Detica

BAE SYSTEMS

Protection Profiles – Expressing your security needs

Doug Stuart, Technical Director

CSM-ACE Conference: November 2012

Detica

BAE SYSTEMS

The Common Criteria

- The Common Criteria (CC) is an internationally recognised IT security evaluation standard:
  - A framework for independent evaluation of IT security products and systems
  - Developed by many nations and many experts over many decades
  - International standard (ISO 15408)

- The CC comprises the following main parts:
  - A common structure & language for expressing product/system IT security requirements (Part 1)
  - A catalogue of standardised IT security requirement components & packages (Parts 2 & 3)
  - Common methodology for gaining assurance that IT security requirements have been satisfied (CEM)

Detica

BAE SYSTEMS

Common Criteria Recognition Arrangement

- The CC is governed by the Common Criteria Recognition Arrangement (CCRA):
  - Established in May 2000
  - Provides the basis for mutual recognition of evaluation results
  - Evaluation completed in any authorizing nation is recognised across all participating countries

- There are 2 types of CCRA membership:
  - **Certificate Authorizing Members** – Operate CCRA compliant Common Criteria certification schemes that produce certificates under the rules of the CCRA
  - **Certificate Consuming Members** – Recognise the results of evaluations and certificates of all Certificate Authorising Participants

Detica

BAE SYSTEMS

Why is this important to Malaysia

In September 2011 Malaysia was accepted as a CCRA Certificate Authorizing Member

Detica

BAE SYSTEMS

The stakeholders

- CCRA governs the CC and mutual recognition through the following:
  - Management Committee
  - Executive Subcommittee
  - Development Board
- Certification Bodies:
  - National authorities that govern an approved scheme
  - Certify the evaluation results of evaluations performed under the scheme
- Evaluation Facilities:
  - Licensed by a scheme to perform IT Security Evaluation using the Common Criteria
  - Accredited against ISO 17025
- Developers:
  - Develop IT products or systems with IT security functionality
  - Submit products to evaluation facilities to undertake CC evaluations
- Consumers:
  - Select and use CC evaluated products
  - Can specify requirements or needs through **Protection Profiles**

Detica

BAE SYSTEMS

The assurance paradigm

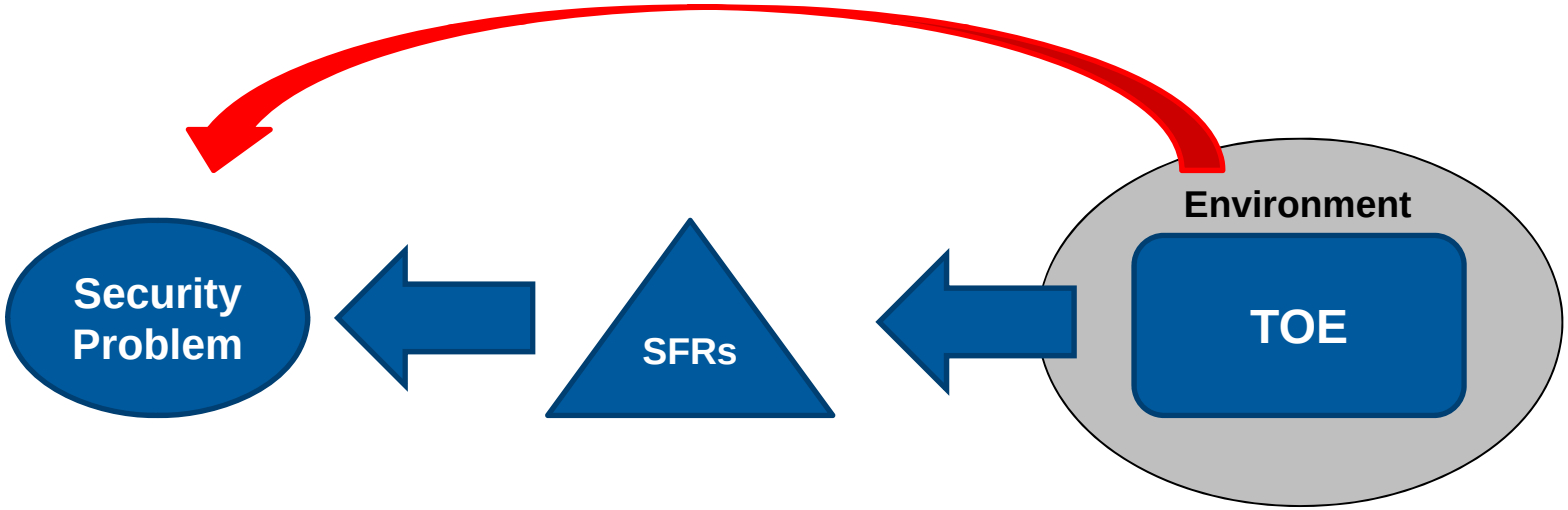
Assurance is the grounds for confidence that:

a Target of Evaluation (TOE)

in it's operational environment

implements a suite of security functional requirements

that solves a specified security problem



Consumers can specify a Security Problem through a **Protection Profile**

Detica

BAE SYSTEMS

The role of the Protection Profile

- Common Criteria Protection Profiles are:
  - An implementation independent statement of security requirements
  - Designed to specify a specific security problem through threats and organisational policy statements

- The development of a PP is appropriate when:
  - Consumer groups wish to specify security requirements for a specific product or application type
  - Government wishes to specify security requirements for a class of security products
  - An organization wishes to purchase an IT system to address its security requirements

Detica

BAE SYSTEMS

Three general kinds of Protection Profiles

Acquisition focused:

- Developed as binding procurement guidance for a specific need
- Needs to be achievable by today's technology
- Usually accompanied by additional technical specifications and designs

Establishment of a security baseline:

- Provides the minimum standard for a product set (often policy based)
- Establishes a baseline for vendors to attain providing a pool or suitable candidates
- Requirements are specified in a broad manner

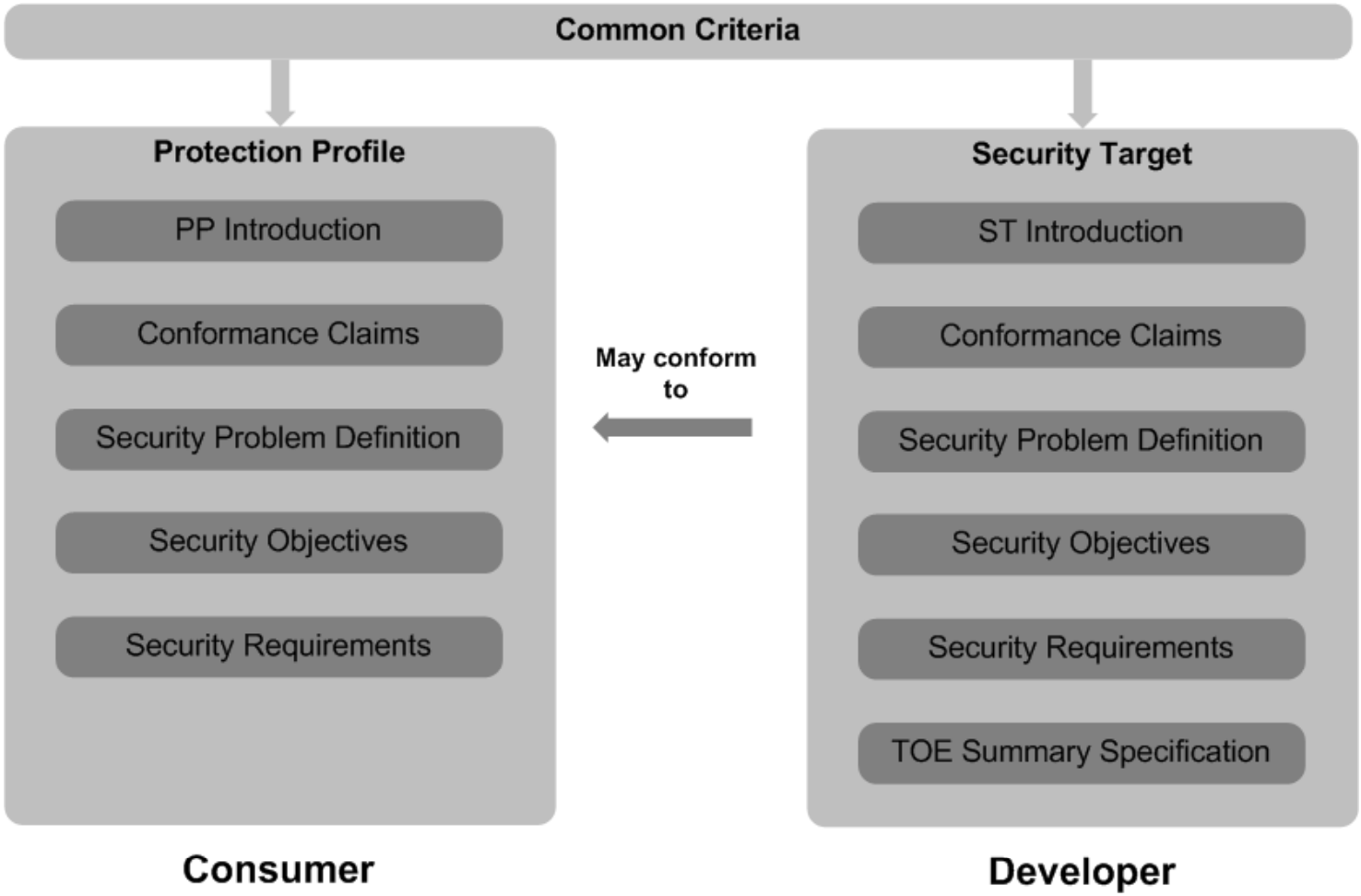
Advancement of technology or capability:

- Developed to influence the development of new technology
- Could be developed to improve the features and functionality of existing technologies (raise the bar)
- Focused on future needs and implementation

Detica

BAE SYSTEMS

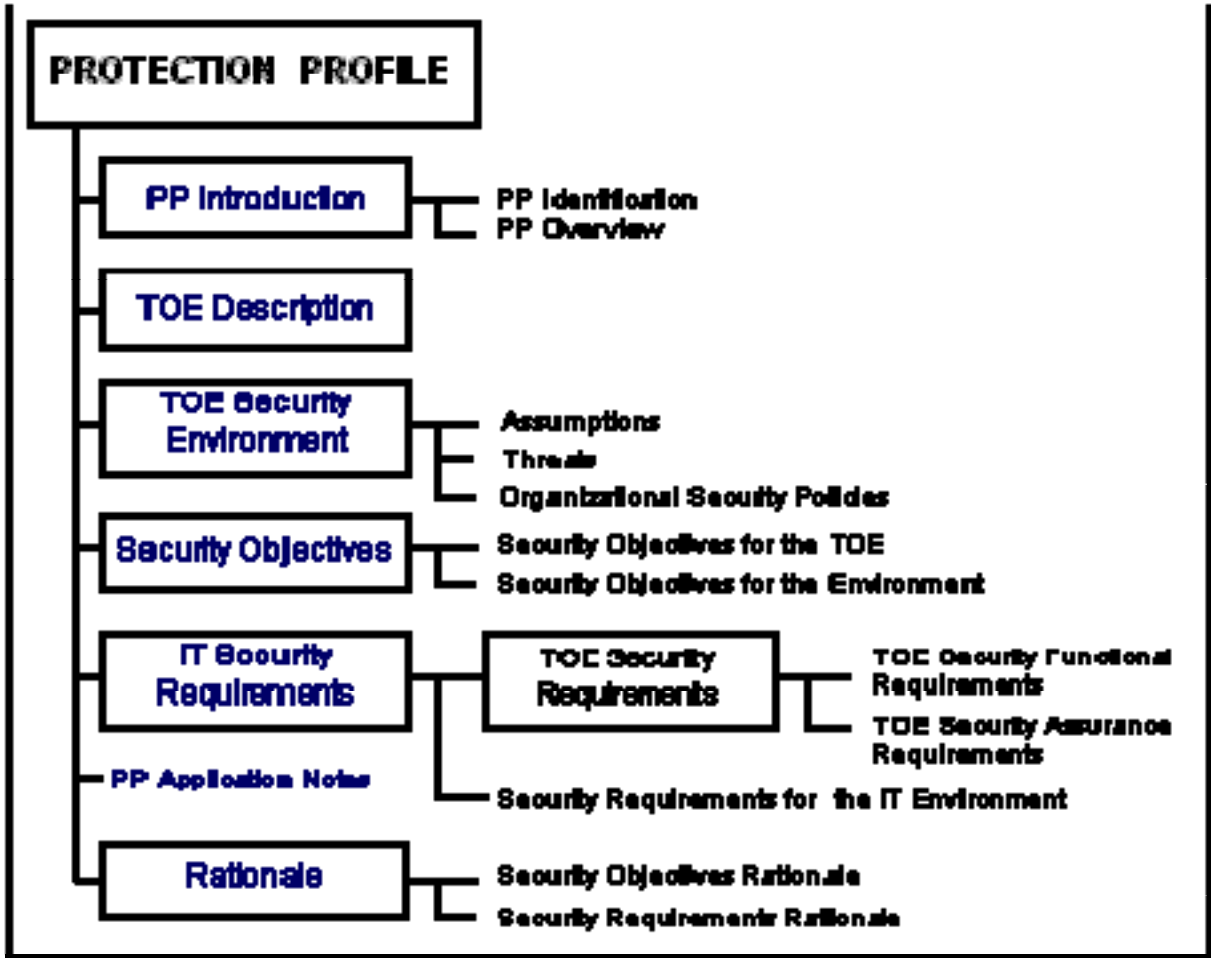
Protection Profile versus a Security Target



Detica

BAE SYSTEMS

Contents of a Protection Profile



Detica

BAE SYSTEMS

Example PP content (threats)

- Protection Profile for Full Disk Encryption

  Mitigating the risk of a lost or stolen hard disk
- Threat statements (the security problem)

T.KEYING_MATERIAL_ COMPROMISE	An attacker can obtain unencrypted key material (the KEK, the DEK, authorization factors, submasks, and random numbers or any other values from which a key is derived) that the TOE has written to persistent memory and use these values to gain access to user data.
T.KEYSPACE_EXHAUST	An unauthorized user may attempt a brute force attack to determine cryptographic keys or authorization factors to gain unauthorized access to data or TOE resources.
T.TSF_ COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted) to gain access to key material or user data.
T.UNAUTHORIZED_DISK_ACCESS	An unauthorized user that has access to the lost hard disk may gain access to data for which they are not authorized according to the TOE security policy.
T.UNSAFE_AUTHFACTOR_VERIFICATION	An attacker can take advantage of an unsafe method for performing verification of a user-entered authorization factor, resulting in exposure of the KEK, DEK, or user data.

Detica

BAE SYSTEMS

Example PP content (security objectives)

- Stated security objectives (how we solve the security problem)

O.AUTHORIZATION	The TOE must obtain the authorization factor(s) from a user to be able to decrypt the data on the hard disk.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF in its operational environment.
O.ENCRYPT_ALL	The TOE will encrypt all data that are stored on a hard drive. (Note that this may exclude the MBR and the bootable partition that it points to.)
O.EXTERNAL_AUTH_FACTOR_PROTECTION	The TOE shall ensure that an external token authorization factor is inaccessible after it is used for authorization.
O.DEK_SECURITY	The TOE will mask the DEK using a key encryption key (KEK) created from one or more submasks (which in turn are derived from the authorization factors) so that a threat agent who does not have authorization factor(s) will be unable to gain access to the user data by obtaining the DEK.

Detica

BAE SYSTEMS

Example PP content (security functional requirements)

FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

FCS_COP.1(1) Cryptographic operation (Disk Encryption)

FCS_COP.1.1(1) **Refinement:** The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection: CBC, CCM, CFB128, CTR, OFB, XTS] mode** and cryptographic key sizes **[selection: 128 bits, 256 bits]** that meet the following: **FIPS PUB 197, "Advanced Encryption Standard (AES)" and *selection: NIST SP 800-38A, NIST SP 800-38C, NIST SP 800-38E]**.

FCS_COP.1(4) Cryptographic operation (Key Masking)

FCS_COP.1.1(4) **Refinement:** The TSF shall perform **key masking** in accordance with a specified cryptographic algorithm **[selection: XOR; AES used in ECB mode]** and the cryptographic key size **[selection: 128 bits, 256 bits]** that meet the following: [**selection: "None" for XOR; "FIPS PUB 197, *Advanced Encryption Standard (AES)* and NIST SP 800-38A" for AES+.**

Detica

BAE SYSTEMS

Recent updates within the CCRA

- The CCRA Management Committee (CCMC) September 2012, agreed on a vision statement for the future direction of the application of the CC and the CCRA.
- This vision statement has the CCRA moving to a more PP-centric way of using the criteria
- Standardisation is to be increased by building Technical Communities (TC) developing collaborative Protection Profiles (“cPPs”) and supporting documents,
- Mutual recognition will be based on the achievable common level of the cPPs.
- TCs will be defined and cPPs will be developed for all product classes where multiple manufacturers provide individual STs for similar products

- What does this all mean?

Protection Profiles are going to play an even more prominent role in the assurance paradigm and the Common Criteria!

Detica

BAE SYSTEMS

More information

- Protection Profiles:
  - Common Criteria Certified Protection Profiles
    http://www.commoncriteriaportal.org/pps/
  - US Government Approved Protection Profiles:
    http://www.niap-ccevs.org/pp/

- Malaysian MyCC Scheme:
  http://www.cybersecurity.my/mycc/