Vendors and Government Cooperate to Produce a Practical Protection Profile

Roger French, Microsoft
Shaun Lee, Oracle
John Kendrick, Sybase

Agenda

- PPs and the NIAP/NSA PP Process
- The Basic Robustness DBMS PP
- Current State
- Conclusions
- Q & A

PP Development (circa 1993)

- Initially PPs were to replace earlier 'profiles' like C2 and B1 from the "Orange Book."
- Customers needed a way to express their security needs.
- Vendors needed a target to build to and to evaluate against.
- The idea was that customer groups would decide on a PP for their industry.
- It was a bit naïve.

Protection Profiles – The What

- Implementation independent set of security requirements.
- Objectives for solutions to similar customer IT security needs.
- Reusable.
- Requirements known as useful/effective in meeting identified objectives.

Protection Profiles – The Why

- Common target for vendors to:
  - Build to.
  - Evaluate against.
- For User communities to express IT security needs.
- Results:
  - Uneven take up by user communities.
  - Defined by developers along with TOE.
  - PP = product/system.

Protection Profiles – The Drawbacks

- A profile should not be a target.
- Specialty Profiles.
  - By Country.
  - By Industry.
  - By Agency/Ministry.
- Written by experts, for experts.
- Vendor experts vs. Consumer experts.

NIAP/NSA PPs

- Initially reflections of "Orange Book" classes.
- Current Aims:
  - US government has comprehensive set of PPs for key technologies.
  - Forge public/private partnerships for PPs in critical infrastructure protection.
  - Provide national and international convergence of key technology PPs.

NIAP/NSA Process Documents

- Development Process for US Government Protection Profiles (PP).
- Office of the Secretary of Defense Information Assurance Policy.
  - Basic Robustness (equates to good commercial practice.)
- Consistency Instruction Manual For development of US Government Protection Profiles For use in Basic Robustness Environments.

The DBMS PP - Steps to V1.0

- Various PP Drafts issued on IATF Website.
- Some vendors commented on draft versions.
- September 2004: Version 1.0 completed Evaluation.

The DBMS PP - Vendor Reaction

- October 2004: CCUF.
- Representatives from major DBMS vendors attended.
- Informal discussion on PPs:
  - Vendor issues with Basic Robustness DBMS PP
  - Current DBMS PP meant no evaluated products.
  - No benefit to customer or vendors.
  - Agreement to work together & with the author to achieve viable PP.

The DBMS PP - Vendor Cooperation

- Vendor Reviews in isolation.
- A Vendor Meeting.
- Work PP item by item:
  - Vendor Neutrality/technology independence.
  - Higher than minimum functionality.
- List of Comments compiled and sent to Sponsor.

The DBMS PP – Total Cooperation

- Sponsor interested in vendor comments, arranged meeting with PP authors.
- Each list item discussed or addressed.
- Mutual Goal: resolution for every item.
  - Some resolved in advance.
  - Some removed or modified to acceptance.
  - Some unchanged, but clarified with notes.
  - A few await resolution, but with agreement in principle.

Current State – A Sample Vendor Comment/Result

- Page: 29, Section: 5.1.1.3.
- Component: FAU_SEL.1.1-NIAP-0407.
- Comment: We need an application note to clarify manageability requirements on the granularity of inclusion/exclusion.
- Expected Results: Will be clarified to show intent to capture enough audit data, not necessarily capture only needed audit data.

Current State – Another Sample Vendor Comment/Result

- Page: 31, Section: 5.1.2.2.
- Component: FDP_ACF.1.4-NIAP-0407.
- Comment: In 1.2, if TOE did not support denial rules for a user, then you would choose "no additional explicit denial rules".
- Comment: Why doesn't this SFR have the same "DBMS-controlled" adjective as in the FDP_ACF.1.3?
- Expected Results: Will add application note to state that specific denial lists need not be implemented.

Conclusion - PPs for/by Users & Vendors

- Vendors are competitors with some common goals.
- Cooperation is possible.
- Cooperation is beneficial.
- Customers and vendors are not adversaries.
- PP developers need to use experts from all parties with a major stake in the results.
- Strong security in products that can and will be developed is the PP bottom line.

Conclusion - More for both 'sides' to learn

- Customers/Users have needs and wishes.
- Many of them are not related to security.
- They (needs & wishes) are still important.
- Vendors also have needs and wishes.
- Many of them are not related to security.
- They (needs & wishes) are still important.
- A practical PP addresses real products and real needs.
- We have a lot more to learn from each other.
- The two-level cooperation on the NSA DBMS PP is a good example.

Conclusion - Other PP's and CCv3/CEM

- DBMS PP is not the only PP.
- Other PPs could benefit from cooperative efforts:
  - PPs in development,
  - PPs in modification,
  - PPs in the concept stage.
- These same kinds of cooperative efforts could/will benefit Common Criteria V3.0 and CEM V2.0 as well.
- There's a Canadian TV show where the host reminds us "We're all in this together."
- We are!

Questions & Some Answers

- No.
- That hasn't been decided yet.
- We'll get back to you on that.
- See me after the session.
- Yes.
- Probably.
- Probably not.
- We hope so.
- Great question, next question.
- Are you volunteering?