



Unofficial Part 4 of the Common Criteria

Lisa Lippard, Senior Systems Security Engineer
James Arnold, AVP Technical Director
22 September 2009



Synopsis



- Problems
- Proposal
- Security Problem Definitions
 - Threats
 - Organizational Security Policies (OSP)
 - Assumptions
- Security Objectives
- Common Criteria (CC) Part 4
- Conclusions and Recommendations

Problems



- **Proliferation**
 - Protection Profiles (PPs) and Security Targets (STs) have come to have relatively long lists of problem and objective statements.
- **Unnecessary Variation**
 - The problem and objective statements for the (otherwise) same problem or objectives vary notably between PPs and STs.
- **Improper Focus**
 - The problem and objective statements often stray away from security functions and into assurances.
- **Improper Abstraction**
 - Problem and objective statements are often restatements of one another. Objective statements are occasionally restatements of requirements.

Problems



- The Common Criteria (CC) offers little in terms of actual requirements to ensure that problems and objectives are actually meaningful and at a proper or good level of abstraction.
- Developers just want their products evaluated and are more than happy to borrow from available sources.
- Evaluators have come to view the problem and objective statements as essentially just extra evaluation work that need be performed because the CC requires it.
- Ultimately, it seems Protection Profile authors are working hard to include as many statements as they can (perhaps to benefit their perceived customers) while Security Target authors are trying to include as few as possible (perhaps to reduce effort/cost).



Common Criteria for Information Technology Security Evaluation Part 4: Security problem definitions and objectives

- Provide a better defined framework for the specification and evaluation of security problems and objectives.
- Provide a catalog of security problems and objectives for common scenarios and technologies.
- Encourage more commonality to improve comparability.
- Diminish the cost and effort to develop and evaluate security problem and objective statements.
- In general, attempt to bring more meaning and value to security problem and objective statements.

Security Problem Definitions



- Security Problem Definitions are currently defined in three parts:
 - Threats
 - Consist of a threat agent, an asset and an adverse action of that threat agent on that asset.
 - Organizational Security Policies (OSPs)
 - A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.
 - Assumptions
 - Made on the operational environment in order to be able to provide security functionality.

Threats



- The Common Criteria (CC) should recognize that some aspects can be vague or potentially absent as long as the resulting statement represents a security problem to be solved.
 - The CC dictates that threats must be represented in terms of agents, assets, and attacks.
 - However, there may be security problems where one or more of these values is unknown or perhaps very vague or general.
 - For example, I may be concerned that my money might be stolen, but I don't really know how that might occur.
 - Similarly, I might be concerned that my system might fail, but it doesn't really matter how it might happen (e.g., human error, natural disaster, Denial of Service (DoS) attack).
 - The security objectives should serve to enumerate what the Target of Evaluation (TOE) brings to bear to address the threat.

Threats



- Threat statements should address issues present in the absence of the Target of Evaluation (TOE).
 - Too many Protection Profiles and Security Targets include threat statements about the TOE itself or about the evaluation of the TOE.
 - For example,
 - » the TOE might be ill designed
 - » the TOE might run out of space
 - » the TOE might not be adequately tested
 - The threat statements should represent the problem that the TOE is intended to solve and should not delve into assurance issues and non-Common Criteria topics (e.g., compliance with other standards) or conjecture about problems the TOE may have.

Threats



- Threat statements should be direct and kept to a minimum to concisely represent the threats that require remediation.
 - For example, if the threat is unauthorized access, there doesn't need to be a threat about accountability or authentication.
 - Indirect issues, such as the need to identify and authenticate users in order to enforce access controls, should be addressed with security objectives and not additional threats.

Organizational Security Policies



- Organizational Security Policies (OSPs) should be used where the security problem cannot (or should not) be readily stated in the form of a threat.
 - OSPs have always been problematic given the sentiment that Security Target authors are not at liberty to speculate or offer their own.
 - However, OSPs should be a tool available to everyone since there are mechanisms developed to solve problems that are better represented as policies rather than threats.
 - For example, user accountability is a policy and not a threat (e.g., users^{agent} might not be accountable for their actions^{asset} due to the absence of an accountability mechanism^{action}).

Organizational Security Policies



- Organizational Security Policies (OSPs) should be subject to suitability evaluation like threats.
 - Currently, If OSPs are included they are required to be defined, but requirements for acceptability stop there.
 - Both OSPs and threats should be subject to evaluation criteria designed to ensure they are meaningful, appropriately focused, and at the right level of abstraction.

Assumptions



- Assumptions are not really part of the security problem definition.
 - They don't serve to represent any security problem, but rather serve to qualify the solution.
 - As such, they fit somewhere between the security problem definition and security objectives – not a statement of problems to be remediated and not objectives to be acted upon to form a solution.
 - Regardless, retaining them as an adjunct to the security problem definition isn't a problem and we don't recommend forming an intermediate abstraction.

Assumptions

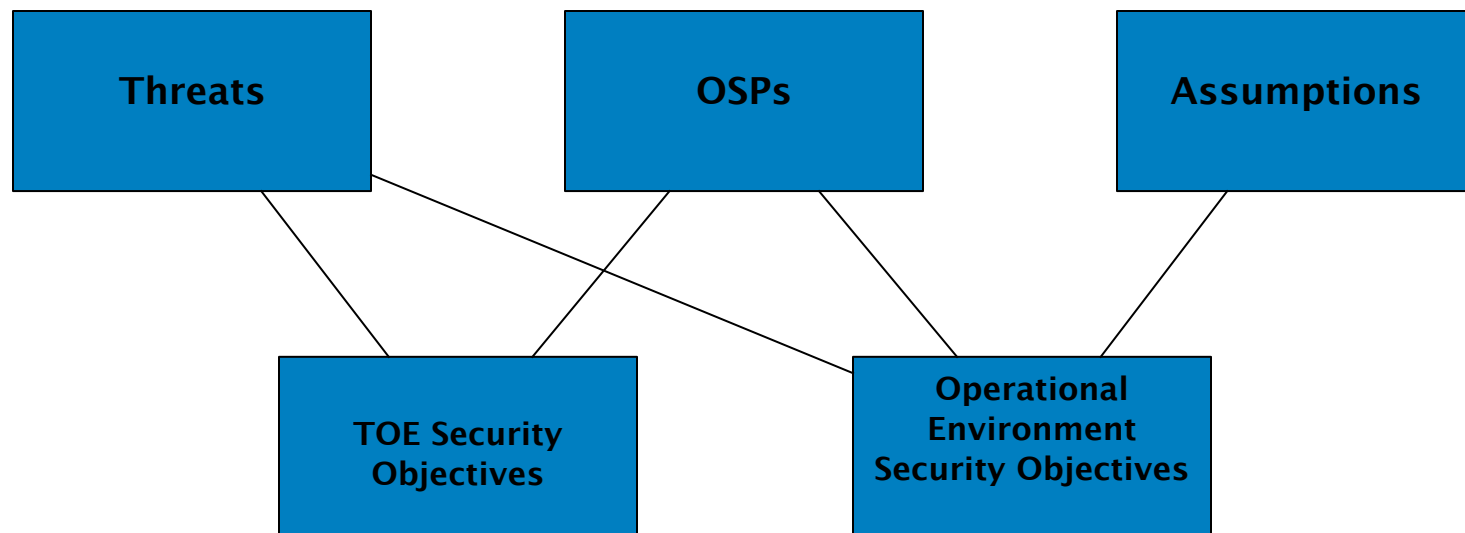


- The handling of assumptions should change in the Common Criteria (CC).
 - There should be no need to address them with objectives.
 - In most cases, the correspondence between assumptions and objectives is one to one so there is really no value there.
 - However, assumptions should be addressed in terms of suitability.
 - Assumptions should not represent characteristics of the Target of Evaluation (TOE).
 - They should focus on issues outside TOE control such as user behavior, operational environment provisions, and TOE placement/connections.
 - They should be as limited as reasonably possible and focused.
 - Trivial assumptions (e.g., power requirements) should be handled indirectly (e.g., by assuming that guidance is followed).

Security Objectives



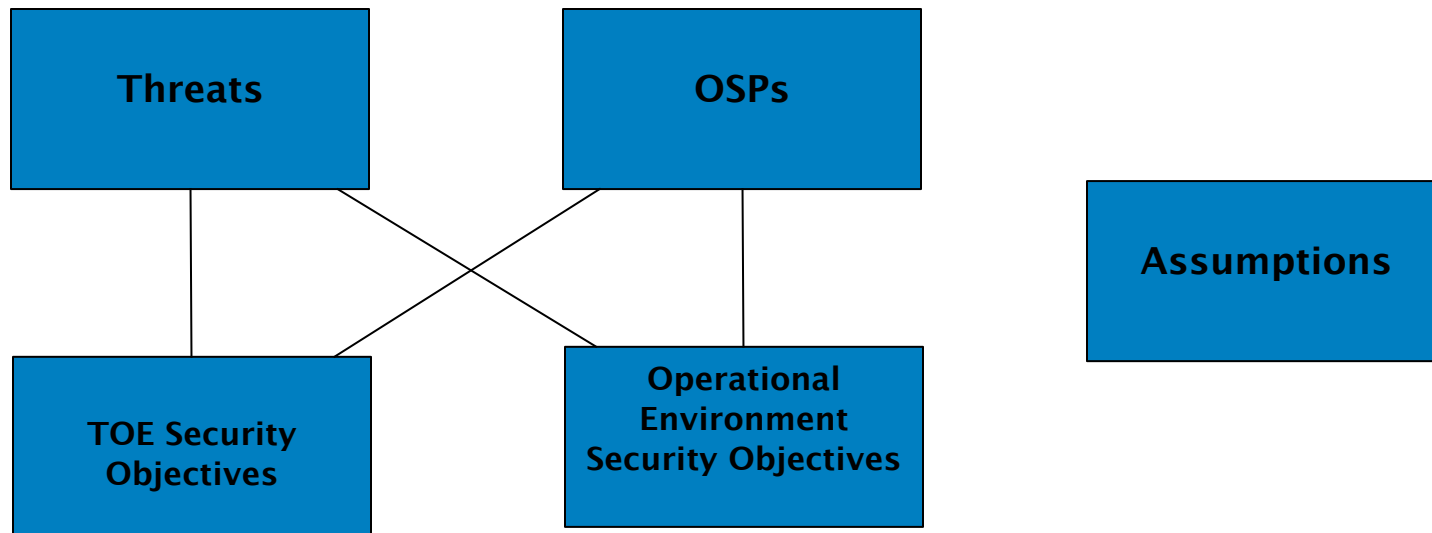
- Security Objectives are currently required to be specified for the Target of Evaluation (TOE) and its operational environment.
 - The following relationships can currently exist between security problem definitions and security objectives.



Security Objectives



- The following relationships are proposed to be allowable between security problem definitions and security objectives.
 - Note that assumptions should have no correspondence to security objectives.



Security Objectives



- The security objectives should represent essentially a “To Do” list in order to address the identified security problems.
 - The Target of Evaluation (TOE) security objectives identify the things the TOE must do.
 - The operational environment security objectives identifies the things the operational environment must do, short of repeating the assumptions which speak for themselves.
 - As a result, the operational environment security objectives should focus on supporting IT capabilities in the operational environment.
- Unlike the security problems, security objectives do account for the TOE and its limitations.

Common Criteria (CC) Part 4



- The existing CC should include some changes in Parts 1 and 3 regarding the general model and specific requirements for the evaluation of security problems and objectives.
- The proposed Part 4 serves security problems and objectives much like the current Part 2 serves security functional requirements.
 - It is intended primarily to be a catalog of security problems and objectives organized by similarity.
 - Just like Part 2, it includes the notion of operations that can be used on the content of the catalog to facilitate flexibility to keep the catalog manageable.

Common Criteria (CC) Part 4



- The proposed Common Criteria Part 4 has an outline similar to that of Part 2, except that much of the outline is repeated to address both security problems and also security objectives.
 - Note that Assumptions are addressed separately but in conjunction with security problems.
- Also, just like Part 2, the intent is to include appendices that serve to offer guidance (e.g., application notes) to better help the reader understand how to utilize the content of Part 4 effectively.
- Arguably, it would be better to actually produce two new parts to distinguish security problems and security objectives.
 - We have been working with a single document for convenience only.

Common Criteria (CC) Part 4



- The general outline of the proposed Common Criteria Part 4 with respect to security problems is as follows:
 - Security Problem and Assumption Paradigm
 - Security Problem and Assumption Structure
 - Class Structure
 - Statement Structure
 - Individual Security Problem Classes (Unauthorized Access, Denial of Service, Accountability, etc.)
 - Individual Security Problem Statements
 - » Proposed CC Part 4 does not distinguish between threats and OSPs since there shouldn't be a difference
 - Individual Assumption Classes (Personnel, Connectivity, Physical, etc.)
 - Individual Assumption Statements

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 security problem examples:
 - Security Problem Classes
 - Unauthorized Access
 - » Addresses threats and OSPs related to disclosure and integrity of sensitive data.
 - Denial of Service
 - » Addresses threats/OSPs related to Denial of Service (DoS) attacks to make assets unavailable to intended users.
 - Accountability
 - » Addresses threats/OSPs that all users can be held accountable for their actions.
 - Intentionally very broad

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 security problem examples:
 - Security Problem statement examples
 - Unauthorized Access
 - » ACCESS – A [selection: user, application, [assignment: other agent]] may gain [assignment: type of access] access to [selection: data, [assignment: other resource]] for which they are not authorized.
 - Denial of Service
 - » AVAILABLE – [selection: data, [assignment: other resource]] might be subject to [assignment: type of attack] attacks rendering it unavailable.
 - Accountability
 - » ACCOUNTABLE – Users of [selection: data, [assignment: other resource]] can be held accountable for their actions.

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 assumption examples:
 - Security Problem Assumption Classes
 - Personnel
 - » Addresses users, guidance, training, etc.
 - Connectivity
 - » Addresses connection requirements to peripheral devices such as network architecture placement, UPS availability, etc.
 - Physical
 - » Addresses physical protection measures such as locked doors, guards, etc.

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 assumption examples:
 - Personnel:
 - » MANAGE – There will be one or more competent individuals assigned to manage the TOE.
 - » NO_EVIL – Administrators are non-hostile, appropriately trained and follow all administrator guidance.

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 assumption examples:
 - Connectivity:
 - » CONNECT – The TOE has access to all the IT system data and resources it needs to perform its functions and all connections are presumed to be secure.
 - » SCALABLE – The TOE environment is appropriately scalable to provide support to the IT systems in the organization it is deployed.

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 assumption examples:
 - Physical:
 - » LOCATE – The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access, and the IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.

Common Criteria (CC) Part 4



- The general outline of the proposed Common Criteria Part 4 with respect to security objectives is as follows:
 - Security Objective Paradigm
 - Security Objective Structure
 - Class Structure
 - Statement Structure
 - Security Objective Classes [Note: For the most part, security objective classes mirror CC Part 2 classes.]
 - Audit
 - Communication
 - Cryptography
 - Identification and Authentication
 - Management
 - Privacy
 - Protection
 - Resource Utilization
 - TOE Access
 - Trusted Path/Channel
 - User Data

Common Criteria (CC) Part 4



- Proposed Common Criteria Part 4 security objective examples:
 - Audit
 - AUDIT – The TOE will provide the capability to detect and create records of security-relevant events associated with users; records will be protected and available for review by authorized users.
 - Cryptography
 - CRYPTO – The TOE will provide cryptographic functions for its own use to protect communications between [selection: TOE components, the TOE and trusted IT systems, trusted IT components [assignment: other entities]].
 - Management
 - MANAGE – The TOE will provide all functions and facilities necessary to support authorized administrators in their management of the security of the TOE and restrict these capabilities for unauthorized use.

Conclusions and Recommendations



- We recommend that the International Common Criteria (CC) community consider furthering the development of a security problem, assumption, and security objective framework and catalog.
- Our work is a work in progress and for the most part can be used within the existing CC paradigm.
- The current draft document will be made available upon request to any who are interested.

Contacts



Lisa Lipphard

SAIC Accredited Testing & Evaluation Labs
Common Criteria Evaluator

Lisa.A.Lipphard@saic.com

410-953-6856

James Arnold

SAIC Accredited Testing & Evaluation Labs AVP/Technical Director

James.L.Arnold.Jr@saic.com

410-953-6833

<http://www.saic.com/infosec/common-criteria/>