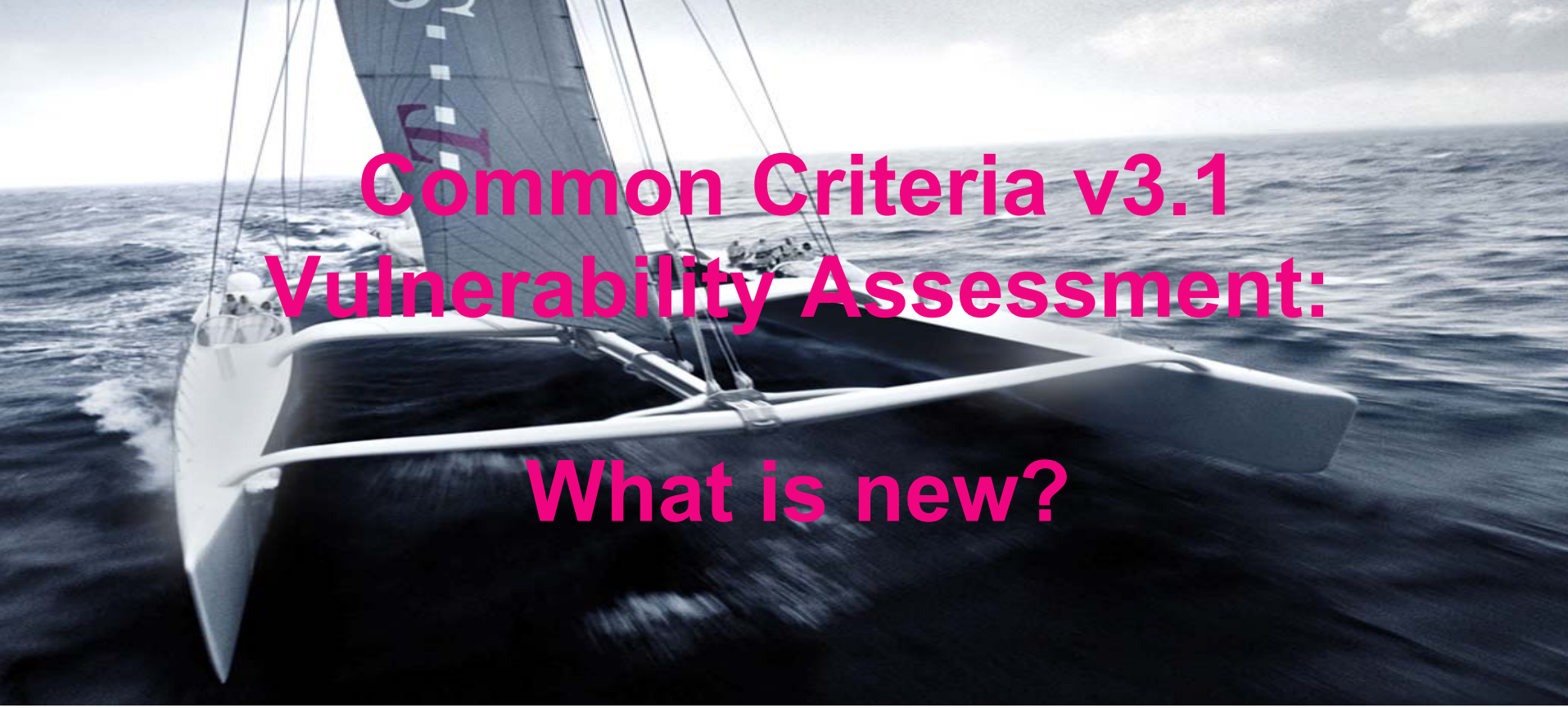


Common Criteria v3.1 Vulnerability Assessment:

What is new?

Dr. Igor Furgel

T-Systems GEI GmbH

T · · Systems ·

Road Map

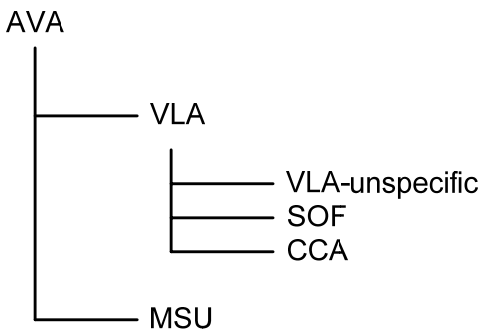
- CC Part 3, Class AVA
- CEM, Class AVA
- CEM, Annex B

T Systems

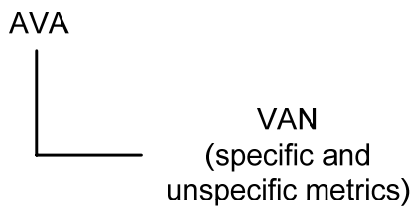
CC Part 3, Class AVA

- Assurance class AVA consists now merely of a single assurance family: AVA_VAN
- Objective of AVA_VAN is to determine, whether potential vulnerabilities identified could allow attackers to violate the **SFRs**.
- The family AVA_VAN is completely to perform by the evaluator; the developer stands on the sidelines.

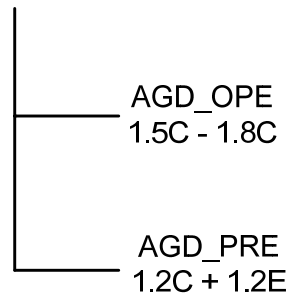
CC v2.x



CC v3.x



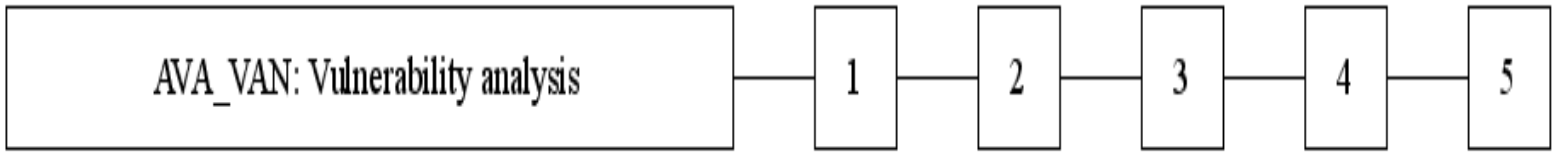
MISUSE:
mentioned (but not addressed!) in AVA;
actually addressed in AGD_OPE and AGD_PRE



T · · Systems ·

CC Part 3, Family AVA_VAN

- The assurance family AVA_VAN consists now of 5 components:



  - AVA_VAN.1 Vulnerability survey
    (TOE Resistance against Basic Attack Potential)
  - AVA_VAN.2 (Unstructured) Vulnerability analysis
    (TOE Resistance against Basic AP)
  - AVA_VAN.3 Focused vulnerability analysis
    (TOE Resistance against Enhanced-Basic AP)
  - AVA_VAN.4 Methodical vulnerability analysis
    (TOE Resistance against Moderate AP)
  - AVA_VAN.5 Advanced methodical vulnerability analysis
    (TOE Resistance against High AP)

T · · Systems ·

CEM, AVA_VAN.1: Survey 1/2

- Objective is to determine whether the TOE, in its operational environment, has easily identifiable exploitable vulnerabilities.
- Input:
  - ST, AGD and TOE for testing,
  - publicly available information supporting identification of potential vulnerabilities,
  - current information regarding potential vulnerabilities (e.g. from a CB)
- Evaluator Actions:
  - to examine TOE's suitability for testing,
  - to identify (public sources like www) and to record potential vulnerabilities regarding TSP,
  - to devise, to produce, to conduct penetration testing being focused on SFRs/TSF,
  - to record and to examine the test results in order to decide whether the TOE is resistant to an attacker possessing a Basic AP,
  - to report the testing approach, test results, exploitable and residual vulnerabilities, if any, as well.
- There are no developer's duties here.

CEM, AVA_VAN.1: Survey 2/2

- §1414: The evaluator is **not expected to test** for attack scenarios (including those in the public domain) beyond those, which possess a **Basic** attack potential. In some cases, however, it will be necessary to carry out a test before the attack potential related can be determined. Where, as a result of evaluation expertise, the evaluator discovers a potential vulnerability that is beyond Basic attack potential (i.e. can be exploited by an attack scenario with an attack potential beyond Basic), this is reported in the ETR as a residual vulnerability.
- Guidance on determining the necessary attack potential to exploit a potential vulnerability can be found in Annex B.4.
- §1424: Information usually reported in the ETR is:
  … b) **TSFI** penetration tested. A brief listing of the TSFI and other TOE interfaces that were the focus of the penetration testing;
  - According to CC part 3, sec. 16.1, § 453 the focus of testing lies on **SFR**s. This correct view can also be found in AVA_VAN.1-11 and in ATE_IND.1.
  - It is important to understand and to test the behaviour of **TSF**, what can be done in form of SFRs-testing **using** TSFI, but not TSFIs themselves!

CEM, AVA_VAN.2: Unstructured Analysis

- Objective is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attacker possessing Basic AP.
- Input (additionally to AVA_VAN.1):
  - ADV_FSP,
  - ADV_TDS,
  - ADV_ARC
- Evaluator Actions (additionally to AVA_VAN.1):
  - to identify (public printed sources like books & research papers + TOE specific sources: ST, AGD, FSP, TDS, ARC) and to record potential vulnerabilities regarding TSP,
  - to devise (respecting ARC), to produce, to conduct penetration testing being focused on SFRs/TSF,
  - to record and to examine the test results in order to decide whether the TOE is resistant to an attacker possessing a Basic AP,
  - to report the testing approach, test results, exploitable and residual vulnerabilities, if any, as well.
- There is a developer's duty to provide a 'vulnerability analysis' in ARC how TSF (i) protects itself and (ii) prevents bypassing.

T · · Systems ·

CEM, AVA_VAN.3: Focused (Unstructured) Analysis 1/2

- Objective is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attacker possessing Enhanced-Basic AP.
- Input (additionally to AVA_VAN.2):
  - ADV_IMP
- Evaluator Actions (additionally to AVA_VAN.2):
  - to identify (public printed sources like books & research papers & conference proceedings + focused search in the TOE specific sources: ST, AGD, FSP, TDS, ARC and IMP) and to record potential vulnerabilities regarding TSP,
  - to devise (respecting ARC & ATE_DPT), to produce, to conduct penetration testing being focused on SFRs/TSF,
  - to record and to examine the test results in order to decide whether the TOE is resistant to an attacker possessing an Enhanced-Basic AP,
  - to report the testing approach, test results, exploitable and residual vulnerabilities, if any, as well.
- There is a developer's duty to provide a 'vulnerability analysis' in ARC how TSF (i) protects itself and (ii) prevents bypassing.

T · · Systems ·

CEM, AVA_VAN.3: Focused (Unstructured) Analysis 2/2

- AVA_VAN.3-4: A flaw hypothesis methodology should be used whereby specifications and development and guidance evidence are analysed and then potential vulnerabilities in the TOE are hypothesised or speculated.
- B.2.2.2.2: The focused approach to the identification of vulnerabilities is an analysis of the evidence with the aim of identifying any potential vulnerabilities evident through the contained information. It is an unstructured analysis, as the approach is not predetermined.

- §1521: The evaluator is **not expected to test** for attack scenarios (including those in the public domain) beyond those, which possess an **Enhanced-Basic** attack potential. In some cases, however, it will be necessary to carry out a test before the attack potential related can be determined. Where, as a result of evaluation expertise, the evaluator discovers a potential vulnerability that is beyond Enhanced-Basic attack potential (i.e. can be exploited by an attack scenario with an attack potential beyond Enhanced-Basic), this is reported in the ETR as a residual vulnerability.

T · · Systems ·

CEM, AVA_VAN.4: Methodical Analysis 1/2

- Objective is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attacker possessing Moderate AP.
- Input (additionally to AVA_VAN.3):
  - none
- Evaluator Actions (additionally to AVA_VAN.3):
  - to identify (public printed sources like books & research papers & conference proceedings + methodical analysis of the TOE specific sources: ST, AGD, FSP, TDS, ARC, IMP) and to record potential vulnerabilities regarding TSP,
  - to devise (respecting ARC & ATE_DPT), to produce, to conduct penetration testing being focused on SFRs/TSF,
  - to record and to examine the test results in order to decide whether the TOE is resistant to an attacker possessing a Moderate AP,
  - to report the testing approach, test results, exploitable and residual vulnerabilities, if any, as well.
- There is a developer's duty to provide a 'vulnerability analysis' in ARC how TSF protects itself and prevents bypassing.

CEM, AVA_VAN.4: Methodical Analysis 2/2

- AVA_VAN.4-4
  - §1558: This approach … is to take an ordered and planned approach. A system is to be applied in the examination. The evaluator is to describe the method to be used in terms of the manner in which this information is to be considered and the hypothesis that is to be created.
  - §1566: … examination of only a subset of the development and guidance evidence … is not permitted in this level of rigour. The approach description should provide a demonstration that the methodical approach used is complete, providing confidence that the approach used to search the deliverables has considered all of the information provided in those deliverables.
  - §1567: This approach should be agreed with the evaluation authority (CB), …
- B.2.2.2.3: The methodical analysis approach takes the form of a structured examination of the evidence. This method requires the evaluator to specify the structure and form the analysis will take (i.e. the manner in which the analysis is performed is predetermined, unlike the focused identification method). The method is specified in terms of the information that will be considered and how/why it will be considered.
- §1578: The evaluator is **not expected to test** for attack scenarios (including those in the public domain) beyond those, which possess an **Moderate** attack potential. In some cases, however, it will be necessary to carry out a test before the attack potential related can be determined. Where, as a result of evaluation expertise, the evaluator discovers a potential vulnerability that is beyond Moderate attack potential (i.e. can be exploited by an attack scenario with an attack potential beyond Moderate), this is reported in the ETR as a residual vulnerability.

T · · Systems ·

CEM, AVA_VAN.5: Advanced Methodical Analysis

- Objective is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attacker possessing High AP.
- Input (additionally to AVA_VAN.4):
  - none
- Evaluator Actions:
  - § 1595: There is no general guidance; the scheme should be consulted for guidance on this sub-activity.

- There is a respective guidance/methodology for vulnerability analysis (for AVA_VLA.4 → High AP) within the German National Scheme in form of AIS34 (Evaluation Methodology for CC Assurance Classes for EAL5+)
  - It could be used, where it is sensible, as long as AVA_VAN.5 has not been guided.

CEM, Annex B: Calculating Attack Potential – General Metric 1/5

- § 1940: The approach described below is to be applied whenever it is necessary to calculate attack potential, unless the evaluation authority (CB) provides mandatory guidance that an alternative approach is to be applied. The values given in Tables 3 and 4 below are not mathematically proven. Therefore, the values given in these example tables may need to be adjusted according to the technology type and specific environments.
- § 1949: The determination of the attack potential for an attack corresponds to the **identification** of the effort required to create the attack, **and** to demonstrate that it can be **successfully applied** to the TOE (including setting up or building any necessary test equipment),….
- § 1950: In many cases, the evaluators will estimate the parameters for exploitation, rather than carry out the full exploitation. The estimates and their rationale will be documented in the ETR.
- § 1966: Where a factor falls close to the boundary of a range the evaluator should consider use of an intermediate value to those in the table 3.

T · · Systems ·

CEM: Attack Potential – General Metric 2/5

Factor	v3.1 Value	v2.x Value (Ident. + Exploit.)
Elapsed Time		
<= 0,5h		0
<= one day	0	5
<= one week	1	
<= two weeks	2	
<= one month	4	8
<= two months	7	13
<= three months	10	(13)
<= four months	13	(13)
<= five months	15	(13)
<= six months	17	(13)
> six months	19	(13)
Expertise		
Layman	0	0
Proficient	3*(1)	4
Expert	6	9
Multiple experts	8	(9)

CEM: Attack Potential – General Metric 3/5

Factor	v3.1 Value	v2.x Value (Ident. + Exploit.)
Knowledge of TOE		
None		0
Public	0	4
Restricted	3	
Sensitive	7	9
Critical	11	(9)
Window of Opportunity / Number of Samples		
Unnecessary / unlimited access	0	0
Easy / < 10	1	6
Moderate / < 100	4	9
Difficult / >= 100	10	13
None / number needed is not available to attacker	**(2)	*
Equipment		
Standard	0	3
Specialised	4(3)	7
Bespoke	7	11
Multiple bespoke	9	(11)

T · · Systems ·

CEM: Attack Potential – General Metric 4/5

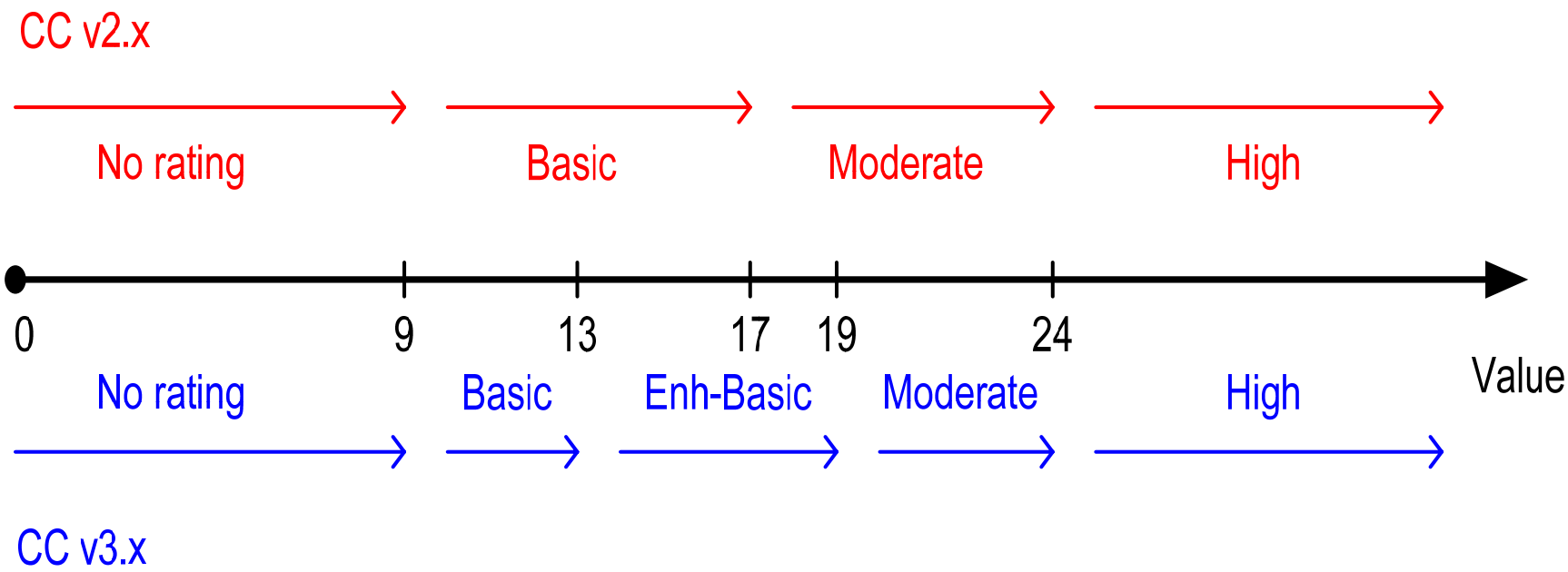
- § 1968 To determine the resistance of the TOE to the potential vulnerabilities identified the following steps should be applied:
  - Define the possible attack scenarios {AS1, AS2, ..., ASn} for the TOE in the operational environment.
  - For each attack scenario, perform a theoretical analysis and calculate the relevant attack potential using Table 3.
  - For each attack scenario, if necessary, perform penetration tests in order to confirm or to disprove the theoretical analysis.
  - Divide all attack scenarios {AS1, AS2, ..., ASn} into two groups:
    - the attack scenarios having been successful (i.e. those that have been used to successfully undermine the SFRs), and
    - the attack scenarios that have been demonstrated to be unsuccessful.
  - For each successful attack scenario, apply Table 4 and determine, whether there is a contradiction between the resistance of the TOE and the chosen AVA_VAN assurance component, see the last column of Table 4.
  - Should one contradiction be found, the vulnerability assessment will fail, e.g. the author of the ST chose the component AVA_VAN.5 and an attack scenario with an attack potential of 21 points (high) has broken the security of the TOE. In this case the TOE is resistant to attacker with attack potential '*Moderate*', this contradicts to AVA_VAN.5, hence, the vulnerability assessment fails.

CEM: Attack Potential – General Metric 5/5

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

T Systems

CEM, Annex B: Calculating Attack Potential – Comparison CC v3.1 vs. v2.x



‘Asymmetry’ of two approaches with successful and unsuccessful attack scenarios 1/3

- **Successful attack scenarios (evaluation approach)**
  - Let be *successful* (undermining TSP) attack scenarios {AS1, AS2, …, ASm} with respective attack potentials {AP1, AP2, …, APm}:
    {AS1, AS2, …, ASm} → {AP1, AP2, …, APm}.
  - Let APmin := min {AP1, AP2, …, APm}.
  - → If **an** ASi being relevant for TSP is *successful* and possesses APmin (APi = APmin, i = 1…m), then the TOE is resistant **at most** to the attack potential less than APmin: **TOE_Resistance < APmin** (upper restriction).
- **Advantage** of applying ‘successful AS methodology’ is that the final decision on the upper restriction of the TOE resistance TR < APmin is also possible for a situation where *successful* **and** *unsuccessful* (i.e. undermining and not undermining TSP) attack scenarios are known.

T · · Systems ·

‘Asymmetry’ of two approaches with successful and unsuccessful attack scenarios 2/3

- **Unsuccessful attack scenarios (design approach)**
  - Let be *unsuccessful* (not undermining TSP) attack scenarios {AS1’, AS2’, …, ASk’} with respective attack potentials {AP1’, AP2’, …, APk’}:
    {AS1’, AS2’, …, ASk’} → {AP1’, AP2’, …, APk’}.
  - Let AP’max := max {AP1’, AP2’, …, APk’}.
  - → If **all** AS’ being relevant for TSP are *unsuccessful* and one of them possesses AP’max, then the TOE is resistant **at least** to the attack potential being equal to AP’max: **TOE_Resistance ≥ AP’max** (lower restriction).
- **Disadvantage** of applying ‘unsuccessful AS methodology’ is that the final decision on the lower restriction of the TOE resistance TR ≥ AP’max is merely possible for a situation where **only** *unsuccessful* (i.e. not undermining TSP) attack scenarios are known: **Should there be one AS undermining the TSP, this assessment becomes not applicable**.

T Systems

‘Asymmetry’ of two approaches with successful and unsuccessful attack scenarios 3/3

- This asymmetry is grounding in the *restrictive* definition of what state is considered/defined as a secure one:

  Absence of any attack scenario undermining TSP is necessary and sufficient condition for the secure state.

Dr. Igor Furgel

T-Systems GEI GmbH
ICT Security

Rabinstrasse 8
53111 Bonn

☎ +49 (228) 9841-512
💻 igor.furgel@t-systems.com

T · · Systems ·