This presentation will probably involve audience discussion, which will create action items. Use PowerPoint to keep track of these action items during your presentation:

1. In Slide Show, click on the right mouse button
2. Select "Meeting Minder"
3. Select the "Action Items" tab
4. Type in action items as they come up
5. Click OK to dismiss this box

This will automatically create an Action Item slide at the end of your presentation with your points entered.

**Agenda for CCAE presentation**

- Progress and Status Overview
- MILS, the Common Criteria, and the CCAE
- CCAE Concept of Operation Review
- CCAE Architecture Review
- CCAE Principles of Operation Overview
- CCAE Prototype Demonstration Overview
- CCAE Demonstration
Progress

- CCAE Documentation
  - Part 1 - Introduction and Concept of Operation
  - Part 2 - Architecture
  - Part 3 - Principles of Operation

- CCAE Implementation
  - Experimental and prototype new code
  - Stable older code (shortcomings fixed as they appear)

- AFRL Layered Assurance Workshop (2nd LAW) presentation
  - High-Assurance Development and Evaluation: Rethinking the Common Criteria and EAL7

- Digital Avionics Systems Conference (27th DASC) paper
  - The MILS Component Integration Approach to Secure Information Sharing

- International Common Criteria Conference (9th ICCC) participation
  - Continuing our effort to influence future CC directions (like steering an oil tanker)
CCAE documentation overview

**Current**

- Part 1 - Introduction and Concept of Operation
  - Chapter 1 - Executive Summary
  - Chapter 2 - Introduction
  - Chapter 3 - Concept of Operation
- Part 2 - Architecture
  - Chapter 4 - Architecture
- Part 3 - Principles of Operation
  - Chapter 5 - Functional Description
  - Chapter 6 - Theory of Operation
- Appendices
  - A - Glossary
  - B - Fuzzy Unification
  - C - Workflow Management Language
  - D - Definite Clause Translation Grammar Examples
  - E - Document Generator Sketch
  - F - Repository Documents
  - G - Importing the XML Version of the Common Criteria
  - H - Publishing with LaTeX
  - I - Functional Allocation
  - J - Prototype Demo
  - K - Development Plan

**FUTURE**

- Upcoming documentation tasks for coming year
  - Continue to keep Parts 1 - 3 current and in sync with implementation
  - Appendices of current Parts 1 - 3 are a “down payment” on Part 4
  - Loose collection of low-level topics
  - Will be made complete and uniformly developed in Part 4
  - Functional Allocation (Appendix I) and Functional Description (Chapter 5) expanded to include all CONOP referenced capabilities
  - Development Plan (Appendix K) will provide detail on the planned development of all the CONOP referenced capabilities

- Updated Part 2 - Architecture
  - Chapter 4 - Architecture updated to reflect system as (being) built

- Part 4 - Development
  - Chapter 7 - Detailed Design
  - Appendix K - Development Plan (updated)

- Part 5 - Implementation
  - Chapter 8 - Implementation Commentary
  - Appendix X - Implementation Code (assuming other detail appendices may be added)
CCAED Technology

• Advances
  – Generates a PP in format and style that can be adjusted independent of the content
  – Guarantee the accuracy of normative Common Criteria material such as SFR/SAR
  – Automatically check CC dependencies and hierarchy
• Expected Advancements in Coming Work
  – Objective (and quantitative) assessment of PP quality and completeness
  – Representing and applying “fuzzy” expert knowledge
• Technical Risks
  – None in the core functional areas
  – Applying expert knowledge
  – Only the degree (somewhere between successful and “jaw-dropping” successful) of achievement in applying ontology, reasoning, and expert knowledge
• “Effort” Risks
  – Effort needed to import new versions of CC
  – Effort to encode expert knowledge and ontology

Status Summary

• CCAE Document
  – Parts 1 through 3 DRAFT, undergoing continuing refinement
  – Parts 4 and 5 to come: detailed design and implementation commentary
• Implementation goals for this timeframe substantially achieved
  – see Appendix I: Functional Allocation, pp. 171-174
  – All code for demo goals in, at least, experimental phase (see description in Appendix K: Development Plan, section K.2, pp. 182-184)
  – Skeleton is in place, now for the body building
• Project a “usable” CCAE by end 2009
  – Text-based User Interface Agent
  – Limited “intelligence” but good “organizational skills” and “attention to detail”
  – May have to contend with move to CC 3.1
Status Summary

• Next Steps
  – Complete Appendix I: Functional Allocation
    • Include all envisioned functions described in Concept of Operation
    • Give a better idea of work to come
  – Functionality needed for expert user to produce all aspects of a PP
• Plans
  – See Appendix K: Development Plan
  – Broad “stable” implementation by end-09
    • Encompassing all mechanical aspects of authoring
    • Usable by others
  – Then begin graphical user interface agent,
  – and add the “intelligence”
    • Ontology
    • Knowledge encoding
    • Reasoning
    • Expert advice

Objectives for 2009

• Establish concrete objectives and set dates for 2009 reviews and deliveries
• Tentative Objectives
  – “Stable”-ize current experimental and prototype code (see Appendix K)
    • User agent activities and UI interactions to include core PP creation and revision “therbligs”
    • Complete internal representations to accommodate all parts of a real example (SKPP)
    • Implement the relational model of T,P,A -> Objectives -> SFRs/SARs
    • Assessment of PPs using CC-based objective criteria, e.g., dependencies, hierarchy, EAL conformance, mapping and rationale, and presence of all required parts
  – Workflow Management
    • Complete integration of workflow management
    • Author and Reviewer Agents
  – Whiteboard
    • Control shell
    • Whiteboard interface rules to knowledge sources
  – Solidify CCAE’s role in MIPP conformance enforcement
• Questions?
Resources

- **CCAE Development Resources (current)**
  - Principals (current and future)
    - Rance DeLong, 80+ hours per month currently and in 2009
    - John Rushby, variable as needed
  - Other resources (medium term)
    - GUI designer when ready to begin that phase
    - Consulting from SRI’s AI Center
    - Apprentice to work on CC 3.1 adaptation and knowledge encoding
  - Outside resources (long term)
    - Reviewers and users
    - Contributing experts

MILS, the Common Criteria, and the CCAE . . .
What CC protection profiles do: The CC provides us with

- A structure for the development of security requirements specifications
- Independent functional and assurance dimensions (like ITSEC, unlike TCSEC)

Unconstrained TOEs in Functionality × Assurance
PPs Constrain TOEs in Functionality × Assurance

CC-based product (TOE) development

We expect multiple TOEs of each product type and have expectations of a relationship among instances of a type and with instances of other types.
MILS is based on composition of cooperating products defined by related Protection Profiles

- Separation Kernel (SKPP)
- Partitioning Communication System (PCSPP)
- MILS Console System (MCSPP)
- MILS Network System (MNSPP)
- MILS File System (MFSPP)
- MILS Integration Protection Profile (MIPP)

MIPP aka MILS Component Integration

Need for MILS theory and an integration PP to coordinate component PPs and avoid integration blowup
We Want MILS PPs to Achieve *This* Goal!

And, Have an Effective Approach to Product Families
Avoiding the potential problems with separate PPs for product family members

by keeping requirements well coordinated

CCAE can assist to achieve a coordinated product family

Define Configurations of a Product Family with Sub-Profiles and CCAE manages complexity
CCAES Concept of Operation Review . . .

How MILS PPs Have Been Written

Existing PP Examples (not always good)

“Produce a PP for Something”

CC v?.?.

Domain Expertise + Security Expertise
(not always both)
Applications of the CCAE

CCAЕ Collaborative Environment
### CCAE-supported author, reviewer, evaluator tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose security environ threats, policies, assumptions</td>
<td>Ontology provides a common framework</td>
</tr>
<tr>
<td>Derive security objectives</td>
<td>Ontology and expert knowledge guidance</td>
</tr>
<tr>
<td>Select SFR/SARs from CC catalog</td>
<td>Check correspondence to security objectives</td>
</tr>
<tr>
<td>Complete SFR/SAR component operations</td>
<td>Tracked in work flow</td>
</tr>
<tr>
<td>Define new component operations for ST</td>
<td>Tracked in work flow</td>
</tr>
<tr>
<td>Supply mappings and rationale</td>
<td>Tracked in work flow and relational model</td>
</tr>
</tbody>
</table>

### CCAE-supported author, reviewer, evaluator tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fashion explicit SFR/SARs</td>
<td>Help avoid gratuitous departure from CC</td>
</tr>
<tr>
<td>Select EAL and guarantee it is met</td>
<td>Ensure minimums for EAL met despite explicit rqmts</td>
</tr>
<tr>
<td>Assess conformance to abstract PP model</td>
<td>Quantitative measurement against model and scoring</td>
</tr>
<tr>
<td>Assure proper use of CC conventions</td>
<td>Conventions applied to form, semantics, typography</td>
</tr>
<tr>
<td>Assure accuracy of CC text and versions</td>
<td>“Automated” version of CC built into CCAE</td>
</tr>
<tr>
<td>Assure dependencies and consistency</td>
<td>Apply known dependencies in CC and knowledge base</td>
</tr>
</tbody>
</table>
CCAET Architecture Review . . .

CCAET Architectural Components

1. Rule Base
   - CC Component Operation Rules
   - Semantic Rules
   - Relational Model
   - Workflow Rules

2. Author/Reviewer
   - Parent PP, MILS TOE Concept, or TOE Flow-down Requirements
   - MILS Integ FW

3. CCAET Document Repository
   - Project Team
   - Exchange or Export

4. Current Document Factbase
   - XML

5. Document Creation/Revision
   - Doc Assembly, Catalog Selection, Checking, Reviewing, Inference, Rule Execution, Queries, XML gen

6. Document Publishing
   - Rendering & Conversion
   - PDF, DOCX, XLSX, ...

7. Documents & Reports
   - PP, ST, stats

Doc Creation
- Library
  - Conventions, Doc comp classes
  - Doc generators: PP, ST, FSP

Env Library
- Components, CC SFRs/SARs, Interps, CIM, Security Ontology, Resource Registry, MILS Integ FW
Model-View-Controller Architectural Pattern

Workflow Process and Agents
CCAЕ Principles of Operation Overview

Relational Structure of a Protection Profile

\[ PP = (2^T \times 2^\Pi \times 2^A \times \Omega \times 2^{SFR} \times 2^{SAR}) \]
Approximation of a MILS PP Oracle

$$PP = (2^T \times 2^R \times 2^A \times \Omega \times 2^{SFR} \times 2^{SAR})$$

$M_C$ a candidate member of $M$

CCA E drives $M_C$ toward $M$ by measuring consistency and coverage with respect to $M_{CCA E}$

$E \subset PP$ evaluable PPs

$M \subset E$ MILS evaluable PPs

Document Development Strategy and Tactics

- Grammar
- Structure
- Sequence
- Printable
- Activities
- Therbligs
- Transitions
- Generate
- Recognize
- Translate
Document Development Strategy and Tactics

1. Document kind: syntactic and semantic spec is in DCTG included in doc generator.
2. Generation of initial document sequence from Γ.
3. Recognition of document seq by Γ part of assessment.
4. Document is re-assessed throughout development.
5. Final state reached when assessment can find no fault and Author agrees.
6. Completed document is submitted for evaluation.
7. Final state of a therblig seq corresponds to new struct.
8. Initial state of next therblig seq.
9. Translation to structure.
10. Translation to printable.
11. Print format is flexible.
12. Primitive actions performed by system and user agents are called therbligs.

Grammar
- Structure
- Sequence
- Printable

Activities
- Author Agent*
- System Agent*
- Reviewer Agent*
- UI Agent
- Whiteboard Control
- Remote Tasking (e.g., email)

Therbligs
- Author
- Whiteboard

Workflow Process (workflow program execution)

* incl. Prolog code or workflow procedures
Whiteboard Architectural Pattern

Knowledge Source Production Rules for Whiteboard Interface

Condition → Action

\[ [C_1, C_2, \ldots, C_n] \rightarrow [A_1, A_2, \ldots, A_m] \]
Constructing a Usage Pattern from Expert Knowledge

A simple example ...

Expert Knowledge Rule Base

Security analyst rule

Certification rule

Countermeasures rule

Robustness (EAL) rule

Expert pattern

Expert Advice Generation

A simple example ...

Advice

m' \approx_F m

Draft PP pattern

m'

m

Threat $t_2$ may be an unidentified threat

Objective $o_1$ is customarily realized by countermeasure $f$ in addition to $g$

Assurance measures $a_i$ and $a_4$ may be needed due to the EAL sought and a certification requirement associated with countermeasure $f$

Draft PP pattern

m'

m

m' \approx_F m

m' \approx F m

Threats

Policies

Assumptions

Objectives

SFRs

SARs
Relational structure of a protection profile superimposed with a security taxonomy

External Factors
- Assumptions
  - IT Personnel
  - Physical
- Policies
  - Assurance
  - Functional
  - Procedural
- Threats
  - Development
  - Configuration
  - Interaction
  - Physical

High Level Properties
- Security Objectives
  - Assurance
  - Functional
  - Operational
  - Procedural
- Environment Security Objectives
  - IT
  - Physical

High Level Dependencies
- FAU, FCO, FCS, FDP, FIA, FMT, FPR, FPT, FRU, FTA, FTP
- ACM, ADO, ADV, AGD, ALC, (AMA), ATE, AVA
- IT Functional Personnel
- Physical

Taxonomy yields better conceptual coverage:
External Factors x High-level Rqmts x Phases ⇒ Properties x Deps ⇒ Rqmts

CCAE Prototype Demonstration Overview . . .
CCAЕ Prototype Demonstration

• What you will see
  – Demo of mostly low-level functionality through recently developed command interface

• The Demo script
  – Initialize a project to develop a new PP using a simple document generator “spp”
  – Show the initial state and publish skeletal document using LaTeX
  – Add some SFRs and SARs
  – Publish modified document using LaTeX
  – Show repository document representation of SKPP
  – Load the SKPP and publish

Simplified Document Generator for a PP

```haskell
document_generator()
  .doc_kind简化了_pp
  .doc_gen_ver(1)
  .doc_grammar(
    (spp::= pp_frontmatter, pp_chapters),
    (pp_frontmatter::= pp_title_page (<:>
      title_info("简化了 Protection Profile\', '0.00\', 'Author\', 'Date'),
      pp_title_page
    )
  )
  .doc_workflow
  .doc_resources([conforms_to(common_criteria('2.3'))])
```
Workflow Program in ‘spp’ Document Generator

doc_workflow
  *activity(author, 'Review and set preferences', [])
  *activity(author, 'Review and modify workflow plan', [])
  *activity(author, 'Schedule review', [])
  *activity(author, 'Provide explanation for security environment', [])
  *activity(author, 'Define security objectives from security environment analysis', [])
  *activity(author, 'Select SFRs from CC catalog', [])
  *activity(author, 'Complete or define CC component operations in chosen SFRs/SARs', [])
  *activity(author, 'Specify (new) component operations to be performed in the ST', [])
  *activity(author, 'Map security objectives to SFRs/SARs package', [])
  *activity(author, 'Define explicit SFRs/SARs as necessary to address objectives', [])
  *activity(author, 'Ensure that explicit SFRs/SARs have objective evaluation basis', [])
  *activity(author, 'Provide rationale that SFRs/SARs are adequate to support explicit SFRs/SARs', [])
  *activity(author, 'Assess leveling and balance of SFRs/SARs', [])
  *activity(author, 'Select appropriate evaluation assurance level package', [])
  *activity(author, 'Identify augmentations to EAL package to address objectives', [])
  *activity(author, 'Assess all aspects of draft PP from an evaluation perspective', [])
  *activity(author, 'Confirm that chosen SFRs/SARs are compatible with EALk', [])
  *activity(author, 'Provide rationale for security objectives wet security environment', [])
  *activity(author, 'Provide rationale for each SFR/SAR wrt security objectives', [])
  *activity(author, 'Provide justification for component operation not completed in PP', [])
  *activity(author, 'Confirm PP is complete, coherent, and internally consistent', [])
  *activity(author, 'Review and modify workflow plan', ['NewTasks'])
  *activity(author, 'External review', ['NewTasks'])
  *activity(author, 'Assess document', ['A'])
  *activity(author, 'Submit PP for evaluation', ['A'])
  *activity(author, 'Apply changes due to review comments', ['A'])
  *activity(author, 'Assess rationale for chosen SFR/SAR', ['A'])
  *activity(author, 'Assure all CC-originated dependencies are satisfied', [])
  *activity(author, 'Compose TOE description to explain product type and features', [])
  *activity(author, 'Assure proper use of CC conventions', [])
  *activity(author, 'Assure quality of conformance by PP', [])

Anatomy of a Repository Document
SKPP Repository Document

- Shown in demo

Artifact Flow in the Demo