Automation Content Repositories

Distributing SCAP

Kent Landfield

Purpose

Today we have created a standardized content format used by multiple SCAP tools from multiple vendors. What we have not addressed is the actual distribution of standardized content.

Organizations are developing, customizing and tailoring content without a means to distribute, reuse and manage it.

For larger sites with multiple SCAP products, changes to content can be painful in assuring all the SCAP products are using and reporting on the same content.

This interactive discussion will focus on defining requirements for creating a standardized means for accessing and distributing content from a central service within an organization.

Current Content Issues

- Ownership
  - Confusion around centralized repositories
  - Is the content authoritative?
  - Is this content really ready to be used or still under development?
  - What content should I run for what situation?
  - How come some vendors include others peoples content in their product and some don't.
- Support
  - Who owns the content?
  - Who do I call for support for content issues?
- Location
  - Where do I find a benchmark for my specific platform or need?
  - Is there anyway to see what those outside my organization have created?
  - If I want to build a benchmark do I need to write all the checks myself?

And …. What's a CPE? Do customers really need to know?

Product Approaches to Distributing Content

- Retrieve them yourself
  - From NIST
  - From Vendors (OS/Product)
- Vendors bundling government developed content
  - Questionable…
- There has got to be a better way…

Today's Reality

- Repositories:
  - NIST Repository
  - MITRE OVAL Repository
  - OS Vendor Repositories
  - Product Content
- Content integrity validation missing
- No way to prove authenticity
- Kludgy ways for an organization distribute the same SCAP content to multiple SCAP validated products on the same network
- Vendors have their proprietary way (or no way) of doing this in an enterprise

Wasn't the goal of SCAP to provide standardized content between products? While the internals work, the distribution does not.

Repository Directions

- More authoritative ownership
  - Vendor Hardening guides
  - Software and Hardware products providing per product configurations
  - Guidance Authors will understand the benefits of actionable content

- Decentralized content availability
  - No longer solely a NIST Checklist focus
  - Yes, this is a good thing

- Commercial content a possibility
  - Availability for subscription or specific use cases

Organizational Distribution Problem

- Large organization (insert an agency or Fortune 500 name here) has multiple SCAP validated tools in their environment with many different sites and departments
- Tools they own are a mixture of point products and enterprise tools
- The organization wants to create their own SCAP-based site security policy which they would like scheduled to run weekly
- Each time they make a change they need to go to each of their tools (and potentially systems) and update the content
- Extremely laborious and time consuming from a staffing perspective…

Guidance Author Distribution Problem

- An organization develops a set of benchmarks and the associated checks that target a specific set of guidance for which they are authoritative for

- They want to maintain control over the content and its distribution to assure they can update the content rapidly as needed to support their community

- They want to be able to widely distribute updated content quickly to assure their community is using the most current guidance

- Do not or cannot rely on an external organization to facilitate the distribution of their content

Content Location / Version Problem

- Standardized Content is available from many sources
- User community has no means to be made aware of what content is available to be used in their SCAP enabled products
- No means to search for the desired content
- Users feel they need to create their own because they do not know where to go find what they need
- Extremely laborious and time consuming from a searching / finding perspective…
- Then when they do find what they are looking for, they have to manually continually monitor the location for any updated versions

So what is needed ?

Need a means:

- To allow content to be distributed globally via automated means and not via manual means
- For guidance authors to be able to register their content as authoritative and publish that content so it can be retrieved and used by the interested or affected community
- For organizations to be able to locate new content and track existing content for updated versions
- For different SCAP products within an organization to be able to retrieve the organization’s approved content to be used in evaluating the state of the local network
- To assure the content being retrieved is the guidance author’s approved version
- To be able to identify the support contact information if issues are encountered with the retrieved content
- To manage the registration process at a global level
- To manage the organizational repository

Pieces and Parts

- Global Registry
  - Management
  - Registration
  - Querying
- Authoritative Repository Servers
  - Injecting Content
  - Registering
  - Retrieval
  - Organizational information
  - Querying
- Organizational Servers
  - External Content Cache
  - Identification of default content to be used
  - Querying
  - Injecting Content
  - Retrieval
- What do these pieces look like?

Global Registry

- Global Registry of Authoritative Content Repositories
  - Root server – Index of repositories
  - Does not contain any content, just information about where to get authoritative content published by others
  - Repository Record
    - Content ID
    - Type of Content
    - Content Name
    - Content Tags
    - Content Version
    - TTL
    - Location of Authoritative repository
    - Organizational Record
      - Organization Name
      - Support Email Address
      - Support Phone Number (optional)
      - Support Web Site (Optional)

……Lots missing here – for discussion only…..

Authoritative Content Servers

- Authoritative Content Servers
- Holds the actual authoritative content to be retrieved
  - Injection
    - Content Validation
    - Signing injected content
    - Version information
    - TTL
    - Authoritative Contact
    - Support Contact information
      - Organization
      - Issue Submission Address
  - Registering content as authoritative
      - Local registry
      - Submission to Global Registry

Organizational Content Servers

- Exists on local network
- Could be set up in a hierarchy in the organization if needed
- Holds the actual content to be retrieved by the SCAP products or Content development tools
- Can be an authoritative server for local organizational or site security policy content
  - Can be authoritative within the organization without registering with an external repository index
- Caching server for external content
- Manages the content allowed or required to be retrieved within the organization
    - What is the default to be used? How do we indicate that, by platform, subnet, ? Do we need to at all?
- Querying
- Injecting Content at a component or package level

Roles and Uses

- Global Repository Administrator
- Guidance Authors / Authoritative Content Publishers
- Organizational Repository Administrator
- Site Ops/Security staff creating / tailoring local content
- Content Distribution to deployed SCAP products
- Content Development Tools

Discussing Repository Models

- Package based retrieval
  - Everything in one package to run a specific benchmark/policy
    - Checks
    - Benchmark
    - CPE support
  - Benefit
    - Consistent content a single entity
    - Ease of verification

- Component based retrieval
  - Menu based approach
    - Individual content potentially retrievable from multiple repositories
    - Checks from potentially multiple repositories
  - Benefits
    - Reuse of content

What content are we going to distribute?

- SCAP complete packages
  - Benchmarks
  - OVAL
  - OCIL
  - CPE
  - Other?

- Individual access to specific components

- Provide a means to introduce new content types?

- How might that occur?

Content Confidence

- Content integrity validation
  - Simple hash ?
  - Encrypted capabilities
- Proving authenticity
  - Certificate use?
- At what level should we focus these concerns?
  - Package
  - Component
  - Both?

Supporting Subscription Model

- Guidance Authors sell their guidance documents today
- Content could be distributed as a subscription service
- While maybe not initially, is this something we want to support ?

Where do we go from here?

- Discussions on emerging-specs? Or specific list ?
- Form a working group around developing this
- Effort more focused on fast prototyping and then document the prototype?
- Is there interest in participating?