Introducing Assurance Measures for the Security Target

Yi Mao

atsec information security corporation

yi@atsec.com

Agenda

- The benign intention of CC
- The weakness of CC
- The proposed solution:
  Introduce assurance measures for ST
- Example
- Summary of potential benefits

The benign intention of CC

Security starts with the protection of assets

Threats reduce the value of the assets to the owner

There are risks associated with exposing the assets to the threats

Countermeasures are imposed to reduce the risks

The goal of CC evaluation

The goal of CC evaluation is to provide a certain level of assurance to the asset owner or TOE users, who may lack the knowledge, expertise or resources necessary to judge the sufficiency and correctness of the TOE on their own.

Such users may use the evaluation results to decide whether to accept the risk of exposing the assets to the threats and gain an increased confidence in using the CC-evaluated IT products.

The two-step evaluation model

- ST evaluation
  - Ensures the sufficiency of the countermeasures to counter the identified threats
- TOE evaluation
  - Ensures the correctness of the implementation of countermeasures

The logic behind the model

(1) If the countermeasures do what they claim to do, then the threats to the assets are countered.

(2) The countermeasures do what they claim to do.

Therefore, the threats to the assets are countered.

The justification of the first premise

(1) If the countermeasures do what they claim to do, then the threats to the assets are countered.

The truth of this premise is justified during the ST evaluation.

The ST evaluation determines the **sufficiency** of the countermeasures implemented in the TOE or provided by the OE.

The verification of the second premise

(2) The countermeasures do what they claim to do.

The truth of this premise is verified during the TOE evaluation.

The TOE evaluation determines the **correctness** of the implementation of the countermeasures in the TOE.

The structure of the ST

- ST introduction
- Conformance claims
- Security problem definition
  - Threats
  - OSPs
  - Assumptions
- Security objectives
  - TOE objectives
  - OE objectives
- Extended components definition
- Security requirements
- TOE summary specification

The evaluation of the ST (1)

- ASE_INT: ST introduction, 1
- ASE_CCL: Conformance claims, 1
- ASE_SPD: Security problem definition, 1
- ASE_OBJ: Security objectives, 1 → 2
  - Objectives for TOE
  - Objectives rationale

The evaluation of the ST (2)

- ASE_ECD: Extended components definition, 1
- ASE_REQ: Security requirements, 1→ 2
  - Traces each SFR back to the security objectives for the TOE
  - Rationale that demonstrates that the SFRs meet objectives
  - Rationale for SARs
- ASE_TSS: TOE summary specification, 1→2
  - Describes how the TOE protects itself against interference and logical tampering
  - Describes how the TOE protects itself against bypass

The weakness of CC

Some loose ends

- CC sets very few restrictions on the acceptance criteria for security problem definitions
  - If an ST has no threats, it must have OSPs
  - If an ST has no OSPs it must have threats
- CC does not require that there must be at least one objective for the TOE
- Correct instantiation of the OE is assumed, and its assessment falls outside the scope of CC evaluation

Notes from the CC

- CC Part 1, Section A.6.1, paragraph 287:

  "The security problem definition is … axiomatic … the process of deriving the security problem definition falls outside the scope of the CC."
- CC Part 1, Section A.6.1, paragraph 288:

  "The usefulness of the ST strongly depends on the quality of the security problem definition."
- CC Part 1, Section A.7.3.3, paragraph 319:

  "Countering a threat does not necessarily mean removing that threat, it can also mean sufficiently diminishing that threat or sufficiently mitigating that threat."

CC features (or defects?)

- CC is very flexible with regard to definition of assumptions, OSPs and threats
  - The scope of defined threats is left to the decision of the author and is not specifically mandated to be complete
  - Vulnerabilities in the TOE environment can be “dismissed” by asserting sweeping assumptions
- CC does not prevent ST writers from defining unrealistic TOE boundaries
  - Result: consumer complaints that evaluation results are not useful; for example, evaluation of an OS that is defined to have no network connectivity is not useful to consumers
- Applicability of CC evaluation results is very restrictive
  - A CC certificate is valid for a specific release and patch level only

The problem with the CC framework (1)

- The assurance level of the TOE does not accurately reflect the consumer's risk in using the TOE because of
  - risks associated with sweeping assumptions that "dismiss" vulnerabilities in the OE
  - risks associated with threats that are overlooked and hence fall outside the TOE border

These risks are not addressed in the ST evaluation.

These risks are not reflected in the EAL of the TOE.

The problem with the CC framework (2)

- CC evaluation results are difficult for non-CC experts to fully understand because
  - assessing the real value of the evaluation result requires understanding the “fine print” in the ST
  - while a layman takes it for granted that EAL4 products are more secure than EAL3 products, it really depends …
    - What assumptions have been made?
    - What threats have been defined, and how have those threats been countered?

Is the goal of the CC met?

The goal of having a CC evaluation is to provide a certain level of the assurance to the asset owner or TOE users who may lack the knowledge, expertise or resources necessary to judge sufficiency and correctness of the TOE on their own.

They may use the evaluation results to decide whether to accept the risk of exposing the assets to the threats and gain an increased confidence in using the CC-evaluated IT products.

Not completely met!

The proposed solution:
Introduce assurance measures for ST

The big picture

- Evaluate assumptions, OSPs and threats as part of the ST evaluation.
- Record ST evaluation results in an assurance level for the ST.
- A paired ST assurance and TOE assurance together represents the total risk of exposing the assets to threats if the evaluated product is in use.
- The higher the ST assurance level, the lower the risk.
- The ST assurance level being equal, the higher the TOE assurance level, the lower the risk.

The required changes

- Remove the ASE class from the TOE EAL packages (denoted as TOE_EALs)
- Create EAL packages for ST (denoted as ST_EALs)
- Use the ASE class as a base for ST_EALs
- Extend the ASE class to include families for the assessment of assumptions, threats, OSPs, and their interrelationships

Possible extended families for ASE

- Assess the appropriateness of assumptions
  - Is every assumption necessary?
  - Are assumptions redundant?
- Assess the appropriateness of threats
  - Is the list of threats exhaustive?
  - Is a rationale given for any dismissed threat?
- Interdependency between assumptions and threats
  - Threats should not simply be countered by assumptions
  - Threats must be countered by security features in the TOE and/or the OE
- Mutual exclusiveness of threats and OSPs
  - An OSP to be enforced cannot be a threat
  - A threat is not covered by an OSP
- Scrutinize division between objectives for TOE and OE

Example:
PKIFv2 (an EAL4+ CC evaluation)

- PKIFv2 is a software library toolkit that enables developers to easily incorporate secure PKI functionality into an application
  - Certification path processing
  - Data encryption/decryption
  - Signature generation/verification
- The product itself does not perform any cryptographic operations.
- It operates with cryptographic module or Common Access Cards through the underlying operating system and middleware.
- Certified under NIAP scheme on Jan. 8, 2008 at EAL4 augmented with ALC_FLR.2

IT environment of the PKIFv2 TOE

- The operating system together with the cryptographic module
- The application utilizing the TOE
- Certificates and revocation status information interfacing with the TOE

Assumptions about the PKIFv2 IT environment

- OS provides protection for the TOE
  - Identification and authentication of users to ensure that only authorized users have the access to TOE
  - Domain separation for multiple instances of the TOE at runtime to ensure that variables do not share or re-use data across applications
  - Auditing capabilities to capture improper configuration of OS or TOE
- Application developers are non-hostile
  - Will not bypass TOE security functionality
  - Will not misuse TOE security functionality
  - Will not ignore the returned results of the invoked functions
  - Will follow all user guidance

The comparability problem

What EAL4+ means for PKIFv2:

- The TOE in the evaluated configuration as defined by the ST was certified at TOE assurance level EAL4 augmented with ALC_FLR.2.
- The TOE in the evaluated configuration consists of PKIFv2 and substantial security-relevant functionality provided by the IT environment.

Therefore, the EAL4+ result applies to …

– the TOE (PKIFv2) with substantial dependency on the IT environment.

Compare this EAL4+ result to …

An OS certified at EAL4 augmented with ALC_FLR.2.

- The security functionality of the OS is relatively self-contained, without any substantial dependency on the IT environment for security-relevant functionality.

The EAL4+ result applies to …

- the TOE (the OS) with very little dependency on the IT environment.

Conclusion: the TOE assurance level alone does not convey enough information for a non-CC expert to understand the evaluation result.

Try out the proposed solution

- PKIFv2 is certified at

  <ST_AssuranceLevel.x, EAL4+>
- The OS is certified at

  <ST_AssuranceLevel.y, EAL4+>
- y is a higher assurance level than x for ST

The CC evaluation result of PKIFv2 is now usefully differentiated from that of the OS.

- The ST assurance level reflects the appropriateness of the defined scope and depth of TOE security features.
- TOE assurance level marks how well these features are designed and implemented in the product.

Summary of potential benefits

1. The ST assurance level indicates how well the security problem is defined.

2. The ST assurance level gained through the critical assessment of the threats, assumptions, and OSPs as proposed in the ST validation reflects the real risks involved in using a CC-evaluated IT product.

3. Paired assurance for the ST and the TOE better matches the two-step evaluation process.

4. Paired assurance for the ST and the TOE provides an extended common ground for the comparability of security features among IT products.

5. Paired assurance for the ST and the TOE better handles the patch situation. If patches do not have an impact on the ST, then the ST assurance level can remain unchanged.

6. The ST evaluation methodology can influence secure system design. CC is not only an evaluation standard and vehicle, but also provides valuable guidance for secure system design. Influencing system design in this way can subtly boost the visibility and influence of the Common Criteria in the IT security community.

Acknowledgement

I thank my atsec colleagues for review and helpful feedback:

Brenda Grove

Helmut Kurth

Fiona Pattinson

Ken Hake

David Ochel

Thank you for your attention!