



Making a Better Protection Profile

James Arnold, AVP Technical Director
22 September 2009



Synopsis



- Protection profiles
- What's wrong with protection profiles?
- Making better protection profiles
- Conclusions and recommendations

Protection Profiles (PP)



- ~31 current PPs representing ~17 technologies
 - ~75% (24) PPs currently unused
 - ~50% (8) technologies unused
- ~50 archived PPs representing ~18 technologies
 - ~60% (29) PPs unused
 - ~50% (9) technologies unused
- Over 30 conformance claims each for operating system, firewall, and intrusion detection system PPs
 - Less than 10 conformance claims each in every other technology

Protection Profiles (PP)



- ~300 evaluations completed in the U.S.
 - ~25% with PP conformance
 - ~16% of those with multiple claims
 - Using 23 distinct PPs in 9 technologies
 - » ~20 PPs archived or obsolete
 - » ~5 products evaluated against ~3 **current PPs**
- ~65 evaluations on-going in the U.S.
 - ~38% with PP conformance
 - ~32% of those with multiple claims
 - Using 18 distinct PPs in 9 technologies
 - » ~11 PPs archived or obsolete
 - » ~11 products being evaluated using ~7 **current PPs**

Protection Profiles (PP)



- The U.S. currently requires PP or Evaluation Assurance Level 4 (EAL4) conformance for evaluation
 - ~38% of on-going evaluations claiming PP conformance
 - ~33% of these evaluations are targeting basic robustness PPs (meaning less than EAL4 is required)
 - ~62% of on-going evaluations have forgone PP conformance
 - ~63% claiming EAL4 or higher or
 - ~37% not meeting currently policy (due to age or some apparent exception)

Protection Profiles (PP)



- What do the statistics mean?
 - Increase in PP conformance claims
 - Scheme requirements for evaluation?
 - Increase in multiple PP conformance claims
 - Similarities in the requirements in certain PPs?
 - Relative decrease in the PPs used of those available
 - Revision of historically unused PPs?
 - Some technologies not represented in evaluations?
 - Lack of consumer demand?
 - Most PP conformance claims focused on few technologies
 - Experience, reuse, consumer demands?

Lots of unused PPs!

What's Wrong With Protection Profiles (PP)?



- PP Conformance Should be Preferred
 - Lower cost of security target development
 - Someone else has already done much of the work
 - Lower cost of evaluation
 - Just presume the a certified or validated PP evaluation results
 - More consumer buy In
 - PPs lend themselves to community recognition and comparison

So, what has gone wrong?

What's Wrong With Protection Profiles (PP)?



- Problems in PP Conformance
 - Problem requirements
 - Requirement bloat
 - Common criteria defiance
 - Obsolescence
 - Moving targets
 - Content reuse problems

What's Wrong With Protection Profiles (PP)?



- Problem requirements
 - While targeted at specific technologies, some PPs include requirements that are not often fulfilled by otherwise applicable products
 - Banner requirements for products that primarily communicate via standard network protocols or application programming interfaces (API)
 - Session limits for products designed to facilitate many simultaneous connections
 - Audit requirements for events that either no one would care about or that occur at extremely high rates (e.g., audit all network packet flow decisions or all cryptographic operations)
 - Resource quotas for primarily single user products

What's Wrong With Protection Profiles (PP)?



- Requirement bloat
 - Many current and historical PPs have a very large number (e.g., ~90) of security functional requirements
 - Not only are there large numbers of requirements, the requirements are often complex going well beyond relatively simply single statements
 - This necessarily introduces a lot of work in developing and evaluating security targets not to mention the subsequent evaluation
 - The requirements often require quite a bit of interpretation that adds significant risk to evaluations attempting such conformance

What's Wrong With Protection Profiles (PP)?



- Common Criteria (CC) defiance
 - Lately PPs have mostly gone back to using CC assurance requirements, but there was a period where many of the assurance requirements were explicit or extended
 - The former notion of Medium Robustness in the U.S. involved the use of assurance requirements that served as input to the defunct CC v3.0
 - Non standard assurance requirements are not subject to mutual recognition and there is little if any guidance for their application

What's Wrong With Protection Profiles (PP)?



- Common criteria (CC) defiance
 - Extended functional requirements remain popular in current PPs and even many non-extended requirements do not actually conform with the CC (e.g., illegal refinements)
 - The use of extended requirements introduces substantial risk, since in many cases the Scheme is required to make interpretations or issue judgment
 - Barring the occasional precedent, many decisions are project-specific leading to inconsistency for developers and evaluators
 - Extended requirements are often used to reference non-CC standards for compliance introducing additional work that is not well defined or constrained

What's Wrong With Protection Profiles (PP)?



- Common Criteria (CC) defiance
 - The U.S. Scheme has published its intent to provide explicit guidance with regard to the evaluation of requirements in PPs
 - While this is expected to improve consistency, it more likely will introduce more subjectivity (at least on the part of the Scheme)
 - It would be better to offer guidance relative to common evaluation methodology work units to be applied to all evaluations more-or-less uniformly

What's Wrong With Protection Profiles (PP)?



- **Obsolescence**
 - PPs are rarely kept up to date with the current version of the common criteria (CC)
 - Conforming with the current CC version often necessitates rationale with regard to PP conformance
 - For the most part, it seems lots of effort goes into the initial PP development or later for substantial rewrites, but little to no attention is paid to minor or incremental updates

What's Wrong With Protection Profiles (PP)?



- **Obsolescence**
 - PPs are occasionally retired (e.g., “sunsetting”) rendering them unusable for evaluation, except when the Scheme (at least in the U.S.) grants explicit permission
 - This is primarily a problem when there is a substantially different replacement or there is no replacement at all impairing PP conformance migration for some products

What's Wrong With Protection Profiles (PP)?



- Moving targets
 - Counter to obsolescence, occasionally draft PPs are offered (and even required in order to start an evaluation) for use in evaluations
 - PPs that change during an evaluation, particularly where lots of extended requirements are involved, can serve to increase risk and cost substantially
 - PPs subject to substantial interpretation or judgment by the Scheme or PP author represent a lesser form of moving target, but the consequences can be the same

What's Wrong With Protection Profiles (PP)?



- Content Reuse Problems
 - Extended requirements are sometimes ill- or not-defined
 - Refinements are sometimes “illegal” in the context of the Common Criteria
 - Threats and objectives sometimes dwell on assurances rather than functions
 - Correspondence rationale is sometimes incomplete or erroneous
 - While such problems can often be ignored when fully conforming, borrowing content is a different matter leaving a Security Target author responsible to resolve the problems left by the PP authors

Making Better Protection Profiles (PP)



- Obvious Ways to Improve PPs – Be Mindful of Problems
 - Emphasize key requirements for the core security problem
 - Keep PPs simple and to the point
 - Make sure that PP content is Common Criteria (CC) conformant
 - Publish PPs that are stable and as objective as possible
 - Stray away from the CC only where absolutely necessary

Making Better Protection Profiles (PP)



- Other Ways to Improve PPs – Potential Improvement Mechanisms
 - Use tools and references
 - Use Packages
 - Change the common criteria (CC)
 - Address non-CC standards otherwise

Making Better Protection Profiles (PP)



- Use of Tools
 - Publishing PPs in an open machine-readable form would enable the use of tools for better PP maintenance and also for better PP consumption
 - Developing content using tools (or converting content for use in tools) will help prevent or reveal problems in the PP
- Use of References
 - Including content by reference can produce similar benefits as using tools allowing the PP to automatically (implicitly) change when the references are revised rather than leaving the PP with outdated, copied content

Making Better Protection Profiles (PP)



- Use of Packages
 - PPs could be defined as packages that can be used in defined combinations, for example:
 - Required: Core Security Requirement Package
 - Optional: Audit Security Requirement Package
Remote Security Requirement Package
Flaw Remediation Assurance Requirement Package
 - One of: Evaluation Assurance Level 2 (or higher) assurance requirement package
 - Requirements in packages could consist of combinations of functional and/or assurance requirements
 - Requirements in packages could be defined as contingent on the inclusion of one or more other packages

Historically, PPs included requirements for the IT environment

Currently, some PPs have omitted those requirements and others have left them though the common criteria doesn't recognize them

They could be embodied in optional packages to be used if the target of evaluation happens to implement the function otherwise allowed to be assigned to its operational environment

Making Better Protection Profiles (PP)



- Change the Common Criteria (CC)
 - Offer more requirement flexibility
 - Conditional requirements
 - Alternative requirements
 - Allow the scope of security functional requirement (SFR) to be diminished in some cases (why should SFRs always be all or nothing?)
 - Allow more SFRs to require capabilities (“be able to”) rather than always-on functions
 - Treat Part 2 as a catalog that can and should be extended over time
 - There are a number of SFRs used and reused in PPs over time that haven’t made it into the CC
 - Require more guidance in PPs to assist security target (ST) authors
 - PP extensions could be treated as an ST-defined package

PPs need not be treated as a subset of STs

Making Better Protection Profiles (PP)



- Address non-Common Criteria (CC) Standards Otherwise
 - Non-CC standard conformance should be addressed via other programs
 - Conformance with some non-CC standard is not a security function or assurance relative to the CC
 - At most non-CC conformance expectations (or requirements) should be addressed as assumptions
 - Assumptions must be true for the evaluation results to remain valid in a given operational environment

The CC was not designed to evaluate other standards and should not be used for that purpose

Conclusions and Recommendations



- Lots of wasted effort on unused or little-used protection profiles (PP)
- Make PPs better
 - Focus on core technology – focused and to the point
 - Offer more flexibility using packages and available operations
 - Publish PPs in more consumable forms using tools and references
 - Reduce special cases and subjectivity
 - Pay attention to the CC to promote use (even if just in part)
- Revise the Common Criteria (CC)
 - Some improvements can be made now
 - Others require Common Criteria revisions
- While plenty of effort is spent creating PPs, some of that effort should be directed at making PPs as useable as possible

Contacts



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/>