Delivering the Right Assurance

Application of Semantic Techniques to CC Problems

Erin Connor, Mark Gauvreau, and Samuel E. Moore

EWA-Canada

20 September 2006

Presenter: Mark Gauvreau (mgauvreau@ewa-canada.com)

Your Trusted Partner

Overview

- Introduction To EWA-Canada
- Semantic Tool – Kayvium Desktop
- Application of Tool Functions to CC Tasks
  - Model-Guided Searches
  - Knowledge Extraction
  - Conformance Analysis
- Summary

- Note: This is a Work in Progress, not a final analysis of the CC-relevant capabilities of the tool.

Introduction to EWA-Canada

- What we do
  - Lab
    - Common Criteria Evaluation – Canadian Scheme
    - FIPS 140-2 Cryptographic Module Testing – CMVP
    - Point of Sale Terminal & Encrypted PIN Pad Certification
      - Interac Financial Services Network
      - Payment Card Industry PED
      - Payment Terminal Security (PoS Terminals)
  - Documentation Development Assistance to Vendors
  - Managed Security Services
  - Information Assurance Consulting
  - Site Security Audit and Vulnerability/Penetration Testing

Semantic Tool

- Kayvium Desktop
  - Kayvium Corporation www.kayvium.com
- Semantic Tool Type: Unstructured Data Analysis
- CC-Relevant Semantic Capabilities
  - Model-Guided Searches
    - of the Internet
    - of an Internal Collection
  - Knowledge Extraction
    - From Single Documents
    - From Collections of Documents
  - Automated Conformance Assessment

Potential Applicability to CC Tasks

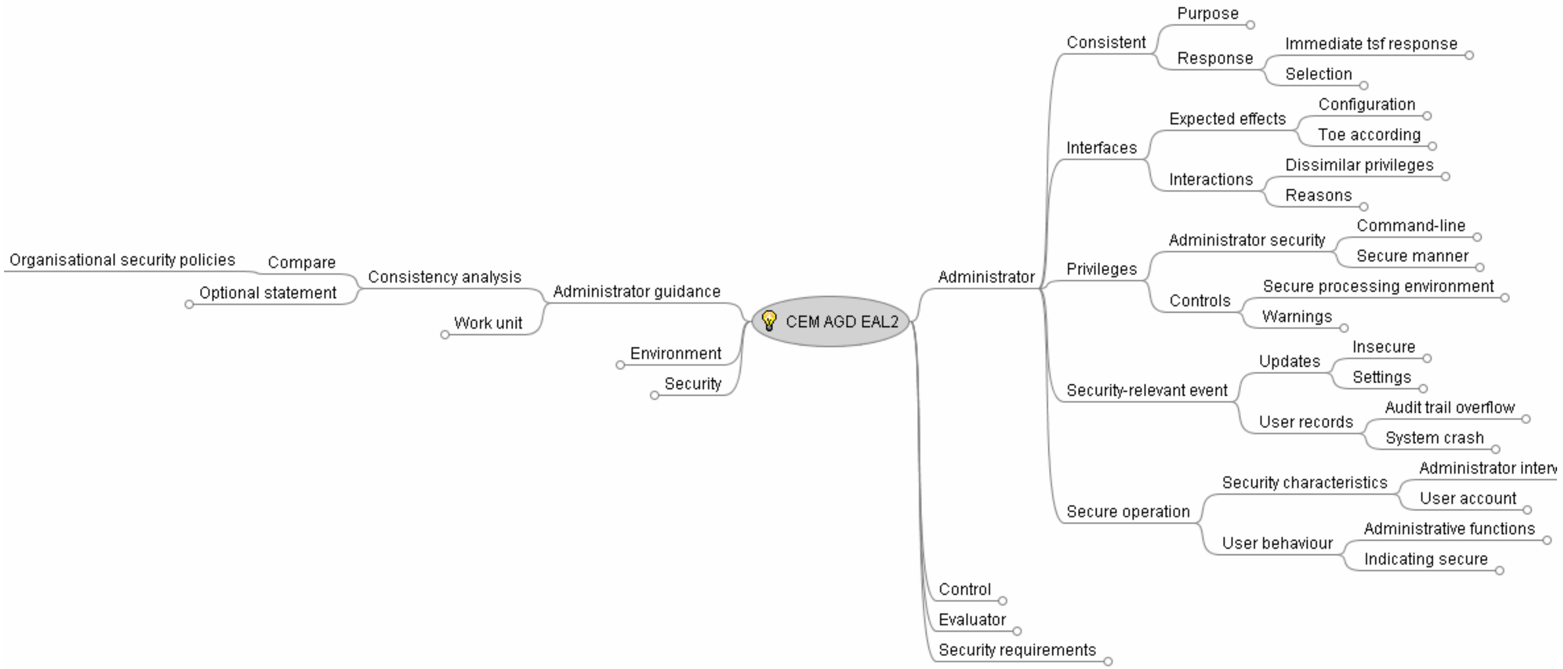
- Model-Guided Searches
  - Where, in the suite of developer documentation, do I find the specific information I'm looking for?
- Knowledge Extraction
  - How do I correlate the information found in the developer documentation?
- Automated Conformance Assessment
  - How can we reduce the labour involved in a CC assessment?
  - Can we do a "quick look" at documentation to see what security functions are supported?

Model-Guided Searches

- Start with a Mind Map Model
- Run the Model against a set of documents
  - Internet
  - Local repository
  - Local collection
- Themes in model are recast as search phrases
- Results presented as a Mind Map with links to relevant documents
  - Examples follow, based on the CEM AGD section at EAL2, applied to the IBM Linux Security Documentation, publicly available on the Internet

Model-Guided Searches (Model)

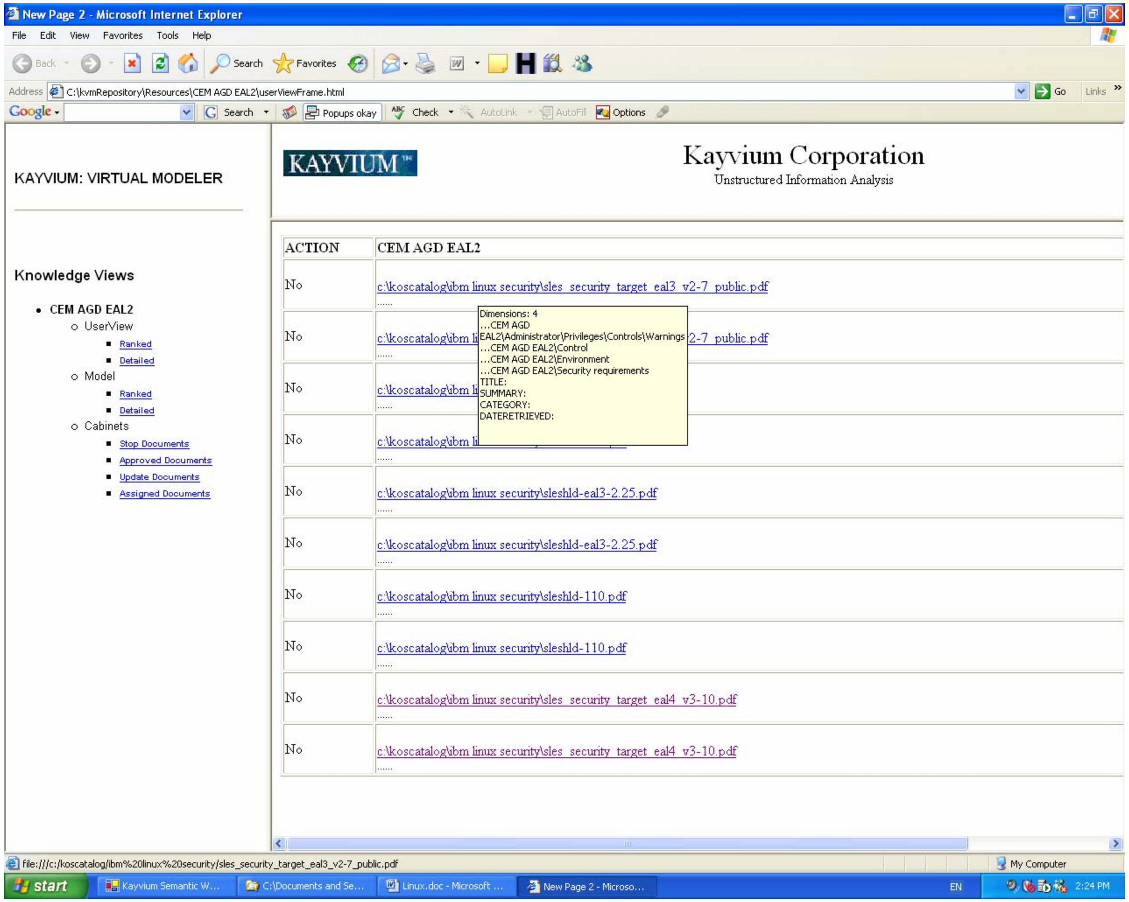
- Auto-Generated Search Model
  - using FreeMind to display the results



EWA

Delivering the Right Assurance

Model-Guided Searches (Ranked Results)



Address C:\kvmRepository\Resources\CEM AGD EAL2\userViewFrame.html

Kayvium Corporation

Unstructured Information Analysis

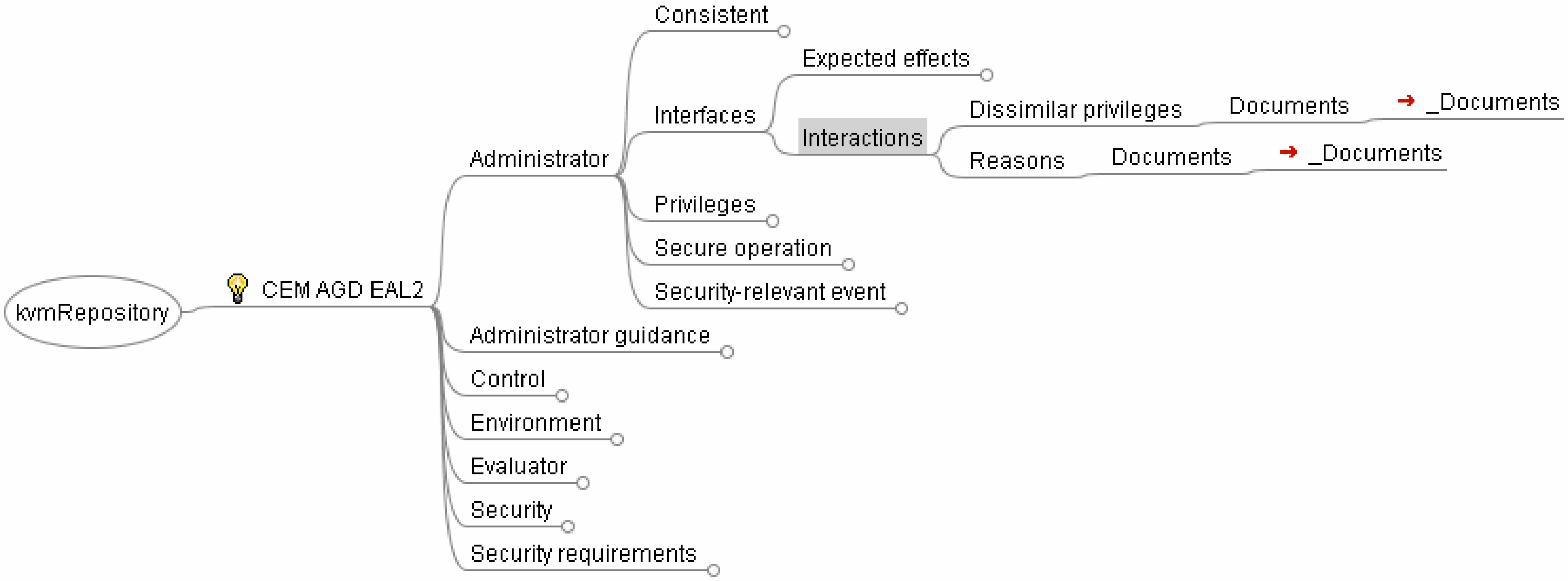
ACTION	CEM AGD EAL2
No	c:\koscatalog\ibm linux security\sles_security_target_eal3_v2-7_public.pdf ......
No	c:\koscatalog\ibm li 2-7_public.pdf ......
No	c:\koscatalog\ibm li ......
No	c:\koscatalog\ibm li ......
No	c:\koscatalog\ibm linux security\sleshld-eal3-2.25.pdf ......
No	c:\koscatalog\ibm linux security\sleshld-eal3-2.25.pdf ......
No	c:\koscatalog\ibm linux security\sleshld-110.pdf ......
No	c:\koscatalog\ibm linux security\sleshld-110.pdf ......
No	c:\koscatalog\ibm linux security\sles_security_target_eal4_v3-10.pdf ......
No	c:\koscatalog\ibm linux security\sles_security_target_eal4_v3-10.pdf ......

Dimensions: 4
...CEM AGD EAL2\Administrator\Privileges\Controls\Warnings
...CEM AGD EAL2\Control
...CEM AGD EAL2\Environment
...CEM AGD EAL2\Security requirements
TITLE:
SUMMARY:
CATEGORY:
DATERETRIEVED:

file:///c:/koscatalog/ibm%20linux%20security/sles_security_target_eal3_v2-7_public.pdf

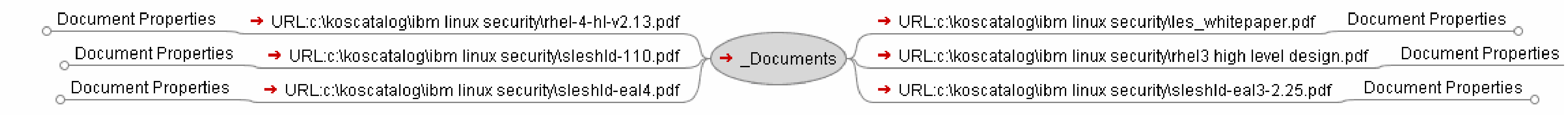
Your Trusted Partner

Model-Guided Searches (Results Related to Model)



- kvmRepository
  - CEM AGD EAL2
    - Administrator
      - Consistent
      - Interfaces
        - Expected effects
        - Interactions
          - Dissimilar privileges
            - Documents
              - ➜ _Documents
          - Reasons
            - Documents
              - ➜ _Documents
      - Privileges
      - Secure operation
      - Security-relevant event
    - Administrator guidance
    - Control
    - Environment
    - Evaluator
    - Security
    - Security requirements

Model-Guided Searches (Results Related to Model)



➔ _Documents

➔ URL:c:\koscatalog\ibm linux security\rhel-4-hl-v2.13.pdf — Document Properties

➔ URL:c:\koscatalog\ibm linux security\sleshld-110.pdf — Document Properties

➔ URL:c:\koscatalog\ibm linux security\sleshld-eal4.pdf — Document Properties

➔ URL:c:\koscatalog\ibm linux security\les_whitepaper.pdf — Document Properties

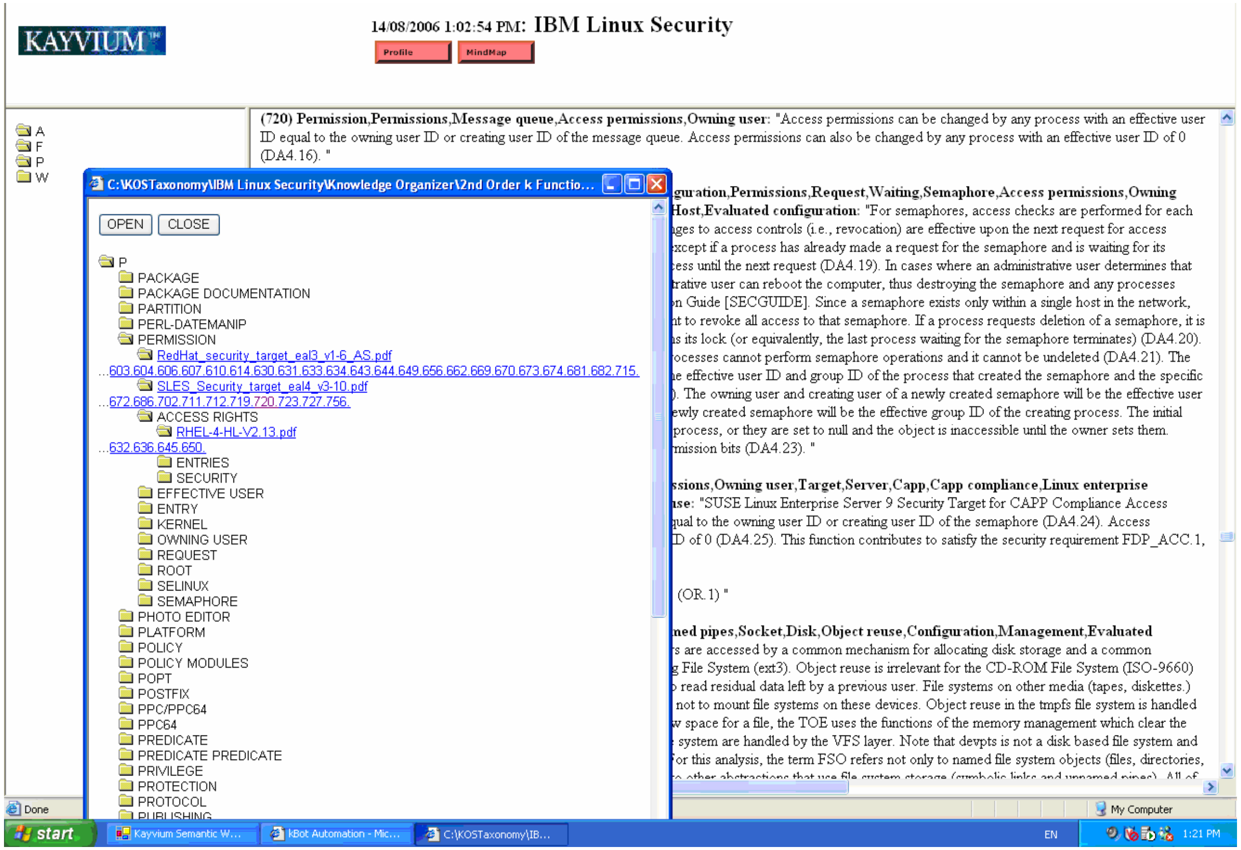
➔ URL:c:\koscatalog\ibm linux security\rhel3 high level design.pdf — Document Properties

➔ URL:c:\koscatalog\ibm linux security\sleshld-eal3-2.25.pdf — Document Properties

Knowledge Extraction

- Import directory to form collection
- Index Collection
  - Generates Kavium Learning Index (Internal)
  - Generates Taxonomy
    - Pointers to themes in documents
    - Summary “Speed Read” and “Power Read”
  - Generates Mind Map
  - Shows Profile of Indexing Process
- Example follows extracting knowledge from the IBM Linux Security Documentation, publicly available on the Internet

Knowledge Extraction (Taxonomy View)



14/08/2006 1:02:54 PM: IBM Linux Security

(720) Permission,Permissions,Message queue,Access permissions,Owning user: "Access permissions can be changed by any process with an effective user ID equal to the owning user ID or creating user ID of the message queue. Access permissions can also be changed by any process with an effective user ID of 0 (DA4.16). "

C:\KOSTaxonomy\IBM Linux Security\Knowledge Organizer\2nd Order k Functio...

```
P
    PACKAGE
    PACKAGE DOCUMENTATION
    PARTITION
    PERL-DATEMANIP
    PERMISSION
        RedHat_security_target_eal3_v1-6_AS.pdf
...603.604.606.607.610.614.630.631.633.634.643.644.649.656.662.669.670.673.674.681.682.715.
        SLES_Security_target_eal4_v3-10.pdf
...672.686.702.711.712.719.720.723.727.756.
        ACCESS RIGHTS
            RHEL-4-HL-V2.13.pdf
...632.636.645.650.
            ENTRIES
            SECURITY
        EFFECTIVE USER
        ENTRY
        KERNEL
        OWNING USER
        REQUEST
        ROOT
        SELINUX
        SEMAPHORE
    PHOTO EDITOR
    PLATFORM
    POLICY
    POLICY MODULES
    POPT
    POSTFIX
    PPC/PPC64
    PPC64
    PREDICATE
    PREDICATE PREDICATE
    PRIVILEGE
    PROTECTION
    PROTOCOL
    PUBLISHING
```

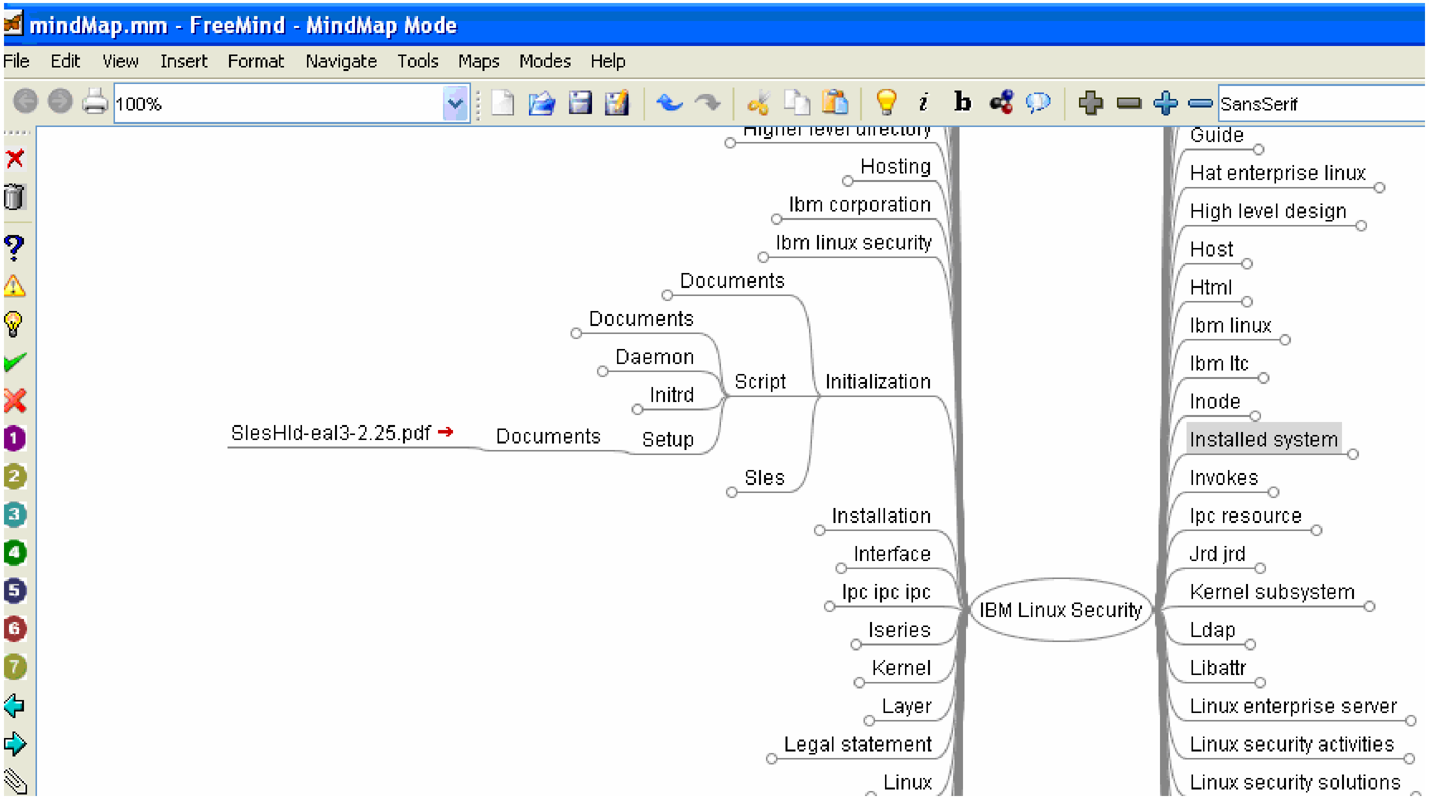
guration,Permissions,Request,Waiting,Semaphore,Access permissions,Owning Host,Evaluated configuration: "For semaphores, access checks are performed for each
nges to access controls (i.e., revocation) are effective upon the next request for access
except if a process has already made a request for the semaphore and is waiting for its
cess until the next request (DA4.19). In cases where an administrative user determines that
trative user can reboot the computer, thus destroying the semaphore and any processes
on Guide [SECGUIDE]. Since a semaphore exists only within a single host in the network,
nt to revoke all access to that semaphore. If a process requests deletion of a semaphore, it is
as its lock (or equivalently, the last process waiting for the semaphore terminates) (DA4.20).
ocesses cannot perform semaphore operations and it cannot be undeleted (DA4.21). The
he effective user ID and group ID of the process that created the semaphore and the specific
). The owning user and creating user of a newly created semaphore will be the effective user
ewly created semaphore will be the effective group ID of the creating process. The initial
process, or they are set to null and the object is inaccessible until the owner sets them.
rmission bits (DA4.23). "

**ssions,Owning user,Target,Server,Capp,Capp compliance,Linux enterprise
use**: "SUSE Linux Enterprise Server 9 Security Target for CAPP Compliance Access
qual to the owning user ID or creating user ID of the semaphore (DA4.24). Access
D of 0 (DA4.25). This function contributes to satisfy the security requirement FDP_ACC.1,

(OR.1) "

ned pipes,Socket,Disk,Object reuse,Configuration,Management,Evaluated
rs are accessed by a common mechanism for allocating disk storage and a common
g File System (ext3). Object reuse is irrelevant for the CD-ROM File System (ISO-9660)
o read residual data left by a previous user. File systems on other media (tapes, diskettes.)
not to mount file systems on these devices. Object reuse in the tmpfs file system is handled
w space for a file, the TOE uses the functions of the memory management which clear the
e system are handled by the VFS layer. Note that devpts is not a disk based file system and
For this analysis, the term FSO refers not only to named file system objects (files, directories,
o other abstractions that use file system storage (symbolic links and unnamed pipes). All of

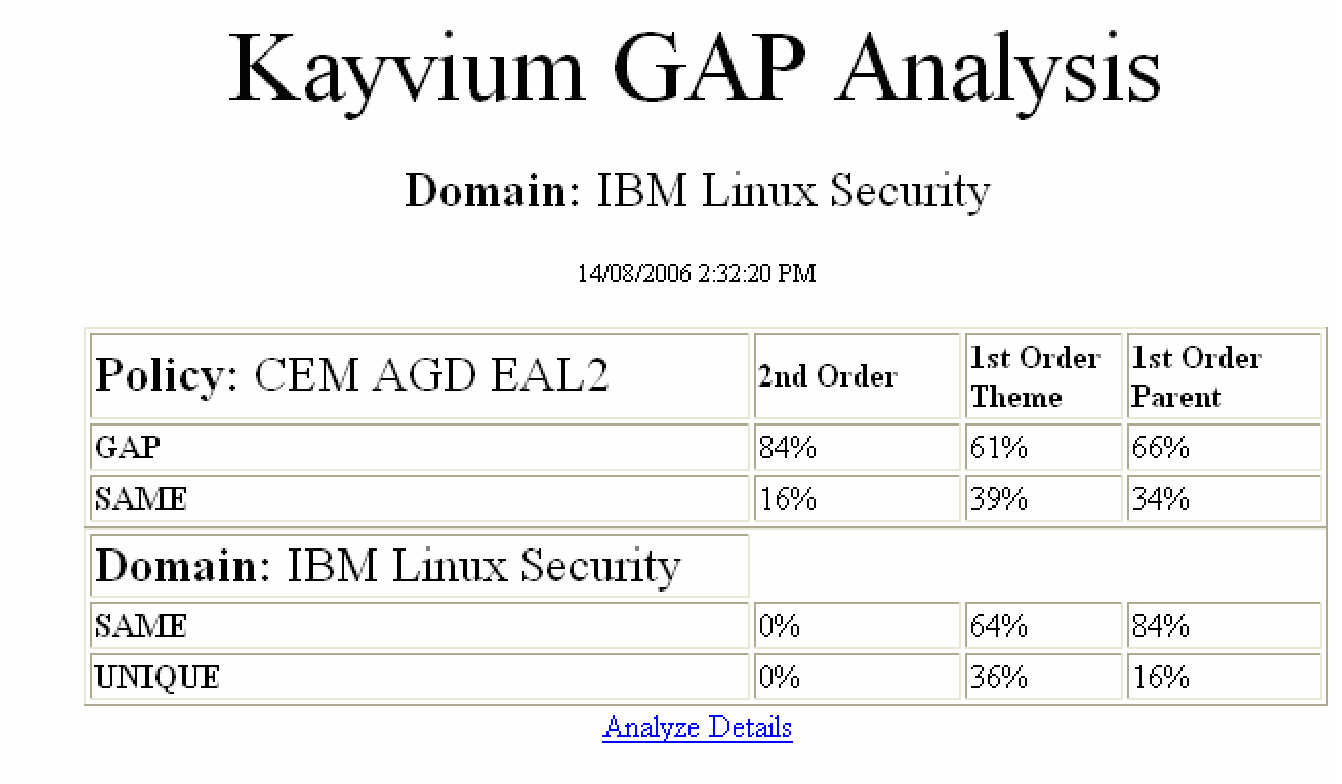
Knowledge Extraction (Model View)



Conformance Analysis

- Conformance Analysis
- Compares knowledge from two collections
    - One is Policy Model
    - Second is Performance Model
- Example follows, based on the CEM AGD section at EAL2, applied to the IBM Linux Security Documentation, publicly available on the Internet

Conformance Analysis (Summary)



Kayvium GAP Analysis

Domain: IBM Linux Security

14/08/2006 2:32:20 PM

Policy: CEM AGD EAL2	**2nd Order**	**1st Order Theme**	**1st Order Parent**
GAP	84%	61%	66%
SAME	16%	39%	34%
Domain: IBM Linux Security			
SAME	0%	64%	84%
UNIQUE	0%	36%	16%

Analyze Details

Summary

- Initial results with the Kayvium Desktop, which is an automated semantic discovery tool, show that it can provide significant improvements in the initial "reading-in" period of a project, and can provide valuable ongoing support during the evaluation.
- It provides a flexible, extensible approach to information management
- It multiplies a user’s ability to understand and correlate multiple documents
- It supports user assessments

Summary (Applicability)

- Automated semantic discovery techniques have been found to be applicable to CC problems in areas such as:
  - assisting the ST author and the CC evaluators in gaining an understanding of the volumes of documentation received from a developer
  - detecting relationships between the documents and the CC requirements and evaluation methodology
  - detecting inconsistencies across various developer documents
  - doing a “first cut” conformance analysis

Summary (Potential Benefits)

- One benefit to this approach is that it provides evaluators a means (through common models) of consistently applying CC evaluation methodology for a CC project and across CC projects. That is, the evaluators would all use a common set of models.
- The model development process also enables effective sharing of knowledge amongst the evaluators and the refinement of models as the evaluators gain more knowledge and experience.

Future Work

- Models of CC requirements and CEM need to be developed to use the full potential of the tool

Questions

?

For further information:
mgauvreau@ewa-canada.com