CCE Analysis and Semantic Techniques

Matthew N. Wojcik

MITRE

CCE: A quick review

- CCE is the Common Configuration Enumeration
- Standard enumeration of security-relevant configuration controls
- Technical and platform-specific
  - Similar configuration controls on different platforms are assigned separate CCE IDs
- Does not assert a recommendation
- Allows fast, accurate correlation
  - Across repositories
  - By different groups of people
  - Between different tools

CCE Example

ID	CCE-2891-0
DESCRIPTION	The "Disable CTRL+ALT+Delete Requirement for Logon" policy should be set correctly.
PARAMETER	Enabled / Disabled
TECHNICAL MECHANISM	(1) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD (2) Computer Configuration/Windows Settings/Security Settings/Security Options/Interactive logon: Do not require CTRL-ALT-DEL
REFERENCE	NIST SP 800-68: Table: 5.28 Value: disabled

CCE Maintenance Challenges

- Federated content creation model
  - Contributors from various organizations
  - Need to maintain consistency
- Growing corpus
  - Now over 5250 entries
  - Need to have useful search
- Increasing workflow
  - 3000 entries added in the last 12 months
  - Some proposed edits (entry creation, descriptions) require more scrutiny than others (references, technical mechanisms?)
  - Need to have a streamlined process
- Lack of infrastructure
  - CCE lists traditionally presented and edited as spreadsheets
  - Need enhanced editing, tracking, and publishing capabilities

CCE Analysis and Semantic Techniques

- Semantic approaches show promise for machine-assisted human analysis of CCE submissions
  - Semantic infrastructure will “suggest” matches that humans can confirm or reject
- Does a submission address the same thing as something already in CCE?
  - CCE ID as inverse functional property
- Is it similar to an existing CCE?
  - Key terms and thesaurus, topic tags (non-canonical, but potentially extremely useful!)
  - We may need to update other CCE entries as well
- Who asserted what?
  - Reification may allow less stringent review of certain updates
- Added benefit: advanced users can build on CCE ontology