ECP Recommendations

IETF 94

11/05/2015
Agenda

• Status

• Background

• Criteria

• Recommendations

• Next steps
Status

• Discussed the ECP specifications during the last SACM Virtual Interim Meeting\(^1\)
  • Resulted in a call for contributions for endpoint posture assessment\(^2\)

• Discussed the idea of bringing the TCG TNC specifications to the IETF with the TCG Board at the last TCG Meeting
  • TCG Board seemed fine with the transfer, but, would like more information (i.e. which specifications and when)

Background

• Examines the ECP specifications and SACM documents and provides high-level recommendations\(^1\)

• Considers the ECP specifications in the context of the endpoint self-reporting use case

• Aims to help the WG to form an opinion about the ECP specifications

\(^1\) https://datatracker.ietf.org/doc/draft-haynes-sacm-ecp-recommendations
Criteria

• Alignment with SACM
  • 1: Poor alignment with SACM (requires extensive modifications)
  • 2: Good alignment with SACM (requires some modifications)
  • 3: Strong alignment with SACM (requires minor modifications)

• How the specification may be used in SACM as well as potential modifications

• Priority for sending the specification to SACM based on the need for a capability
  • LOW: Not critical to SACM
  • MEDIUM: Somewhat critical to SACM
  • HIGH: Very critical to SACM
NEA PA-TNC$^1$

• Protocol that carries attributes between Posture Collectors and Posture Validators

• Alignment (3 – Strong alignment with SACM)
  • Highly extensible, lightweight, and compatible with TNC IF-M$^2$
  • Supports standard and vendor-specific extensions
  • Basic data model for collection guidance, posture attributes, and assessment results

• Potential changes
  • Extend to support additional posture assessment information and data models
  • Remove out-of-scope capabilities

• Priority (HIGH)
  • Charter calls for "a protocol and data format for collecting actual endpoint posture"

---

NEA PB-TNC\(^1\)

- Protocol that routes the exchange of posture assessment information messages

- Alignment (3 – Strong alignment with SACM)
  - Highly extensible, lightweight, and compatible with TNC IF-TNCCS\(^2\)
  - Operates independent of the Posture Collectors and Posture Validators

- Potential changes
  - Standardize the computation of global assessment results and delegate to the evaluation function
  - Examine the state machine regarding the transmission of messages

- Priority (HIGH)
  - Facilitates the transfer of posture assessment information by routing messages between an endpoint and server

NEA PT-TLS\textsuperscript{1}

- Protocol to transport posture information between the endpoint and server using TLS

- Alignment (3 – Strong alignment with SACM)
  - Highly extensible, lightweight, and compatible with TNC IF-T TLS\textsuperscript{2}
  - Provides authentication, integrity, and confidentiality of data in a content-agnostic way
  - Provides an authenticated endpoint identity

- Potential changes
  - Could be used in SACM without any changes

- Priority (HIGH)
  - Ensures that posture assessment information is carried over a secure communication channel

2. http://www.trustedcomputinggroup.org/resources/tnc_ift_binding_to_tls
TNC SWID Message and Attributes for IF-M

• Extension of the TNC IF-M protocol to support the exchange of ISO Software Identification (SWID) tags

• Alignment (3 – Strong alignment with SACM)
  • Contains IPR, but, TCG Board amenable to transfer
  • Satisfies key use cases (software inventory, vulnerability management, etc.)
  • Supports near real-time change detection

• Potential changes
  • Could be used in SACM without any changes
  • Need to determine if it contains all of the relevant metadata

• Priority (HIGH)
  • Software inventory data is critical to achieve SACM’s use cases

1. http://www.trustedcomputinggroup.org/resources/tnc_swid_messages_and_attributes_for_ifm_specification
TNC IF-IMC\textsuperscript{1} / IF-IMV\textsuperscript{2}

- Standard interfaces by which Posture Collectors can interact with a Posture Broker Client and Posture Validators can interact with a Posture Broker Server

- Alignment (3 – Strong alignment with SACM)
  - Contains IPR, but, TCG Board amenable to transfer
  - Provides standard interfaces that are extensible and platform and language independent
  - Allows for the easy addition and removal of Posture Collectors and Posture Validators

- Potential changes
  - Remove out-of-scope capabilities
  - Examine the state machine regarding the transmission of messages

- Priority (HIGH)
  - Reduces the level-of-effort to develop and deploy Posture Collectors and Posture Validators

1. http://www.trustedcomputinggroup.org/resources/tnc_ifimc_specification
TNC Server Discovery and Validation

• Provides endpoints with a mechanism to discover servers and determine if they are trusted

• Alignment (2 – Good alignment with SACM)
  • Contains IPR, but, TCG Board amenable to transfer
  • Extensible to support new types of servers, identifiers, and trust parameters

• Potential changes
  • Support additional server types
  • Align identifiers with the SACM Information Model
  • Extend to support role and context based authorizations

• Priority (MEDIUM)
  • Needed by SACM, but, not as critical as transport protocols

1. http://www.trustedcomputinggroup.org/files/resource_files/3D59FB5E-1A48-8294-DDF322A08B48E02E/Server_Discovery_And_Validation_v1_0r19-PUBLIC%20REVIEW.pdf
NEA PT-EAP\textsuperscript{1}

• Protocol that carries posture assessment messages over an Extensible Authentication Protocol (EAP) tunnel

• Alignment (1 – Poor alignment with SACM)
  • Highly extensible, lightweight, and compatible with TNC IF-T EAP\textsuperscript{2}
  • Provides authentication, integrity, and confidentiality of data in a content-agnostic way
  • Provides an authenticated endpoint identity
  • Focuses on communication prior to an endpoint joining the network

• Potential changes
  • Could be used in SACM without any changes

• Priority (LOW)
  • Network access control is currently out-of-scope for SACM

Recommendations

• Adopt PA-TNC, PB-TNC, and PT-TLS (NEA protocol stack)

• Adopt TNC SWID Message and Attributes for IF-M (if PA-TNC is adopted)

• Adopt TNC IF-IMC and IF-IMV (if PA-TNC and PB-TNC are adopted)

• Adopt TNC Server Discovery and Validation (if PB-TNC is adopted)

• Do not adopt PT-EAP
Next steps

• Determine if there is consensus around adopting ECP specifications for endpoint self-reporting use case
  • Begin work adopting ECP specifications into the SACM Architecture

• Prepare a transition plan for the TCG Board