Comments to the SCAP_Messages_For_IFM_v0_16.pdf

First of all, I thank you for the opportunity you give me to put in my two cents to this effort. I am basing my input on the presentation that Charles Schmidt gave on Fri 5 Sep 2012 during the IT Security Automation conference in Baltimore.

1. To an SCAP audience, some of the terminology is not defined and not as easy to follow. Suggest including a glossary at the end to familiarize the SCAP audience.
2. The term integrity as used in paragraph 1.1 "that enforces network operators to enforce policies regarding endpoint integrity when access granting access to a network infrastructure" is not clear. Perhaps the paragraph should read "that facilitates network operators to query and enforce policy regarding endpoint security state in terms vulnerabilities, configuration, patching, and inventory tracking when determining to grant access to a network infrastructure."
3. Is integrity in the IF-M model the same notion as the integrity defined in NIST IR 7802 (Trust Model Security Automation Data, or TMSAD) that is part of SCAP 1.2? The trusting security objective of TMSAD appears to be in line with the objectives the MD5 usage, but the TMSAD is more complete.
4. The document identifies some specifications from SCAP 1.2 (Waltermire, Quinn, Scarfone, & Halbardier, 2011), but not others. The document does not include Asset Identification (AI) and Trust Model Security Automation Data (TMSAD).
5. The use of OCIL is not explained.
6. If MD5 Hash is used, how will this work when TMSAD is used? The MD5 uses 128 bits, but TMSAD uses the 256, 384, or 512 versions of the SHA (Booth & Halbardier, 2011, p. 8)
7. Applicable to CPE, perhaps it is a good idea to mention the Official CPE dictionary as the authoritative mechanism for de-conflicting identifier names (Cichonski, Waltermire, & Scarfone, 2011, p. 1). Furthermore, it is highly likely that organizations will create extended dictionaries as explained in IR 7697. The IR 7697 CPE 2.3 specification states "For example, "an organization may have to create identifier names for proprietary products that are only useful within that organization" (Cichonski, Waltermire, & Scarfone, 2011, p. 1).

Statistical comment

The probability of the supplicant passing one (1) test is ½ (pass or fail) or 50%. The probability of a supplicant obtaining access to an infrastructure expecting compliance with N requirements is (1/2) to the Nth power, or (1/2)** N where N is the number of tests. For a supplicant requesting access to an infrastructure that requires ten (10) tests, the probability of getting accepted is (1/2)**10, which is 1/1024. This means that devices requesting access to an infrastructure expecting compliance with ten or more requirements have less than on in one thousand chances to be accepted. If this is the idea behind "absolute result" (an IMC can only send the IMV an absolute result as paragraph 1 on page 33 indicates) then accessing the infrastructure will be extremely rigid. The impact of this approach is that, potentially, some implementors and organizations will reject it because it is too rigid.

References

Booth, H., & Halbardier, A. (2011). *IR 7802, Trust Model for Security Automation Data 1.0 (TMSAD).* National Institute of Standards and Technology.

Cichonski, P., Waltermire, D., & Scarfone, K. (2011). *IR 7697 - Common Platform Enumeration : Dictionary Specification Version 2.3.* National Institute of Standards and Technology.

Waltermire, D., Quinn, S., Scarfone, K., & Halbardier, A. (2011). *SP 800-126 Rev 2 - The Technical Specification for the Security Content Automation Protocol (SCAP) SCAP version 1.2 (Draf).* NIST.