Assessment Results Format

Abstract

Assessment Results Format (ARF) is a proposed open specification for exchanging security assessment results and device inventories of IT assets. The ARF specification describes how to create ARF instance documents and describes what must be placed in each field for the document to be considered valid. Accompanying XML schemas describe the structure of an ARF instance document and how it should be encoded in XML. ARF is currently managed by the Department of Defense Computer Network Defense Research & Development Program Management Office (CND R&T PMO), with MITRE performing current development under their direction.

December, 2010

John Wunder, MITRE
Jon Baker, MITRE
Lieutenant Colonel Joe Wolfkiel, Computer Network Defense Research & Development Program Management Office

Scope

ARF belongs to a suite of specifications that enables the reporting of assessments of IT assets in an enterprise environment, known collectively as security automation interfaces. Once completed, the security automation interfaces specifications will describe an end-to-end process for delivering assessment content to network sensors or data stores, requesting assessments against that content, reporting on the results of those assessments, and aggregating assessment results at the local enclave and enterprise levels. See the forthcoming security automation interfaces whitepaper for further description of each of the pieces of the suite and how they interact.

Based on the identified use cases (see below), Assessment Results Format (ARF) is scoped to include a specification for reporting detailed information on inventory, configuration, vulnerability, compliance, and other security assessments of one or more IT assets and accompanying metadata (including organization, location, people, and replication). It does not describe how the information inside an ARF document should be collected, how ARF documents should be transported, or when and where ARF producers should send ARF documents. Other specifications in the security automation interfaces suite, notably the Policy Language for Assessment Results Reporting (PLARR), include mechanisms for the request and transport of ARF documents.

Technical Use Cases

The following tentative technical use cases for ARF were identified based on current and proposed capabilities in enterprise environments. Although ARF may currently provide capabilities beyond the following use cases and ARF may be useful for other purposes, the immediate focus of ARF is meeting these use cases.

1. Report the results of an assessment of one or more IT assets against a Security Content Automation Protocol (SCAP)[1] content stream as defined by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-126.
2. Report the results of a device inventory of platforms, configurations, patches, and/or vulnerabilities in the absence of an SCAP content stream for one or more IT assets.
3. Report operational context metadata for one or more IT assets

Community

The primary implementers of ARF will be assessment tool vendors that produce ARF documents and asset databases, security information managers, or other asset managers that will consume ARF. The

[1] Per NIST SP 800-126 (Stephen Quinn, David Waltermire, Christopher Johnson, Karen Scarfone, John Banghart): "The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information."

end users of these products are the primary drivers behind capabilities and use cases while the product developers themselves are the primary drivers behind technical implementation details.

Format

The ARF specification includes text documentation on how ARF documents must be constructed, XML schema documents describing the format and validation of ARF documents, and a data dictionary that provides detailed explanations about the meaning of each field.

The major sections of an ARF document are, for each IT asset:

- Device Inventory
  - Vulnerabilities (using CVE[2])
  - Configuration items (using CCE[3])
  - Software (using CPE[4])
  - Patches
  - OVAL[5] results
  - XCCDF[6] results
- SCAP Assessment Results
- Assessment Metadata
- Organization Record (owning organization)
- Person Record (point of contact)
- Network data
- Physical Location
- Other operational attributes

Distribution

ARF has been submitted to NIST as an emerging SCAP specification by CND R&T PMO. MITRE, in coordination with CND R&T PMO, will continue to develop the specification to meet both sponsor

---

[2] Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures.
[3] Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues.
[4] Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms, and packages.
[5] Open Vulnerability and Assessment Language (OVAL) is an information security community standard to promote open and publically available security content, and to standardize the transfer of this information across security tools and services.
[6] The Extensible Configuration Checklist Description Formation (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents.

requirements and, primarily, the needs of the enterprise reporting community. In particular, MITRE will begin a community involvement effort in order to encourage adoption while updating the specification per community feedback.

Outreach

MITRE will perform in-person outreach by holding talks at security conferences and hosting sessions at developer days, as well as performing one-on-one interviews with interested parties.

Online, MITRE will host an ARF page on the Making Security Measureable Incubator site. This will point to an Enterprise Reporting mailing list for combined feedback and discussion on ARF, Assessment Summary Results (ASR), and PLARR as well as an arf@mitre.org e-mail address for direct feedback to the team.