AGENDA

- COMMON CRITERIA 101
- PROTECTION PROFILES 101
- COLLABORATIVE PROTECTION PROFILES
- COMPLYING WITH A PROTECTION PROFILE
COMMON CRITERIA - PLAYERS

VENDOR
Submits product for evaluation.

LAB
Evaluates against criteria and submits results to scheme. (EVALUATOR)

SCHEME
Reviews lab work and issues certificates. (CERTIFIER / VALIDATOR)

CONSUMER
Buys certified products if required by policy.
TARGET OF EVALUATION (TOE)

The thing under evaluation.

- Usually a subset of security functions
- Defined in the Security Target (document)
- Sets the scope of evaluation
The Security Target (ST) is the capstone document for a CC evaluation.

- **INTRODUCTION**: Basic product / TOE details
- **CONFORMANCE CLAIMS**: CC specific claims including PPs.
- **SECURITY PROBLEM DEFINITION**: Threat model and security objectives
- **SECURITY FUNCTIONAL REQUIREMENTS**: The functions under evaluation.
- **SECURITY ASSURANCE REQUIREMENTS**: CC defined actions for vendor and evaluator.
- **TOE SUMMARY SPECIFICATION**: How the TOE meets the Security Functional Req's
SECURITY FUNCTIONAL REQUIREMENT (SFR)

A function that the TOE must perform.

Example:

FIA_UAU.5.1 The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.
SECURITY FUNCTIONAL REQUIREMENTS (SFRs)

- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
An action that the evaluator or developer must perform to generate assurance.

Example:

ATE_IND.1.1D The **developer** shall provide the TOE for testing.

ATE_IND.1.2E The **evaluator** shall test a subset of the TSF to confirm that the TSF operates as specified.
EVALUATION ASSURANCE LEVEL (EAL)

A pre-packaged set of assurance requirements.

ATE_IND.1.1D The developer shall provide the TOE for testing.
SECURITY TARGET

**SECURITY FUNCTIONAL REQUIREMENTS**

The functions under evaluation.

**SECURITY ASSURANCE REQUIREMENTS**

CC defined actions for vendor and evaluator.

Historically selected by the vendor to match product.

Historically included by reference to an EAL.
POP QUIZ

TOE

Security Target

SFR and SAR

EAL
Protection Profiles

KEY CONCEPTS
A Protection Profile is a CC requirements specification.
CONSUMER

I want this

Protection Profile

Widget PP
Consumer XYZ

VENDOR

I can do that

Security Target

Best Widget ST
Vendor XYZ
Protection Profiles

Security Target

Best Widget ST
Vendor XYZ

Protection Profile

Widget PP
Consumer XYZ

Conforms with:
Protection Profiles

Vendor ensures that their product implements the required functions.

SECURITY FUNCTIONAL REQUIREMENTS
The functions under evaluation.

SECURITY ASSURANCE REQUIREMENTS
CC defined actions for vendor and evaluator.

Consumer specifies the assurance required. Custom packages are becoming more common (i.e. no EAL).
FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records if the audit trail is full.

Assurance Activity:

The evaluator shall examine the TSS to ensure that it describes the size limits on the audit records, the detection of a full audit trail, and the action(s) taken by the TSF when the audit trail is full. The evaluator shall ensure that the action(s) results in the deletion or overwrite of the oldest stored record.
COMMON CRITERIA - PROTECTION PROFILES

VENDOR
Security Target
Best Widget ST
Vendor XYZ

LAB

SCHEME

CONSUMER
Protection Profile
Widget PP
Consumer XYZ
Collaborative Protection Profiles

KEY CONCEPTS
COLLABORATIVE PROTECTION PROFILES (cPP)

International Technical Community (iTC)

Protection Profile
- Widget PP
  - Consumer XYZ

Supporting Doc
- Widget PP
  - Consumer XYZ

Additional Guidance
Assurance Activities
PROTECTION PROFILE MODULES - CC 3.1 R5

Base PP

Widget PP
ITC XYZ

PP Module

Red Widget PP Module
ITC XYZ

Previously ‘extended package (EP)’
JOIN A TECHNICAL COMMUNITY

cccusersforum.org
commoncriteriaportal.org
niap-ccevs.org
github.com/commoncriteria
Complying with a PP

KEY CONCEPTS
PP COMPLIANCE PROCESS

PP Selection
Based on business requirement & product type

Gap Analysis & Doc
Should include full test run to identify all gaps. ST can be created here.

Code Spin
There will be gaps to remediate. Repeat gap analysis testing.

Evaluate
Complete evaluation. Leverage gap analysis results / test plan.

Certify & Maintain
Leverage initial investment for subsequent certs.
THANK YOU

QUESTIONS?

info@lightshipsec.com