UNIVERSITÄT
HILDESHEIM

Universität Hildesheim • Marienburger Platz 22 • W-3200 Hildesheim

Dr. Andreas Pfitzmann
Institut für Informatik
Gebäude Samelsonplatz 1

☎ +49 5121 883735 (office)
☎ +49 5121 83312 (home)
Fax +49 5121 860475
e-mail pfitza@informatik.uni-hildesheim.de

Commission of the European Communities
Directorate XIII/F
InfoSec Central Office (TR61 3/9)
Rue de la Loi, 200
B - 1049 Brussels
Belgium

Fax: 0032 2 236 6271
E-mail: ISCO@postman.dg13.cec.be

28th May 1992

Subj. **ITSEM Comments to V0.2**

Dear Ladies, dear Sirs,

following please find my **Statement of Observations** concerning the Information Technology Security Evaluation Manual (ITSEM), V0.2, April 2, 1992.

If there is new material, e.g. a synopsis of all statements of observation, please send it to me. At any time, I am interested to receive answers to my questions and feedback about my comments and/or the future versions of ITSEC and ITSEM.

I appreciate the comments of Kai Rannenberg (Technical University of Berlin).

Yours sincerely

A. General Observations

Except for the first and the last general observation, which concern ITSEM as a whole, the other observations are in a sequence which reflects the ordering of the referenced Paragraphs within ITSEM.

1. Lack of correction of ITSEC problems

Except in the area of re-evaluation and re-use of evaluation results, ITSEM V0.2 does not even try to overcome the deficits of ITSEC V1.2. This means that all points raised on ITSEC V1.2 in my Statement of Observations of November 29, 1991, and that of the *Data Protection and Data Security Task Force* of the *German Society for Informatics* (more than 18000 members) of February 24, 1992, are still valid except those in the respective Chapter 5. Both, me and the *German Society for Informatics* are not only waiting for an answer regarding the contents of our statements, but we are waiting for the urgent needs of an information society being really and thoroughly addressed by the ITSEC/ITSEM actors. Except for its Chapters 8 and 9, ITSEM V0.2 is a missed opportunity in this respect.

2. ITSEC needs much deeper and therefore more improvements than admitted in ITSEM §1.5

There are much more severe deficits in ITSEC V1.2 than those admitted here. Given the two public Statements of Observations mentioned above, §1.5 of ITSEM V0.2 raises severe concerns whether its authors are capable and willing first to understand and thereafter to work on overcoming these deficits. Therefore, the CEC should sponsor the development of alternative proposals and evaluation experiences for future versions of ITSEC and ITSEM.

3. Who oversees the Certification Bodies?

It is not only necessary to oversee evaluations (and thereby ITSEFs) as noted in §1.16 of ITSEM V0.2, but Certification Bodies as well. For inside the European Community, an appropriate institution might be the European Parliament.

4. Several classes of potential attackers are not covered

As ITSEC, ITSEM does not – by far – consider all potential attackers. E.g., the designers of the TOE might implant a universal Trojan Horse, the designers of the tools used in generating (and analysing) the TOE might implant a transitive Trojan Horse, and so forth, as noted already in my statement of observations to ITSEC V1.0. In ITSEM, this deficit becomes even more explicit:

In §3.34, it is completely forgotten that the designers of the TOE know details which are not in the public domain *and* which they did not obtain maliciously.

In §4.192 b) and c) the following persons have to be added:

Designers of the TOE;
Designers of tools used to build the TOE;
Designers of tools used to build tools used to build the TOE;
and so forth.

This has to be reflected throughout the rest of ITSEM.

5. Threats cannot be enumerated and must be specified the other way round

As is well known both within the fault tolerant computing and within the security community, neither errors nor threats can be enumerated with a reasonable confidence in completeness. Therefore, errors and threats must be specified the other way round, i.e. it has to be stated what properties of which components and subsystems are assumed.

If necessary, the assumptions have to be qualified:

1) Under which circumstances are they considered to be true?
2) In distributed systems, it has to be stated: For whom are they considered to be true? (In other words: Who has to rely on them?) In general, in distributed systems, the one who has to rely on an assumption has to be the one who can make it true.

Within their computing capabilities, components and subsystems with assumed properties may behave arbitrarily as long as they do not thereby violate these explicitly stated assumptions. All other components and subsystems may behave arbitrarily within their computing capabilities. For a TOE to be considered secure, all its security properties have to be deduced from these assumptions. If these assumptions are reasonably weak, this deduction gives the best attainable confidence in the security of the TOE. Therefore, formulations like "... countering the threats enumerated in the security target." (ITSEM V0.2 §3.39) and "... covers all threats enumerated in the security target." (ITSEM V0.2 §10.23) are not state of the art and misleading to users of ITSEM.

6. The discrimination between strengths of mechanisms in only three classes (basic, medium or high) is very poor and not adequate.

ITSEM §4.193 is a clear indication that the discrimination between strengths of mechanisms in only three classes (basic, medium or high) is very poor and not adequate. By comparing the statements given in b), d), and f) it is evident that resistance to completely different severe attacks is mapped to the same class "high".

7. Requirements for Tools and Techniques are missing

In Chapter 7 of ITSEM V0.2, essential requirements on tools and techniques are missing. In part, this is due to the fact that ITSEC does not state, as in [Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3-88784-200-6; German Information Security Agency, 1989, p. 53], that evaluation levels beyond E6 are possible, very desirable, and might be defined in the future.

One reason for this and the reason why *essential* requirements in Chapter 7 of ITSEM are missing is that there are **transitive Trojan Horses**, cf. the Turing award lecture by [Ken Thompson, Reflections on Trusting Trust; Communications of the ACM 27/8 (1984) 761-763]. These transitive Trojan Horses can spread through the used tools into the TOE. If the Trojan Horses are **universal** ones [D. Denning: Commutative Filters for Reducing Inference Threats in Multilevel Database Systems; Proc. 1985 IEEE Symp. on Security and Privacy, April 1985, Oakland, Computer Society, 134-146], this threat becomes especially severe.

Examples for evaluation levels beyond E6 are

Level E7: Verified design history of all tools used to develop the TOE.

Level E8: Verified design history of all tools used to develop tools used to develop the TOE.

and so forth.

The ultimate level would require that all (recursive definition!) used tools have verified design, i.e. you need some form of secure bootstrap in generating these tools.

The implictions for Chapter 7 of ITSEM are obvious: T&Ts must either have completely diverse design history (if possible between each other and – most important – in any case between the TOE and any T&T) or must be checked by the evaluator thoroughly. Therefore, in §A.116 b) (or at least in the corresponding Paragraph on the highest evaluation level to be defined) it has to be stated that the used tools themselves have to be checked and how this shall be done thoroughly. In §A.119 (or at least in the corresponding Paragraph on the highest evaluation level to be defined), the source code of all compilers used has to be checked.

8. All acronyms should be explained and references given

Please give both explanations and references to all acronyms used within ITSEM. Otherwise, reading and understanding ITSEM is unnecessarily difficult. An example might be "SPADE" in ITSEM V0.2 §3.61 b) first indent.

B. Specific Observations

page 14 §2.26 e) 3. indent:

"...configuration data, ... which could affect security." It is dangerous to leave this decision to the sponsor. If this sentence is not changed, it has at least to be clarified what happens if a sponsor, e.g. a manufacturer of IT-products, does not adhere to this requirement.

page 14 §2.27 b):

What is done with this information? Who has the duty to inform all users of the TOE on this?

page 15 §2.32:

Delete comma in the first line.

page 18 §2.43:

The rating of cryptographic mechanisms has to be done by the scientific community, in this case represented by the ITSEF, and has to be international and as objective and reproducible as possible. This requires that all cryptographic mechanisms be published in any detail. Any secret mechanisms are not suitable for certified secure systems.

page 51 §4.84:

This Paragraph is dangerous at least as it is formulated at the moment. If, as a sponsor, I would like to get an insecure TOE certified, I would deliver more information than I am obliged to. Because I can always say that this information has been used, I can object to nearly any penetration test whose result I do not like.

page 55 §4.114:

It is only reasonable to require repeatability for *deterministic* machines. Since not all TOEs will be deterministic, the applicability of this Paragraph has to be restricted.

page 58 §4.132:

Damage may not only be done to enterprises, but to citizens as well, both in the role of user (the one using the TOE) and usees (the ones whose person-related data are processed).

page 70 §4.192 d) last three lines:

For keeping the combinations restricted, the given restriction is appropriate, since one can always use the upper bound. But in reality, the given restriction may be meaningless, e.g. there may be hacker shareware with a nice user interface, which may be so easy (but nevertheless efficient) to use that even a layman can profitably use it. ITSEM should clearly state this.

page 73f §4.203:

The meaning of this Paragraph is unclear to me.

page 119 §8.4:

"... it is the responsibility of the Sponsor to classify the change type and determine the consequences for the certificate." It is dangerous to leave this decision to the sponsor. If this sentence is not changed, it has at least to be clarified what happens if a sponsor, e.g. a manufacturer of IT-products, does not adhere to this requirement.

page 123 §8.19:

The scheduler of an operating system is security *enforcing* (and not only security relevant) if the TOE comprises any availability requirements.

page 124 §8.21:

The indents "Result i:" and "Result d:" are both in contents and especially in wording according to the very bad habit of first stating the result and only thereafter starting to think about the basic facts. For security, I strongly discourage to follow this bad (although widely used) practice.

page 136 §9.33 S7:

Is this a statement? Shall this be checked?

page 140 §10.48:

It is hard to believe that no relevant progress in IT security has been achieved by the computer security community after 1977 (in words: after the year nineteenhundredseventy-seven) which is worth referencing here.

page 196 §C.22 b):

As explained in *7. Requirements for Tools and Techniques are missing*, even configuration control for the tools used is a security issue. The formulation in this Paragraph "... believed that they were being followed." seems to be completely inadequate to that fact.

C. Suggestions for Additions or Modifications

See under B. Specific Observations

page 42 §4.29:

The last sentence is clarified, if "detail" is inserted: "The more detail that is specified in the security target, ..."

page 47 §4.58:

The last sentence says the contrary of what the authors want to say and it must read, e.g.: "If all this is not the case, a verdict can be assigned."

page 57 §4.124 a):

The sentence inside the brackets must read: (i.e. at least one error, as defined later in this section, is not fixed by the Developer)

page 71 §4.196 a):

"C2.10" should read "C.210".

page 97 §6.66:

The content of this Paragraph should be written more clearly. What are "... isolatable components of the hardware *components* ..." ? I assume you want to say: "For the hardware components (as described above), the firmware description should specify all version/release numbers for isolatable firmware components that are relevant to the ..."

page 105 §7.29:

It is implicitly assumed that all used T&Ts (and in some cases, the TOE) are deterministic. This assumption should be made explicit, since it is a restriction on the allowable T&Ts (and the evaluatable TOEs).

page 125 §8.23 Group 1 R2:

Insert an "o" in "chose", i.e. "... should the Sponsor choose not to supply ...".

page 126 Figure 8.2:

State that "X" means: impossible combination.

page 129 Headline of Chapter 9:

The headline makes more sense to the reader if "for Composition" is appended. "RE-USE OF EVALUATION RESULTS FOR COMPOSITION" avoids the confusion with Re-Evaluation. This is especially helpful if someone starts to understand ITSEM by reading its Table of Contents.

page 134 §9.28:

I suppose that the stated conditions are not meant to be *necessary*, but are meant to be *sufficient*. Therefore, the first sentence must be formulated the other way round: "For example, if the combination is according to case 1, the following conditions are sufficient for component C3 to maintain its predicates P3:"

If the interface of C2 is passive in the sense that no operations trigger themselves, then "Cond 3:" can be weakened, which makes the whole Paragraph much more useful. Please append: "If no operations of C2 trigger themself spontaneously, it is sufficient that the consumer interface of C1 is a subset of the producer interface of C2."

Please define the meaning of predicate p1 "makes up" predicate p2 or use the usual terminology, if applicable, throughout the rest of ITSEM, e.g. predicate p1 "implies" predicate p2.

Please define the meaning of "Cond 5:". What shall mean "... be exploitable with respect to a predicate."?

page 134 §9.29 first two indents of the 2nd indent:

If §9.28 is left unchanged, "subset" must be replaced by "proper subset" and "superset" must be replaced by "proper superset". If you change §9.28 according to my proposal, you have to remove the first indent of the 2nd indent.

page 135 §9.29 fourth indent:

"cond 6" must be replaced by "cond 5" and "cond 7" must be replaced by "cond 6".