

Brian,

The comments you refer to have been made by someone from atsec working on an evaluation for HP. We have separated the team working on printer evaluations from the people that do the P2600 Protection Profile evaluation to avoid any conflict of interest.

Concerning the requirement FPT_STM.1: This comes into the PP from a dependency in FAU_GEN.1, which requires the audit record generated to include the date and time of the event that triggered the audit record to be produced. So there is a requirement to have a reliable source for this information. When you include FPT_STM.1 in the functional requirements for the TOE, the requirement states that "The TSF shall be able to provide reliable time stamps". So the generation and maintenance of the date and time has to be part of the TSF which would require to have the design information available describing how this is done. The use of an external time source via NTP (as provided in the PP you gave as an example) is acceptable as long as the implementation of NTP protocol itself is part of the TSF such that its correct implementation and use can be validated as part of the evaluation. In this case a Security Target for a product that uses NTP should state an assumption that the provider of the time service is reliable.

In your case you have to be aware that the inclusion of FPT_STM.1 as a requirement for the TOE requires the functions to generate and manage the date and time to be part of the TSF, either directly or via a trusted time source and a secure link to this time source. It would not be possible to use the time function of an underlying operating system used within the device unless this operating system itself is considered to be part of the TSF. I can imagine that a number of manufacturers of devices that are intended to comply with a P2600 PP would like to treat the underlying operating system as part of the IT environment. In this case they would just the function of the underlying operating system to provide the date and time. Strictly speaking this would require the operating system (or at least the part that provides and manages the timer) to be part of the TSF - which may make the evaluation more complicated than it needs to be. This problem could be solved if the operating system itself has been evaluated with FPT_STM.1 included in its Security Target since in this case one could draw on an already evaluated component and a function that has been part of the evaluation.

In your case a product needs to show only demonstrable compliance with at least one of the PPs. This makes things a little bit easier. Still this does not allow to push a requirement for the TOE to the environment. I agree that you should try to stay away from defining extended components. You should discuss within the group if the provision and management of a reliable time stamp by the TOE itself is a requirement you make mandatory or if you allow a TOE to use a time stamp provided by the environment. Using a reliable time stamp provided by the environment can be used as an argument in the rationale how the dependency to FPT_STM.1 is satisfied. The CC allow the author of a ST or PP to provide arguments why a dependency between SFRs defined in the CC either does not apply or is resolved in a different way. In your case my suggestion would be that you leave it to the individual STs if the the reliable time stamp is provided by the TOE (and its TSF) or by the IT environment. Keep in mind that even if you allow the time stamp to be provided by the environment a specific product may still provide such a time stamp itself and claim FPT_STM.1 in its Security Target.

Concerning user authentication the situation is similar (but slightly

more complicated). What is not acceptable is a TOE that just asks the IT environment if the user has been successfully authenticated and therefore relies totally on the environment for user authentication. Then there are solutions that partly rely on the environment for authentication. One example is a system that just relies on the environment to store the data used for authentication (userid, password) in some protected way in an external database and where the authentication process itself is performed by the TOE itself, which retrieves the data from the external storage and compares those to the data entered by the user. This would be an acceptable solution for user authentication performed by the TOE. Another potential solution is where the TOE receives the userid and the authentication credentials and just passes them on to a system in its environment for verification. This system then tells the TOE if it was able to successfully authenticate the user. In this case the TOE itself does not perform the authentication but just acts as an intermediate in the authentication process. In this case the TOE at a first glance seems to provide an interfaces for user authentication but in reality just provides a proxy to an external authentication function. Strictly speaking this would not be compliant with a requirement for the TOE to perform user authentication. There is a common understanding within the different CC schemes that a security functional requirement for the TOE must be fully satisfied by the TSF of this TOE and can not be satisfied by a function in the TOE environment.

In the case of user authentication this requires that the TSF is in full control of the authentication mechanism and may only rely on the environment for the storage of user security attributes (including passwords) as long as the security functions of the TOE and/or the assumptions on the environment ensure that this data is protected from unauthorized access that would allow to spoof or bypass the user authentication function.

I think with respect to user authentication the members of your group should identify which user authentication scenarios they intend to allow for a product compliant with a P2600 PP. Based on this set of scenarios one can then decide how to best phrase the requirement in the PP to allow for all those scenarios. There is a potential to define options where one defines two (or more) set of assumptions, objectives and SFRs both addressing the same set of threats and where the author of the PP requires an ST to take one of the defined options. Remember that in one of our talks with NIAP Shaun Gilmore stated such options are acceptable for NIAP and we recently have developed a PP for BSI that also defines options. The CC does not explicitly allow such "options" but also does not explicitly forbid them. In a recent drafting meeting for ISO 15408-2 (the ISO version of part 2 of the CC) held in Madrid, this was one of the issues discussed. Since the Chairman of the CCMB (Miguel Banon) as well as the chairman of the CCMC (Mats Ohlin) participated at this meeting, there is a good chance that such a greater flexibility in developing Protection Profiles will get included in future versions of the CC. A Protection Profile may deliberately allow a product developer to choose how his product counters threats allowing the PP to be used in different operational environments as long as the threat is countered efficiently. This is more than just "demonstrable" conformance, since demonstrable conformance still does not allow to add assumptions or security objectives to the environment that are not already in the PP.

So far on your questions. Regarding the phone conference this morning, I think it went well and I am not too much concerned about NIAP requiring modifications that are not acceptable to other schemes. I think most of

the comments made by Howard are valid and should be taken into account. I think with comment no. 3 Howard has recognized himself that the requirement FTA_TAB.1 is not a realistic one especially since in the CC terminology a "user" may well be another IT system. How to "print" a banner to another system connecting itself over the network using standard protocols that also perform authentication (e. g. TLS) is something NIAP will have a hard time to answer. In the real world such a banner - if it is required by an organization - will be generated and displayed at the user's system in accordance with a system policy. Normally it is not the printer that is responsible to tell the user about the usage policy but this is centrally defined and applies for all printers the user is allowed to use within the system.

so far my comments. I hope they help. I will perform a more detailed and in-depth analysis of the PP soon and send you my comments.

with best regards

Helmut Kurth

Brian Smithson wrote:

> Ken and Helmut,

>

> During today's P2600 WG meeting, we received comments from Brian Volkoff of HP regarding the subject SFRs. He attributed those comments to someone from atsec, but I do not know if either of you might have been involved. I am hoping that we can discuss them with you or you could forward us to someone else at atsec who might have made the comments. I hope that we can get some clarification of this matter promptly so I can relay the information at tomorrow's WG meeting.

>

> The issues with these three SFRs are similar: timestamps, identification, and authentication, might actually be performed by services that are external to the TOE. Some implementations may feature an administrative function that allows the TOE to use either local time/ID/auth or external time/ID/auth services, so we must be able to accommodate either or both options in the PP.

>

> The proposal as stated in Volkoff's comments was to define an extended component that explicitly allows external services to fulfill the time/ID/auth functions. In the case of timestamps, the proposal also gave an option to remove FPT_STM.1 with some rationale for its removal.

>

> The WG position on this matter is that we would strongly prefer /not/ to define extended components. This may be particularly important if we are to successfully negotiate with NIAP to not allow NIAP-specific SFR interpretations. Can we do so and still permit either/both local and external services for time/ID/auth? I think so, but I do not have enough experience with CC evaluation to know for certain. Let me explain:

>

> When I read the subject SFRs and the CC part 2 appendix, I don't see that the SFRs require the TOE to actually provide generation of time values or actually perform identification and authentication functions. As I read them, these SFR only require that "the TSF shall provide reliable time stamps", "the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user", and "the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated

actions on behalf of that user", none of which require that the underlying functions must be performed by the TOE. I believe that the TSF could provide reliable timestamps if it received the correct time from an external server, and could identify and authenticate a user if it passed the user credentials to an external server for validation and received a trusted response.

>

> Ms Carmen Aubry of Oce, who you may know, did find some precedents that may help. Take a look at http://www.commoncriteriaportal.org/files/ppfiles/PP_TFFWPP-MR_V1.1.pdf which is a US Government PP for Traffic Filter Firewalls, Medium Robustness, EAL4, far exceeding our own requirements:

>

> They use FTP_STM.1 without extensions, and on page 111 of the PP they state that the administrator can select either local timestamp generation or external NTP services.

>

> On page 63, they use an explicit version of FIA_UAU.1 that specifies authentication must be performed locally. I believe that their use of an explicit version of the SFR indicates that the non-explicit CCRA FIA_UAU.1 accommodates either local or external authentication services.

>

> So what does atsec think about these issues? Can we use FPT_STM.1, FIA_UAU.1, and FIA_UID.1, in their unchanged form from CCv3.1r2 part 2, to allow an ST author to satisfy those SFRs with /either or both/ local or remote performance of time generation, user identification, and user authentication services?

>

> If so, do you think we will need to also add any kind of requirements about trusted paths to such services, and/or an environmental objective about trusting those services? I hope not, because such requirements might imply that all conforming STs must address such requirements even though some products may not use external services.

>

> I would really appreciate if you can give any kind of response to this message during your Tuesday so I can relay the answers to the WG meeting on Wednesday. I'd really like to put these issues to bed at the WG meeting while we have the opportunity to get consensus from the WG in real time.

>

> Thank you,

> --

> Regards,

> Brian Smithson

> Project Manager, Security Research

> PMP, SSCP, CISSP, CISA, ISO 27000 PA

> Advanced Imaging and Network Technologies

> Ricoh Americas Corporation

> (408)346-4435

--

Helmut Kurth, atsec information security
www.atsec.com