Protection Profile Development for Hardcopy Devices: Lessons Learned

22 September, 2010

Brian Smithson
PM, Security Research
Ricoh Americas Corporation
Cupertino, California, US

Lead Editor, Protection Profiles
IEEE P2600 Standards Working Group
Agenda

- Background of protection profile development for hardcopy devices
- Challenges and solutions presented at the 8th ICCC - did those solutions work?
- Lessons Learned
- Wish list for Common Criteria Version 4
- IEEE Std. 2600 in practice
- Q&A
Background

- IEEE P2600 Standard Working Group formed in 2004, to:
  - Create a general standard for hardcopy device security
  - Create protection profiles for hardcopy devices
  - In particular, create a US Government Protection Profile

- Most major hardcopy device vendors participated

- IEEE Std. 2600 was published in 2008

- Four protection profiles were produced in 2009-2010:
  - IEEE Std. 2600.1 published and certified by NIAP CCEVS as the “US Government Protection Profile for Hardcopy Devices in Basic Robustness Environments” in 2009
  - IEEE Std. 2600.2 published in 2009 and certified in the German scheme in 2010
  - IEEE Std. 2600.3 published in 2009, not certified
  - IEEE Std. 2600.4 published in 2010, not certified
Challenges and solutions presented at the 8th ICCC

- By 2007, approximately mid-way through protection profile development, we had faced many technical challenges.
- Proposed solutions to some of those challenges were presented at the 8th ICCC:
  - What is the protection profile for a class of products that is used in a wide variety of operational environments?
  - What is the security problem definition where a combination of one or more security problems are solved by common objectives?
  - Can one protection profile satisfy a class of products that is composed of many combinations of functions and options?
- Let’s look at how well those proposed solutions worked...
Operational environments

- Hardcopy devices are used in many different operational environments, by many different kinds of users, for many different purposes
  - Government, healthcare, finance, enterprise, education, retail, small office, home, ...
- A security problem definition is based on how, where, why, and by whom a hardcopy device is used.

**What is the protection profile for a class of products that is used in such a wide variety of operational environments?**

- We defined four representative environments, distinguished by level of user accountability:
  A. Highly proprietary or regulated information
  B. General enterprise
  C. Public-facing /self-service
  D. Small/home office

- One protection profile for each environment
- The differences between environments A and B were small and somewhat artificial
Combinations of security problems that share objectives

- There are some security problems that are solved by common objectives. For example:
  - Identification and authentication is a solution to access control, auditing, and accounting problems.
  - Audit logs are a solution to detection of security events and conforming to some regulations.
- Within a given operational environments, customers will be concerned about some combination of those security problems.
- We don’t know which combination, but we do know that they want the objective in place.

What is the security problem definition where a combination of one or more security problems are solved by common objectives?

- We used Organizational Security Policies (OSPs) for some elements of the SPD
  - Data were defined as assets, and associated with threats of disclosure and alteration
  - All other security problems were described by OSPs
  - User authorization
  - Protection of customer networks
  - Audit logging
  - Power-on self-test
Combinations of product functions and options

- There are many product configurations for hardcopy devices
  - Single function printers, scanners, fax machines, and copiers
  - Multifunction devices combining several functions in one product
  - Security-relevant options, such as hard disks and networking

*Can one protection profile satisfy a class of products that is composed of many combinations of functions and options?*

- We proposed to make a “family of protection profiles” in a single document
  - One independent protection profile for each hardcopy function (print, scan, fax, etc.) and option (hard disk, network, etc.)
  - The container document provided a set of conformance rules that prescribe the protection profile(s) to which a security target must conform, based on the configuration of the product

- This approach was rejected, because common functions (e.g., user authentication) were distributed among the profiles, and their mutual relationship was unclear.

*Our eventual solution was to make a single protection profile with a common set of SFRs, augmented by SFR packages for each function and option.*
Lessons learned

In the process of developing protection profiles for hardcopy devices, we learned many other lessons:

- Organizing a vendor community
- Ownership
- Funding
- Customer requirements
- Common Criteria learning curve
- International acceptance
Organizing a vendor community

- In the US (at least), vendors who get together to decide important standards might be considered to be collusion, exposing participants to anti-trust laws and lawsuits

- Meeting under the authority of a recognized standards-setting organization (SSO) reduces exposure to anti-trust laws and competitive litigation

- There can be other benefits to using an SSO:
  - The SSO may have well-defined policies and procedures in place regarding:
    - Open membership
    - Appropriate/inappropriate topics for discussion
    - Intellectual property and patent disclosure
    - Operations, such as election of officers, voting, and record-keeping
  - The SSO may provide support for finance, legal, insurance, meetings, and other services
  - If the SSO is nationally or internationally recognized, it lends legitimacy to the effort

✓ We used the IEEE Standards Association for the development of protection profiles, and we issued those protection profiles as IEEE standards

Brian Smithson  
22 Sep, 2010
Ownership

- Who owns the protection profile? Who can make changes?
- Is the policy for making changes consistent with the policy for creating it?

- Consider the ownership issue at the beginning of the development process
- “Copyright © Vendor Community” may prevent unwanted changes or derivative works
- Make sure that you can make it freely available:
  - Many SSOs are supported by the sale of standards and will not give anything away for free
  - Common Criteria schemes require that PPs are freely available
  - If you are using an SSO, negotiate the copyright issues up front

IEEE-SA holds the copyright on IEEE hardcopy device protection profiles, which means that the IEEE P2600 working group retains control over changes and updates

It was necessary for P2600 member companies to purchase distribution rights from IEEE to make the protection profiles freely available before any scheme would certify them

If we want to make changes or updates, we will again need to negotiate the purchase of distribution rights
Funding

- Lab fees for evaluation of protection profiles can be substantial
- Some schemes have fees associated with evaluation oversight and certification

- It is difficult to get a firm quotation until the protection profile is largely completed; however, some labs will provide a budgetary quote, off-the-record
- It can be difficult to get funding from vendors unless they receive some benefit or special treatment for doing so (press releases, product listings, etc.)
- It is easier to ask companies for many small payments than one large payment
- If someone outside of the vendor community offers to pay for or otherwise sponsor protection profile evaluation and certification, be careful (see: “Ownership”)

✔️ We raised money from almost all of the P2600 member companies
❌ Costs were identified late in the process, so we asked companies for one large payment
✔️ We cashed the checks before the economy melted down 😊
Customer requirements

- Government requirements can be difficult to pin down
  - When we started, NIAP was an NSA - NIST partnership with plans for commercial outreach (this encouraged our goal of creating one government PP and three commercial PPs)
  - NIST dropped out, and NIAP focused solely on government agencies
  - Now NIAP is promoting a new approach to protection profiles and EALs
  - National CC schemes may not have the final word for government agencies’ C&A processes

- Commercial requirements may be even more difficult to pin down
  - There are more commercial customers than there are governments
  - Some commercial customers have even less understanding of CC than do government agencies

- Expect a moving target (or, work very quickly 😊 )
- Don’t expect requirements up front; propose something and get their feedback
- Try to get sample government and commercial requirements from team members
- Don’t overestimate growth of commercial market demand for CC

- The P2600 working group made frequent contact with NIAP
- Commercial requirements were not so clear; we should have focused on one protection profile and then considered doing others based on market demand
Common Criteria learning curve

- Writing a protection profile is not like writing a security target
- Product certification experience is helpful, but not sufficient

- You need a team with diverse expertise:
  - Product marketing – as a proxy for customer requirements
  - Product engineering – to make sure your SFRs can be implemented!
  - Information security – to follow established security concepts, practices, and terminology
  - Standards development – to manage the process effectively, efficiently, and fairly
  - Common Criteria evaluation, from the perspective of multiple vendors, labs, and schemes – to ensure the successful evaluation of the protection profile and of conforming products

✅ The P2600 working group had a good mix of expertise
  - Member companies provide product, security, and standards expertise
  - We received guidance by inviting labs, schemes, and CC consultants to participate in meetings
  - Our lab provided expert consulting and (separately) evaluation

❌ We should have engaged a lab at a much earlier stage of protection profile development
International acceptance

- Although our major focus was on US government acceptance, most hardcopy devices are CC certified in Japan
- National schemes are unlikely to commit to accept a protection profile until they have seen a complete draft (if even then)
- Different schemes may have very different interpretations of the CC
- Acceptance of a protection profile does not necessarily mean acceptance of conforming security targets (!)

- Consider both the scheme under which the protection profile will be certified and the schemes under which conforming products will be certified
- Be creative when seeking feedback from schemes; employ resources that are local to the national scheme

- The P2600 working group recognized the importance of international acceptance
- We used a major trade association to get feedback from the Japanese scheme
- We used our lab to get feedback from the German scheme
Wish list for Common Criteria Version 4

- A way to accommodate product functions and options in protection profiles
  - It is different from accommodating product functions and options in a security target
  - If a function or option is identified in a protection profile, it must be present in the conforming product
  - For example, an multifunction device might have a fax modem or it might not have a fax modem
  - “Modes of operation” will not work, because the function or option may be absent from the Target of Evaluation (TOE)

- A way to describe objectives in terms of what the TOE shall *not* do
  - For example, we needed to ensure that external interfaces of the TOE could not be maliciously bridged
  - We could not use flow control requirements, and so we wrote an extended component

- A way to fulfill objectives by architecture, not just by TOE Security Functions (TSFs)
  - For example, customers want to be assured that you cannot make a data connection to the fax modem and use it to establish a connection to the TOE’s network interface
  - Typically, this is prevented by the architecture of the TOE: there is no data path from here to there

- A way to describe threats and objectives that occur when the TSF is not active
  - For example, data stored on a hard disk is vulnerable to disclosure when the TOE is powered off
  - We found it necessary to write an extended component for this
IEEE Std. 2600.1 in practice

- **Vendor experience so far:**
  - Vendors wrote the protection profile, and yet, some difficulties have been reported in understanding how to write a conforming security target
  - The protection profile is intended to be abstract and architecture-independent, and yet, there have been some reports of difficulty describing product functionality in a way that matches the assets, threats, objectives, and requirements are described in the protection profile
  - Several schemes were consulted during protection profile development, and yet, there have been reports of differing interpretations among schemes
  - All things considered, the protection profile is working as expected

- **Certification progress:**
  - One product has been certified to conform to IEEE Std. 2600.1
  - At least three other vendors have multiple products under evaluation
  - By estimate, eight to ten certificates will be issued in the next six months, certifying thirty to forty conforming product models
Questions?

- For more information:
  - IEEE P2600 working group: [http://grouper.ieee.org/groups/2600](http://grouper.ieee.org/groups/2600)
  - Sponsor’s certified products: [http://grouper.ieee.org/groups/2600/conforming_products.html](http://grouper.ieee.org/groups/2600/conforming_products.html)
  - 8th ICCC presentation: [http://grouper.ieee.org/groups/2600/presentations/8iccc/smithson.pdf](http://grouper.ieee.org/groups/2600/presentations/8iccc/smithson.pdf)
  - This presentation: [http://grouper.ieee.org/groups/2600/presentations/11iccc/smithson.pdf](http://grouper.ieee.org/groups/2600/presentations/11iccc/smithson.pdf)

- To contact the presenter:
  - About IEEE P2600: brian.smithson@ieee.org
  - About Ricoh: brian.smithson@ricoh-usa.com – [http://www.ricoh-usa.com](http://www.ricoh-usa.com)

- Acknowledgements:
  - Input for this presentation provided by Carmen Aubry, Océ; Lee Farrell, (formerly) Canon; Ron Nevo, Sharp; Alan Sukert, Xerox; and Sameer Yami, (formerly) Toshiba

Thank you – Teşekkür ederim