A Taxonomy of Organisational Security Policies

Dr. Gary W. Smith and Richard B. Newton

Science Applications International Corporation
McLean, VA

Abstract: although the Common Criteria provides an exhaustive list of security requirements, it does not include a similarly complete list of organisational security policies or security objectives that can be used to specify a set of requirements for a product or information system. This paper first presents a hierarchy of abstractions at which security policies and requirements can be stated and maps those levels to elements of a Protection Profile. The primary contribution is an extensive taxonomy of organisational security policies that would be useful to Protection Profiles writers.

The Need

The *Common Criteria for Information Technology Security Evaluation* [ISO/IEC 15408] includes a process for producing a Protection Profile (PP) that specifies the security requirements for a product or information system (IS). A Proposed Draft Technical Report, *Guide for the Production of PPs and STs* [ISO/IEC PDTR15446] provides guidance on the preparation of PPs. The end result of the process is to specify a set of security functional and assurance requirements that must be met by a Target of Evaluation (TOE). A TOE can be either a product or IS. The Common Criteria (CC) includes an exhaustive list of requirements. But what set of the many requirements are appropriate for a particular TOE? Production of a PP includes a process that establishes these requirements based on a set of TOE objectives.

In the PP production process, objectives—both for the TOE and the environment—are generated in response to a set of threats, assumptions, and organisational security policies (OSPs). Since there is no comprehensive list of candidate OSPs, one of the challenges for PP writers is to establish a consistent and complete set of security policies to meet the organisational needs—consistent in terms of being stated at the same level of abstraction and complete in terms of covering the security policy domain space. While the draft guidance for producing PPs [ISO/IEC PDTR15446] advocates only stating OSPs that do *not* correspond to a stated threat, we believe the starting point for establishing objectives should be a complete set of OSPs. This need is of particular importance for a PP where the TOE is an IS—a *system PP* where one must fully understand the organisation's policies to ensure that the coverage of the final set of objectives is complete.

The purpose of this paper is to provide a taxonomy of OSPs from which specific policies can be selected to build a system PP. Our goal is for this taxonomy to completely cover the domain space of organisational security policies and for all policies to be stated at the same level of abstraction. It is an ambitious task.

A Policy/Requirement Hierarchy

Before describing the taxonomy, it is important to put OSPs in context of other types of security policies. *Security Policy* is perhaps the most semantically overloaded computer security term. There are security policies published in regulations; security policies for an information system; and even an operating system access control security policy that maybe formally modeled. All of these security policies are

similar, but different. In fact, when someone says *security policy* it is often difficult to recognize to which type of security policy they are referring.

We use the *Practices for Securing Critical Information Assets* report [PSCIA] from the Critical Infrastructure Assurance Office (CIAO) as the starting point for establishing a hierarchy applicable to the elements of a PP. The CIAO report defines an Information Security Policy as "a set of rules and practices an agency uses to manage, protect, and allocate its information resources". The CIAO report goes on to identify three types of policies:

- *Program policy is what management uses to create an organisation's security program. It is high-level, comprehensive, and unlikely to need frequent updating.*
- *System-Specific policy is the body of rules and practices used to protect a particular information system. System-specific policy is limited to the system or systems affected and may change with changes in the system, its functionality, or its vulnerabilities.*
- *Issue-specific policy addresses issues of current relevance and concern to the agency. Issue-specific policy statements are likely to be limited, particular, and rapidly changing. Their promulgation may be triggered by a computer security incident.*

To support security policies and requirements in the context of the PP, we propose a three-tier hierarchy of security policies/requirements. (We combine reasoning about security policies with security requirements for the following reasons: policies and requirements both state *what* a system or organisation must do (as opposed to *how* or *why*); whether a statement of *what* a system must do is a *policy* or *requirement* is "in the eye of the specifier"; and while in some cases requirements drive security policies, in other cases policies drive security requirements.)

Figure 1 shows a three-level hierarchy of security policy/requirements (P/Rs). The top layer, Level 1, corresponds to OSPs—they are the type of policies that are often stated in policy documents such as organisational regulations and directives. Level 1 P/Rs map directly to *program policies* in the CAIO report. The most important characteristic of a Level 1 policy/requirement is that it is independent of whether it is implemented by the TOE or the environment (i.e., physical, personnel, and administrative).

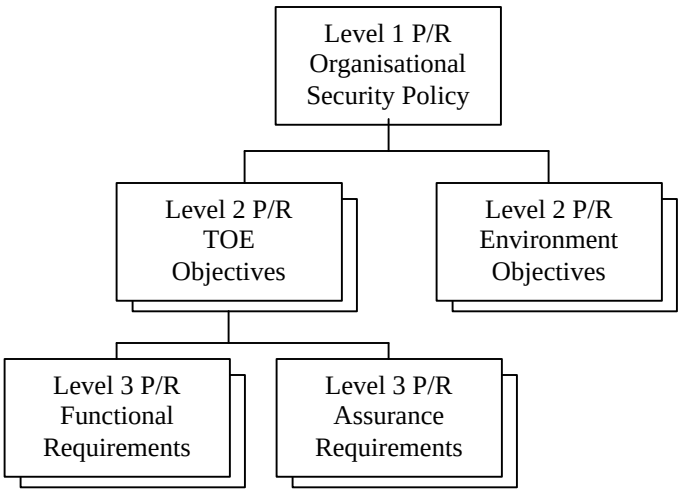

Figure 1: Policy/Requirement Hierarchy

A Level 2 policy/requirement is stated in terms of a specific implementing security discipline. For example, the Level 1 P/R "prevent unauthorized access to classified data based on clearance" would be supported by TOE objectives for labeling and mandatory access control as well as many environment objectives (e.g., physical, personnel). (The TOE and environmental objectives in a system PP correspond to Level 2 P/Rs. Level 2 P/Rs map directly to *system-specific policies* in the CAIO report.

The third, and lowest level P/R corresponds to the functional and assurance requirements in a system PP. (Level 3 P/Rs do not map to any of the security policies identified in the CAIO report.) Each Level 3 P/R states a specific feature or assurance in a way that is independent of exactly how it is implemented in the TOE or environment. It normally is the case that there will be multiple Level 3 P/Rs stated to support each objective.

OSP Taxonomy Considerations

As it turns out there are several challenges involved in creating a taxonomy of OSPs (Level 1 P/Rs). The first challenge is how to break the large domain of security policies into meaningful categories. At the highest level of abstraction the taxonomy includes three sets of P/Rs: functionality, assurance, and management/administration. We choose to use the traditional characterization of security functionality: confidentiality, integrity, availability, authentication, authenticity, and non-repudiation. We also included two other classes of P/Rs: system use (that are applied across multiple other functions) and releasability. Assurance P/Rs address both system/product and developmental considerations. Finally, a set of management/administration P/Rs are stated that deal with system use, administration, and management. This last set of P/Rs generally is implemented through procedures and environmental objectives.

The second challenge for creating the taxonomy is to determine the level of abstraction at which to state the P/Rs. For example, one could state only one confidentiality P/R—prevent unauthorized access to data. In this case, we chose to state three P/Rs related to unauthorized access to data—one for access to classified information based on clearance, one for access to classified data based on need-to-know, and access to sensitive (but unclassified) data. We felt it was important to state three P/Rs since they generate different objectives and functional requirements.

The third, and the most difficult, challenge is to ensure completeness—at what point can the PP writer say with confidence that all the stated OSPs actually fully cover all the organisation's policy domain space? We have used our collective years of system security engineering experience in developing ISs to derive what we believe to be a *reasonably complete* set of OSPs. We look to the community to help in expanding the completeness of the taxonomy.

A Taxonomy of Organisational Security Policies

This taxonomy identifies three basic classes of P/Rs: functionality, assurance, and management/administrative. The P/Rs are stated at a level of abstraction that is independent of whether they are implemented by the TOE, environmental controls, or both. The P/Rs are also independent of security disciplines that will be used to implement the P/R. In fact, one would expect that Level 3 P/Rs (i.e., objectives) would be stated for each of the *applicable* security disciplines: Physical Security, Personnel Security, Procedural (or Administrative) Security, Communications Security (ComSec), Computer Security (CompuSec), and Emissions Security (EmSec) also known as TEMPEST.

Functionality P/Rs

Confidentiality

Confidentiality is defined by NSTISSI 4009 as "Assurance that information is not disclosed to unauthorized persons, processes, or devices." Confidentiality has been the primary focus of security since the founding of the country. Thus, it is no surprise that initial computer security research and policy implementations focused on confidentiality. Although the focus of confidentiality is national security-relevant information, the P/Rs also can be applied to civil agencies and the commercial sector. Confidentiality P/Rs must be applied *at all times*—there are no exceptions. The supporting objectives will cover all security disciplines (information, physical, personnel, procedural, ComSec, CompuSec, Emissions).

T.CF-1. Prevent unauthorized access to classified data based on clearance.
Note: this policy is often called a mandatory access control (MAC) policy and directly applies to military and civil sectors. Although the commercial sector does not normally grant clearances, this P/R could be used where some level of personnel vetting is required.

T.CF-2. Prevent unauthorized access to classified data based on need-to-know.
Note: this policy is often called a discretionary access control (DAC) policy and is directly applicable to military and civil agencies.

T.CF-3. Prevent unauthorized access to unclassified sensitive data.
Note: although normally stated in the context of government organisations, this P/R also applies to commercial needs for controlling access to information (e.g., proprietary) based on a variety of criteria (most of which are instances of need-to-know)—position, organisation, role, as well as the "Chinese Wall Policy" [Brewer-Nash]. The P/R also applies to privacy concerns.

Integrity

NSTISSI 4009 defines integrity as "Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information."

Although we have the above definition, integrity continues to have many interpretations. We have a well defined and understood lexicon to deal with confidentiality—e.g., clearances that represent levels of trustworthiness of a person, and classifications that represent the levels of sensitivity of the data. Integrity has no similar lexicon for dealing with correctness and completeness. Also, in direct contrast to confidentiality, some integrity P/Rs may only need to be applied to a subset of the data. Each P/R below includes an indication of whether the P/R must be applied *at all times* or *selectively*. Also, the notion of distinguishing between *prevention* and *detection* P/Rs is introduced with integrity P/Rs.

T.IN-1. Prevent unauthorized modification to system hardware and software. (All times)

T.IN-2. Detect unauthorized modification to system hardware and software. (Selectively)
Note: objectives would address tamperproof techniques for hardware and software. This P/R is selective because while you certainly want to detect unauthorized changes to security-

relevant code, you may not care about all untrusted applications. In a similar manner, there may be a need to apply tamper resistant techniques to limited hardware assets.

T.IN-3. Prevent unauthorized modification (create, delete, change) of data. (All times)
Note: objectives will address different modes (transmission, storage) and may be based on all types of criteria: position, organisation, role, separation of duties. This "need-to-modify" P/R is effectively the integrity version of "need-to-know".

T.IN-4. Detect unauthorized modification of data. (Selectively)
Note: part of the instantiation of the P/R would be to specify which objects are subject to this P/R.

Availability

NSTISSI 4009 defines availability as "Timely, reliable access to data and information services for authorized users." How availability requirements can be implemented is probably the least well-understood area. Like integrity, we do not have the lexicon to describe levels of availability required. In effect, most availability P/Rs are really related to providing integrity for system resources; however, one P/R stands by itself.

T.AV-1. Prevent denial of service based on resource exhaustion. (All times)

Authenticity

NSTISSI 4009 does not provide a definition of authenticity but does provide two related definitions that together provide the meaning. Authenticate is defined as "To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IS, or to establish the validity of a transmission." Authentication is defined as a "Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information." Authenticity is a fundamental P/R needed to support other P/Rs (e.g., confidentiality, accountability, etc.).

T.AU-1. Determine authenticity of individuals who access system resources. (All times, although access to public web sites would be an exception.)

T.AU-2. Determine authenticity of data exchanged between internal components of the system. (Selectively)

T.AU-3. Determine authenticity of data from external systems. (Selectively)
Note: distinguishing between internal and external authenticity P/Rs is necessary since different objectives may be appropriate for each.

Accountability

NSTISSI 4009 defines accountability as an "(IS) Property allowing auditing of IS activities to be traced to persons or processes that may then be held responsible for their actions."

T.AC-1. Detect attempts by unauthorized personnel to access system resources. (Selectively)
Note: addresses both outsider and insider threat.

T.AC-2. Detect and respond to intrusions by unauthorized personnel. (All times)

T.AC-3. Detect attempts by authorized personnel to misuse systems resources. (Selectively)

T.AC-4. Reconstruct the who, when, and where relating to security-relevant incidents. (Selectively)

Non-Repudiation

NSTISSI 4009 defines non-repudiation as "Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."

T.NR-1. Provide proof of origin. (Selectively)

T.NR-2. Provide proof of receipt. (Selectively)

Releasability

NSTISSI 4009 does not contain a definition for releasability. In fact, the relatively recent operational requirement for coalition warfare has dramatically increased the need to release appropriate information to coalition partners.

T.RL-1. Provide capabilities to release data to coalition partners. (Selectively)

Generic System Access

There are several, access control related P/Rs, that apply to more than one class of functionality P/Rs. They include:

T.GS-1. Prevent access to system resources by unauthorized personnel. (All times)
Note: addresses computer resources through I&A as well as communications pipes through encryption.

T.GS-2. Prevent misuse of systems resources by authorized personnel. (All times)
Note: includes misuse of authorized functions (e.g., fraud).

T.GS-3. N-person control (Selectively)
Note: two-person control for authorizing an action is one example.

Assurance P/Rs

Where functionality P/Rs address *what* security features a system must have, assurance P/Rs address our *confidence* that the system does what it is supposed to.

System/Product Assurance

T.SA-1. Appropriate assurances will be provided that the security mechanisms in a system work properly, are always invoked, and *only do what they are supposed to*.

Developmental Assurance

T.DA-1. Appropriate assurances in the development environment will be provided demonstrating that over the life of the system the correct operation of the system is supported.

Management/Administrative P/Rs

These P/Rs address issues related to the proper use of the system.

Training

T.MT-1. All users will be provided effective training on system capabilities including security.

Procedures

T.MP-1. All users will follow prescribed procedures related to the access and use of system resources.

System Use

T.MS-1. Authorized users will use system resources only in the manner intended to perform their duties.

System Administration

T.MA-1. Authorized users will only be granted access to system resources that are required to perform their official duties. (Least Privilege)

Contingency Planning

T.MC-1.Appropriate plans will be in place to ensure continuity of business operations.
Note: covers system back-ups, off-site storage, hot back-up sites, etc.

Future Work

For the proposed taxonomy to be useful it has to be accepted by the community as a viable and useful tool. We hope to improve the taxonomy through community feedback to ensure that it adequately covers the security policy domain space. We also hope that the revised taxonomy can be incorporated into tools being developed to assist writing PPs [SPARTA]. We have begun work on an expanded taxonomy to include the supporting TOE and environment objectives. Figure 2 shows an example of expanding the confidentiality P/Rs to include supporting objectives. Creating a comprehensive list of objectives—also stated at a consistent level of abstraction—is still a work in progress, but we believe that such a set of objectives also would be helpful to system PP writers.

Finally, our observation is that a complimentary taxonomy of threats would be needed. A taxonomy of threats presents additional challenges since there are multiple levels of abstraction at which threats can be stated.

T.CF-1. Prevent unauthorized access to classified data based on clearance.

TOE Objectives

Labeling

O. All subjects and objects will be labeled to reflect the highest classification of its contents.

Mandatory Access Control

O. The TOE shall enforce a mandatory access control policy between its subjects and objects.

Environment Objectives

Marking

O. All classified hardware and removable media will be properly marked with the highest classification of information contained in the item and appropriate handling caveats.

Physical

O. Appropriate physical controls will be place to prevent access by unauthorized personnel to controlled facilities.

O. All classified material (i.e., HW, SW, removable media) will be stored in approved facilities or containers.

O. Where appropriate, classified containers will include tamperproofing.

Personnel

O. All personnel allowed unescorted access to controlled facilities will have the appropriate clearances.

Administrative

O. Appropriate administrative procedures will be in place to control access to classified data.

Communications

O. All communications lines outside of controlled areas will be properly protected (e.g. Type 1 encryption or a protected distribution system).

Emissions

O. Appropriate TEMPEST controls will be implemented.

T.CF-2. Prevent unauthorized access to classified data based on need-to-know.

TOE Objectives

O. The TOE shall enforce a discretionary access control policy between its subjects and named objects for individuals, groups, and all others.

O. The TOE shall enforce a discretionary access control policy between its subjects and named objects based on roles.

Environment Objectives

Personnel

O. All personnel will control access to material in their possession based on the need-to-know of the individual requesting access.

Administrative

O. Appropriate administrative procedures will be in place to control access to classified data based on need-to-know.

Figure 2: Confidentiality P/Rs with Supporting Objectives

Conclusions

A taxonomy of organisational security policies where the P/Rs are consistently stated at the same level of abstraction and where the totality of the taxonomy reasonably covers the domain space would be of significant help to system PP writers. We believe the proposed taxonomy is a significant first step towards providing a useful tool by the community.

Acknowledgments

The taxonomy presented in this paper was developed as part of providing system security engineering support under contract to the Air Force Information Warfare Center (AFIWC), Kelly AFB, TX.

References

[ISO/IEC 15408] *The Common Criteria for Information Technology Security Evaluation, Version 2.1.*

[ISO/IEC PDTR15446] *Guide for the Production of PPs and STs, Version 0.9.*

[PSCIA] *Practices for Securing Critical Information Assets*, January 2000.

[SPARTA] Protection Profile Writing Tool Kit

[Brewer-Nash] D.F.C. Brewer and M.J. Nash, “The Chinese Wall Security Policy”, *Proceedings of the IEEE Symposium on Security and Privacy*, 1989.