

Semantics Techniques for the Common Criteria

Wayne Stewart and Erin Connor
EWA-Canada
24 September 2009

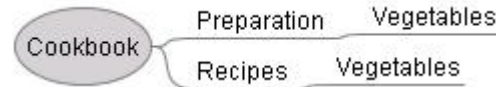
Your Trusted Partner

- **Semantic Tool**
- **Semantic Techniques for CC Documentation**
 - Collection Indexing
 - Modeling CC Requirements
 - Using Expert Models to Lift Relevant Info from Developer Documentation
- **Summary**

- **Kayvium Workbench and SDK**

- **Semantic Capabilities**
 - Model Guided Discovery
 - Search the Web or an Internal Collection for documents matching a model
 - Conformance Analysis
 - Compare and contrast two indexed document collections
 - Collection Indexing
 - Create a comprehensive index of a set of documents based on their content

- Kayvium uses mind maps to represent knowledge domains, for example:



- The central node is the model name, representing the domain
- The other nodes are concepts, or *themes*, representing what is known about the domain, e.g., Preparation, Recipes, Vegetables
- The links indicate relationships between the concepts
- Each complete path from the central node to a leaf node is called a “*dimension*”
- In the example, vegetables are linked to preparation instructions and recipes. Dimensions are Preparation of Vegetables, and Recipes including Vegetables.

Your Trusted Partner

Model Guided Discovery (2)

- **Create a model representing the search target**
 - As complex as it needs to be to find what you are looking for
- **Kayvium decomposes the model *dimensions*, conducts the search, then formats the results**
- **Results can be sorted by dimension, by web site, or by rank**
 - pages are ranked by the number of times a document is discovered across all *dimensions*

Ranked Pages	Detailed Pages	Ranked Websites	Workflow
<h2>Ranked Results Report</h2> <p>Model: Ranked Model Source: WindowsIndexingServicesCustomSearchEngine, 8/31/2009</p>			
Dim	ds_SLES EAL3 ST		
582	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\redhat security target ea3 v1-6 as.pdf		
558	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\redhat security target ea3 v1-6 ws.pdf		
522	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\redhat security target ea4 v2-7-nocb.pdf		
324	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\sleshd-ea3-2.25.pdf		
320	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\sleshd-110.pdf		
306	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\rhel-4-hl-v2.13.pdf		
288	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\sleshd-ea4.pdf		
266	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\ibm-sles-eal4-configuration-guide.pdf		
205	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\rhel3 high level design.pdf		
177	ibm linux security no st\documents and settings\kayvium dev1\desktop\ibm linux security no st\rhel-capp-eal4-ibm-configuration-guide-v1.14.pdf		

Dimensions: 324
 .../Access permissions /DAC/mechanisms/actions
 ... /Access permissions /DAC /mechanisms/DA.1
 ... /audit records/accounts
 ... /audit records/amount
 ... /audit records/TSF such/network/nonTSF software
 ... /audit records /TSF such /network/TOE software
 ... /audit records /TSF such/objective
 OE.HW.SEP/approval
 ... /audit records /TSF such/Software/A.PROTECT
 ... /audit records /TSF such /Software/hard
 ... /CAPP /applications/sufficient/ATTRIBUTE
 ... /CAPP/control/Access/privi

Conformance Analysis

- **Compares and contrasts results of indexing two document sets**
- **Can be used to display a summary page with statistics of the match**
 - e.g., the number of matching themes from two document sets.
- **Provides detailed lists of common and unique themes and relationships**

Your Trusted Partner

Kayvium GAP Analysis

Policy: IBM Linux Security no ST

Domain: SLES EAL3 ST

9/3/2009 8:06:51 AM

Model	Matches		Gaps		Total	
	Theme	Relationship	Theme	Relationship	Themes	Relationships
IBM Linux Security no ST	566 (4%)	79 (0%)	12566 (96%)	25387 (100%)	13132	25466
SLES EAL3 ST	566 (79%)	79 (8%)	144 (21%)	855 (92%)	710	934

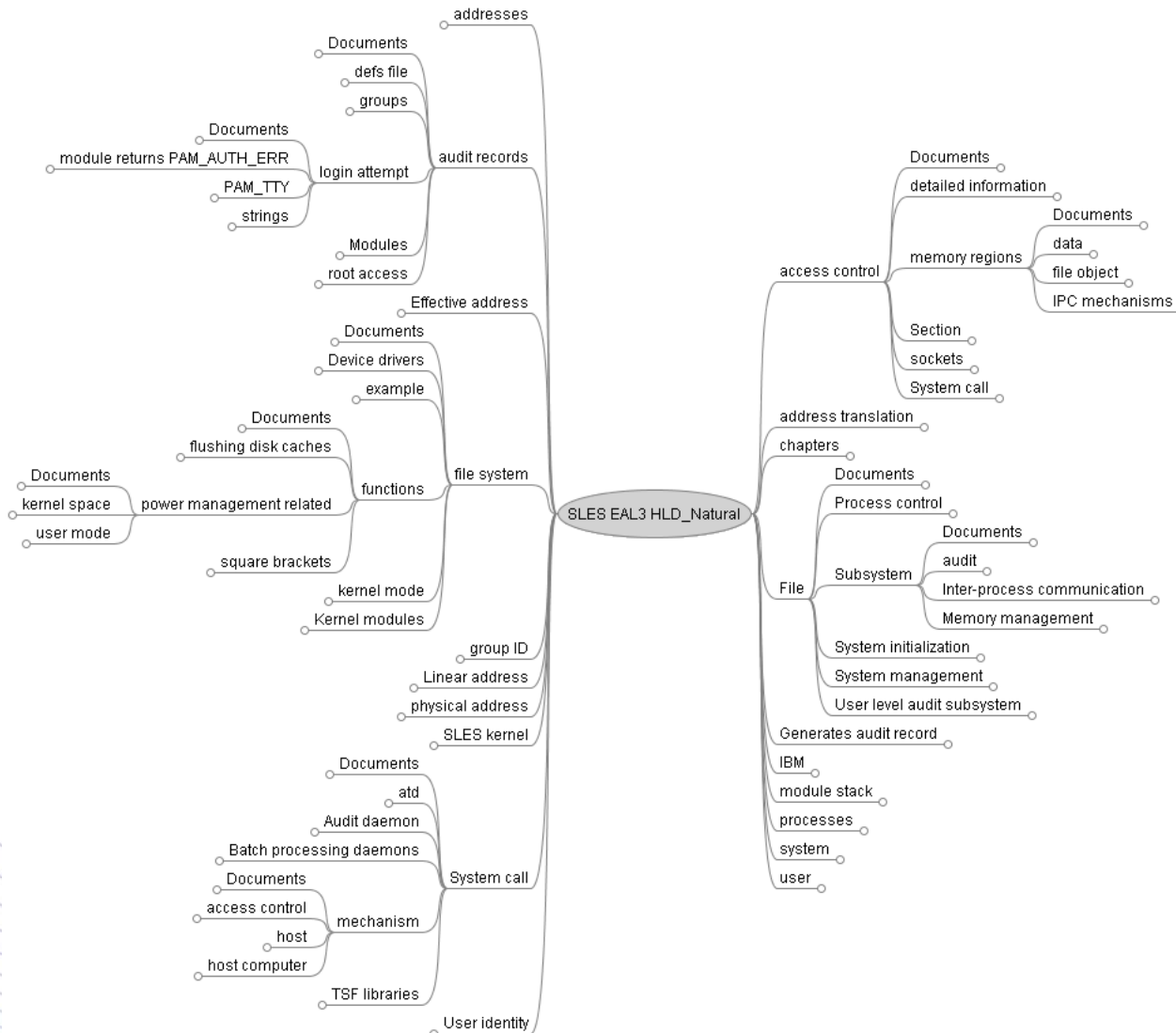
Your Trusted Partner

- **A set of one or more documents**
 - Text, MS Word, pdf, html
- **Imported from a folder on the host operating system**
- **Documents may be added to a collection over time**
- **Examples:**
 - the set of developer documentation for a CC evaluation
 - the CC Parts 1 to 3 and CEM, etc.

- A representation of the *themes* found in a collection. A theme is a concept of interest from the documentation set.
- The themes form a structured hierarchy, with root themes identifying the most prominent concepts.
- Themes provide links into the documents that can be followed down to the paragraph level.
- Indexing parameters and options allow for tailoring the index for specific applications (e.g., analysis of developer documentation).

- **Natural Index is the themes extracted from the source documents without user bias**
- **It is a taxonomy represented by a hierarchical collection of the themes found**
- **It is rendered as a mind map with links to the source documents**

Natural Index (2)



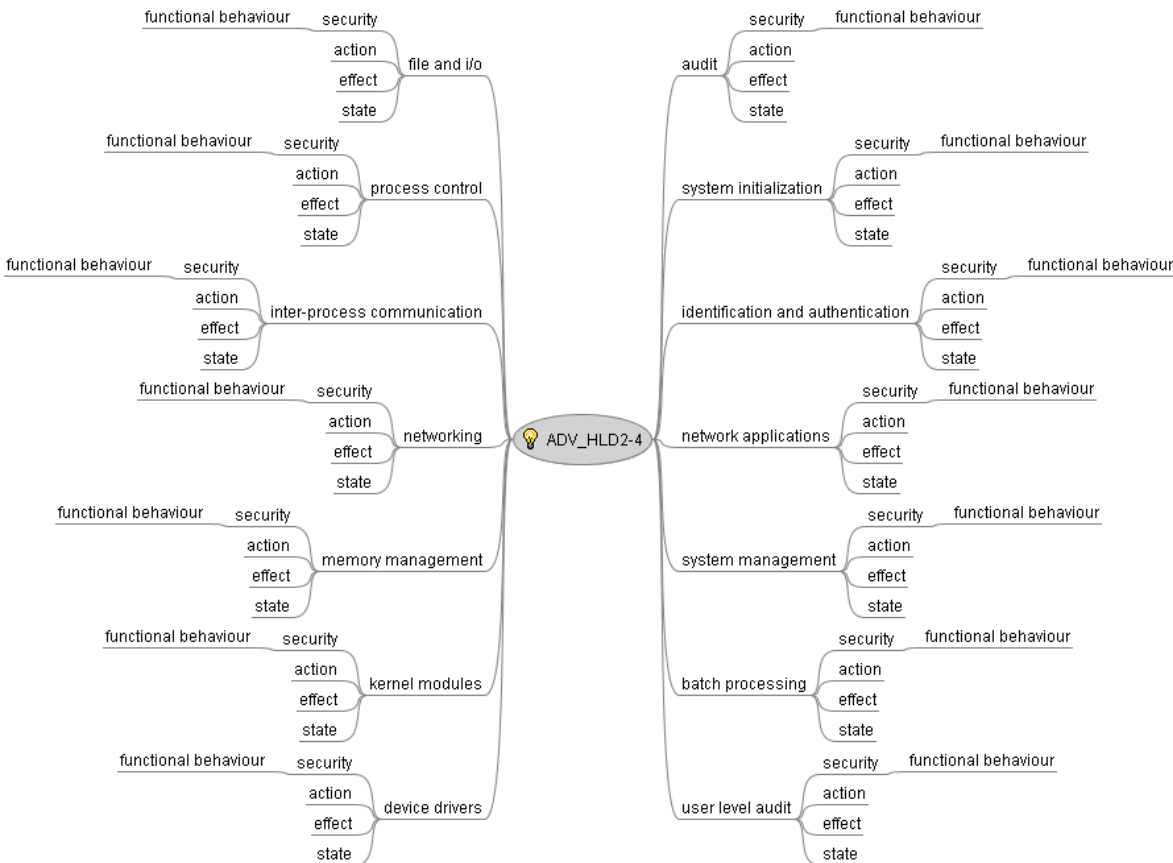
- Natural index of *SuSE Linux Enterprise Server High Level Design*, generated with Kayvium
- Leaf nodes provide link(s) to the document(s) in which the theme was found

Your Trusted Partner

Expert Model Lifting

- **Expert Model is a mind map which represents knowledge modeled by a subject matter expert**
- **Expert Models may be:**
 - rarely just a collection's natural index,
 - developed manually by a subject matter expert, or
 - produced iteratively using a combination of automated and manual techniques.

Expert Model Lifting (2)



- Expert Model depicting ADV_HLD.2-4 requirements from the CEM v1.0
- Based on subsystems identified in *SuSE Linux Enterprise Server High Level Design*

Your Trusted Partner

Expert Model Lifting (3)

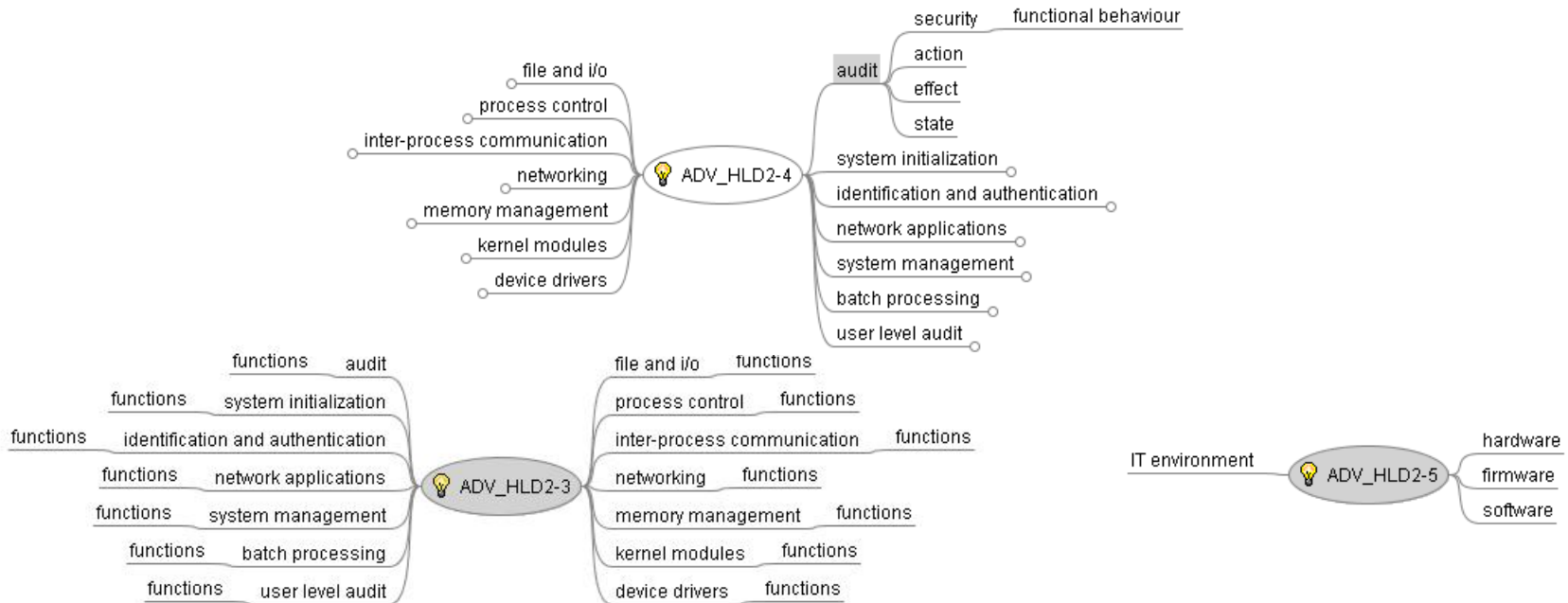
- **Expert Model *lifting* is the generation of a collection index focusing exclusively on the themes presented in an Expert Model**
- **Lifted index may include the context from the original documentation where the Expert Model relationships were found**
 - The context can be used by the user to determine the applicability of the instance of the lifted theme
- **Applications to developer documentation review?**
 - Use a combination of CC requirements, the CEM, and the ST to create Expert Models which describe the evaluation criteria for developer documentation

Your Trusted Partner

- **Sample data set:**
 - SuSE Linux EAL3 CC evaluation documentation, publicly available online
 - CEM v1.0
 - CC v2.1
 - Focus on ADV_HLD requirements, for proof of concept demonstration
- **Use the CEM and SuSE documentation to produce Expert Models describing the HLD evaluation criteria**

Modeling CC Requirements (2)

- **Goal: To produce Expert Model templates that can be used with Expert Model Lifting to generate document indexes that aid in the evaluation of developer documentation.**



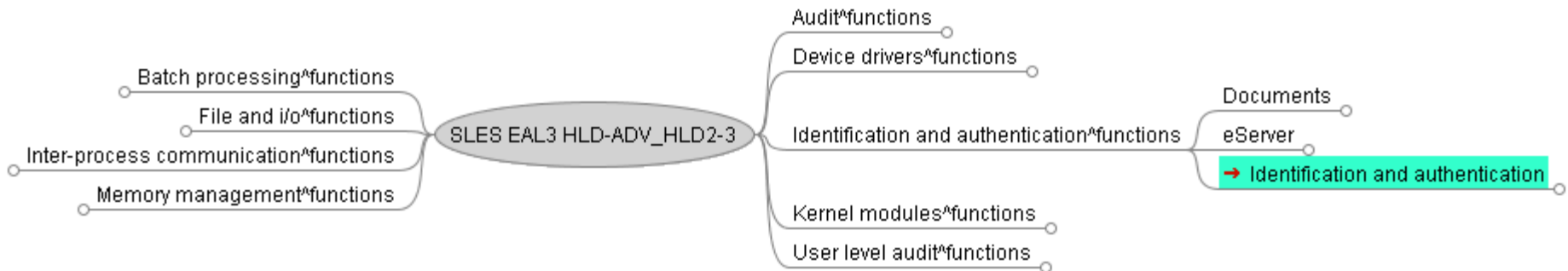
Your Trusted Partner

Lifting Relevant Info from Developer Documentation

- **An expert model is created to describe each evaluator action**
- **A collection is created containing the relevant developer documentation.**
- **The collection is indexed with Expert Model lifting enabled.**
- **The lifted results are examined and used by the evaluator to complete the evaluator actions**

Lifting Relevant Info from Developer Documentation (2)

- Lifted index of *SuSE Linux Enterprise Server High Level Design*, using Expert Model for ADV_HLD.2-3



Your Trusted Partner

- **Collection indexes provide improvements to the initial understanding of complex document sets**
- **Comprehension and correlation between multiple documents is improved with natural indexes**
- **Expert Model Lifting can be used to target the knowledge extraction**
 - Allows the user to focus on topics of interest, e.g., Evaluator Action Elements
 - The automated targeting of Evaluator Action Elements using Expert Model templates allows the evaluator to rapidly explore developer documentation in the context of specific CC requirements

- **Expert Model templates, describing evaluator action elements are in development**
- **An application using the Kayvium SDK (which provides direct access to the underlying semantic operations) is in development**
 - The application is designed to facilitate the document analysis workflow
 - The application uses the Expert Model templates, allowing for customization of the models to assist in the evaluation of different CC projects.

Questions



Erin Connor
Director
+1-613-230-6067 x1214
econnor@ewa-canada.com

Your Trusted Partner