETF[1]
- ECP and SWID Message and Attributes for PA-TNC[2] were just submitted
- Preparing additional I-Ds for submission
  - PC-TNC: Interface between NEA PCs and a PBC based on IF-IMC[3]
  - PV-TNC: Interface between NEA PVs and PBS based on IF-IMV [4]
  - Server Discovery and Validation: Protocol that enables endpoints to discover trusted servers based on PDP Discovery and Validation[5]

[1] https://datatracker.ietf.org/wg/nea/documents/

[2] https://datatracker.ietf.org/doc/draft-coffin-sacm-nea-swid-patnc/

[3] http://www.trustedcomputinggroup.org/resources/tnc_ifimc_specification

[4] http://www.trustedcomputinggroup.org/resources/tnc_ifimv_specification

[5] http://www.trustedcomputinggroup.org/files/resource_files/3D59FB5E-1A4B-B294-D0F322A08B48E02E/Server_Discovery_And_Validation_v1_0r19-PUBLIC%20REVIEW.pdf

Alignment with SACM Use Cases[1]

- Define, publish, query, and retrieve security automation data
  - Extensible to support any data model via PA-TNC
  - Provides a mechanism to communicate information between an endpoint and server via NEA
  - Does not provide an interface to the repository (opportunity to extend ECP)
- Endpoint identification and assessment planning
  - Supports unique endpoint identification (e.g. device certificate)
  - Supports the collection of information required for endpoint characterization
- Endpoint Posture Attribute Value Collection/Evaluation
  - Collection can be triggered by the endpoint, server, or due to some event
  - NEA PCs support the gathering of endpoint information
  - IF-IMC provides a interface by which to easily integrate PCs into NEA

[1] https://datatracker.ietf.org/doc/rfc7632/

Alignment with SACM Architecture[1]

- PVs can subscribe to their corresponding PCs to receive collection data that is of interest

- Need to figure out what a NEA client is[2]
  - Is it an internal collector which serves in one or more component roles?
    - Provider of posture attribute information
    - Consumer of collection guidance
  - Is it a target endpoint that can provide posture attribute information and consumer collection guidance?
  - Does it depend on implementation?

[1] https://datatracker.ietf.org/doc/draft-ietf-sacm-architecture/

[2] https://github.com/sacmwg/draft-ietf-sacm-architecture/issues/38

Alignment with SACM Information Model[1]

- Provides a data model by which to express software inventory data which is represented in the IM as a software instance

- More importantly, ECP is easily extensible and can accommodate new information as needed
    - Update the IM to accurately reflect the new information
    - Create a data model to represent the new information
    - Extend PA-TNC to support the new data model
    - Implement PCs/PVs to support the PA-TNC extension

[1] https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/

Alignment with SACM Vulnerability Assessment Scenario[1]

- Describes how NEA can be used to collect software inventory information using SWID tags
  - Endpoint characterization
  - Guidance applicability
  - Vulnerability status

- Does not currently address the need to collect/evaluate configuration information with respect to determining vulnerability status
  - However, it is extensible and data models based on OVAL could satisfy this need

- Makes this information available to other SACM Components

[1] https://datatracker.ietf.org/doc/draft-coffin-sacm-vuln-scenario/

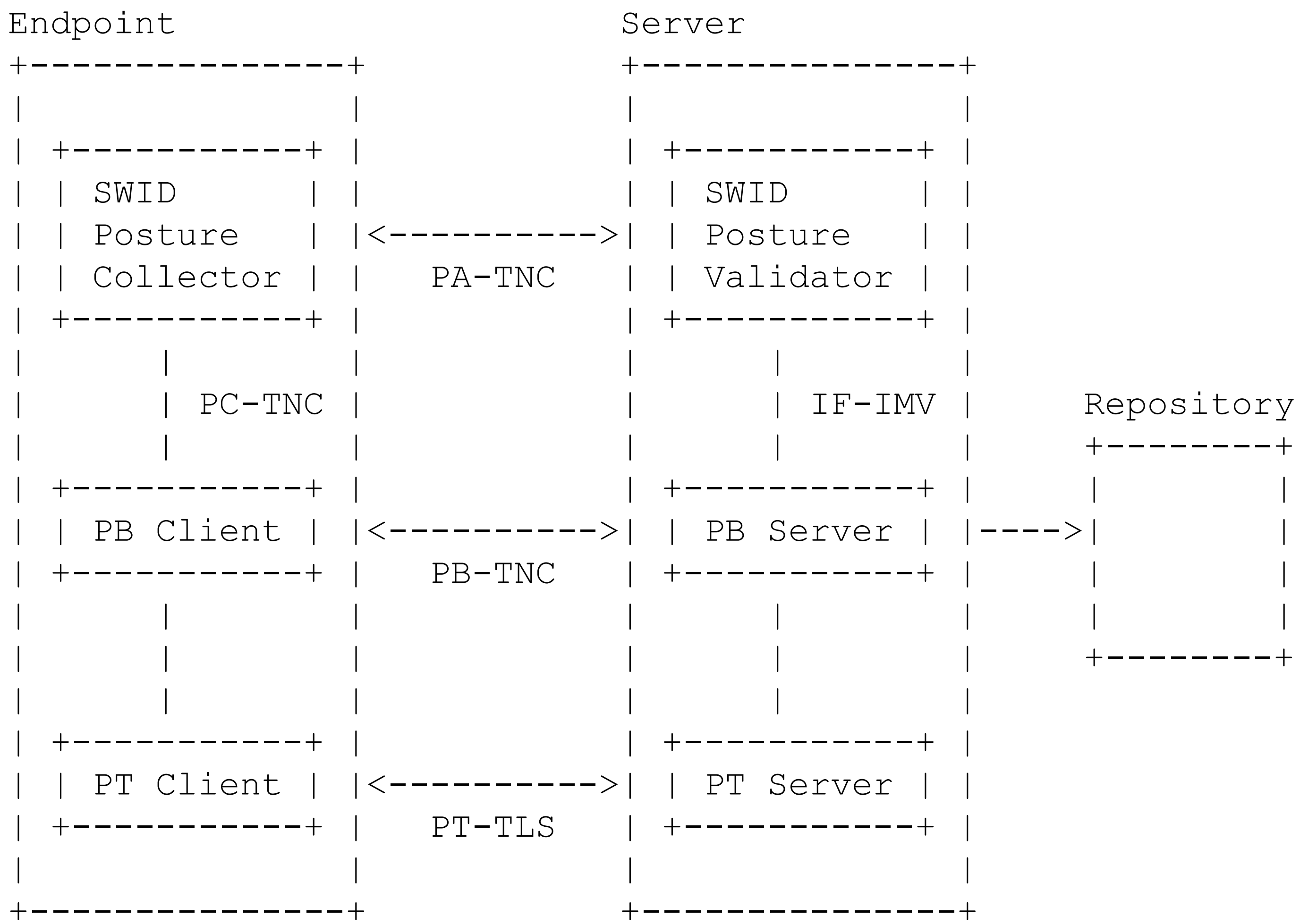
Next steps

- Update this I-D based on feedback

- Request a call for adoption

- Continue to develop additional solutions that build on NEA protocols
  - PC-TNC (VIM after IETF 95)
  - PV-TNC (IETF 96)
  - Server Discovery and Validation (VIM after IETF 96)

Endpoint-Server Communication as Described in ECP



```
      Endpoint                     Server
      +---------------+            +---------------+
      |               |            |               |
      | +-----------+ |            | +-----------+ |
      | | SWID      | |            | | SWID      | |
      | | Posture   | |<---------->| | Posture   | |
      | | Collector | |   PA-TNC   | | Validator | |
      | +-----------+ |            | +-----------+ |
      |       |       |            |       |       |
      |       | PC-TNC|            |       | IF-IMV|     Repository
      |       |       |            |       |       |     +--------+
      | +-----------+ |            | +-----------+ |     |        |
      | | PB Client | |<---------->| | PB Server | |---->|        |
      | +-----------+ |   PB-TNC   | +-----------+ |     |        |
      |       |       |            |       |       |     |        |
      |       |       |            |       |       |     +--------+
      |       |       |            |       |       |
      | +-----------+ |            | +-----------+ |
      | | PT Client | |<---------->| | PT Server | |
      | +-----------+ |   PT-TLS   | +-----------+ |
      |               |            |               |
      +---------------+            +---------------+
(Server found via Server Discovery and Validation Protocol)
```