Endpoint Compliance Profile

IETF 95

04/06/2016

Agenda

- Status
- Overview
- Discussion
- Next steps

Status

- Discussed ECP[1] at the last SACM Virtual Interim Meeting[2]
    - Alignment with SACM Use Cases[3], Architecture[4], IM[5,], and Vulnerability Assessment Scenario[6]

- Haven’t received feedback to revise ECP out of the SACM Virtual Interim Meeting or on the list

- Recently posted a message[7] to the list asking if we should remove the requirements around IF-IMC[8] and IF-IMV[9]

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

[2] https://datatracker.ietf.org/doc/slides-interim-2016-sacm-2-5/

[3 - 6] https://datatracker.ietf.org/wg/sacm/documents/

[7] http://www.ietf.org/mail-archive/web/sacm/current/msg03894.html

[8] http://www.trustedcomputinggroup.org/files/static_page_files/1D8C8F15-1A4B-B294-D0CD725393CC0A93/TNC_IFIMC_v1_3_r18.pdf

[9] http://www.trustedcomputinggroup.org/files/resource_files/DDBC5979-1A4B-B294-D053EAAC35001F96/TNC_IFIMV_v1_4_r11.pdf

Overview

- ECP 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)[1] 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. http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670

What we changed in ECP

- Converted TNC terminology to NEA terminology where appropriate
  - TNC => NEA, IMC/IMV => PC/PV, etc.
- Generalized remediation capabilities to "follow-up actions" and generalized TPM to "cryptographic hardware module"
- Removed references to PT-EAP
  - Want to focus on endpoints already connected to the network

How does ECP fit into SACM?

- ECP is a little different than other IETF documents
  - While normative, it does not define a specific data model or protocol

- The value of ECP is that it demonstrates how to use various solution I-Ds to solve a specific scenario in SACM

Remove requirements around IF-IMC/IF-IMV

- On 3/7, we submitted numerous solution I-Ds (ECP, SWID M&A, OVAL)
  - Wanted to follow up with IF-IMC, IF-IMV, and Server Discovery and Validation[1]
  - However, it may be better to delay these other I-Ds in order to focus on what was already submitted

- Do we want to remove the requirements around IF-IMC/IF-IMV from ECP?
  - PCs/PVs MUST conform to IF-IMC/IF-IMV
  - Use of IF-IMV to extract endpoint identity information from a machine certificate sent over PT-TLS

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

Next steps

- Update ECP based on discussion

- Request a call for adoption on ECP

- Continue to develop solution I-Ds that support ECP