Software Support of the Common Criteria Vulnerability Assessment

Andrzej Bialas(✉)

Institute of Innovative Technologies EMAG,
Leopolda 31, 40-189 Katowice, Poland
andrzej.bialas@ibemag.pl

Abstract. The paper deals with the Common Criteria assurance methodology, particularly vulnerability assessment which is the key activity of the IT security evaluation process. Vulnerability assessment is specified by the Common Criteria Evaluation Methodology (CEM). The paper is focused on software support for vulnerability assessment. As the implementation platform, a ready-made risk management software developed by the author's organization is applied. The paper includes introduction to the vulnerability assessment, review of the existing methods and tools, specification of the CEM-based method to be implemented in the software, implementation and short exemplification. The conclusions summarize the validation and propose future works to extend and improve the tool.

Keywords: Common criteria · Vulnerability assessment · Attack potential · Risk management · IT security development · Security assurance

1 Introduction

Today's societies and economies are based on Information and Communication Technologies (ICT). Digitalization increases cyber security risk across many sectors. There is a necessity to minimize the risk inherent to the ICT use in the society and economy. One of the ways to do it is rigorous development of ICT products as accompanied by their independent evaluation and certification. This approach allows to achieve security assurance for the products, still, it is complex, time and cost consuming. Computer support for developers' or evaluators' works, focused on the most difficult or arduous activities, allows to make the development and evaluation processes much more efficient.

The paper concerns computer support for the Common Criteria compliant IT security development and assessment process. The Common Criteria (CC) [1] methodology presented in the ISO/IEC 15408 standard is a basic assurance methodology. According to this methodology, the assurance is measurable using EALs (Evaluation Assurance Levels) in the range EAL1 to EAL7. The CC methodology comprises three basic processes:

- IT security development process of the IT product or system called TOE (Target of Evaluation); after different security analyses have been performed, a document is

W. Zamojski et al. (eds.), *Advances in Dependability Engineering of Complex Systems*,
Advances in Intelligent Systems and Computing 582, DOI 10.1007/978-3-319-59415-6_3

prepared, called Security Target (ST); the Security Target embraces the security problem definition (SPD), its solution by specifying security objectives (SO), security requirements and functions; security functional requirements (SFRs), derived from the security objectives, describe how security measures should work in the operational environment; security assurance requirements (SARs), related to the EAL, determine how much assurance we can have in an IT product; the ST includes TOE security functions (TSF) meeting SFRs; the TSFs are implemented on the claimed EAL;

- TOE development process (according to the EAL) concerns the IT products (TOE) and their documentation; they are submitted together with the ST to the security evaluation process;
- security evaluation process carried out in an independent, accredited laboratory in a country which is a signatory of the Common Criteria Recognition Arrangement (CCRA) [2].

The Common Criteria methodology is described in publications worldwide [3, 4] and the author's publications [5–8].

A very important issue of the Common Criteria methodology is vulnerability assessment whose rigour depends on the claimed EAL. Vulnerabilities can be exploited by threat agents in the product operational environment. This exploitation results in security breaches. The development process should be focused on the vulnerabilities minimization. The developer, specifying the threat environment (SPD), should consider the attack potential, i.e. a measure of the effort to be expended in attacking a TOE, expressed in terms of the attacker's expertise, resources and motivation [1]/part1.

In addition, vulnerability assessment is one of the key elements of evaluation. The vulnerability assessment is performed according to AVA_VAN (Vulnerability analysis assurance components family). The AVA_VAN assurance requirements (components) are specified in the third part of the Common Criteria standard [1] and the CEM (Common Evaluation Methodology) document [9]. Annex B of this document [9] includes a general guideline for evaluators. They are able to see how to calculate the attack potential possessed by the assumed attackers (threat agents) of the TOE. The methodology presented in the paper complies with these guidelines. Please note that the vulnerability assessment is a specific risk assessment focused on attack potential, expressing possibility of the asset breach. This possibility is related to the term "likelihood" used in the risk assessment. The second factor – "consequences" is considered but not explicitly assessed.

The objective of the paper is to present a software implementation of the Common Criteria vulnerability assessment methodology. The Enhanced Risk Manager (ERM) developed by the author's organization is used as the software implementation platform.

Section 2 discusses the vulnerability assessment issue. Section 3 features the review of publications in the paper domain. The review shows that there are no works related to the automation of the vulnerability assessment. Section 4 presents the methodology, and Sect. 5 its implementation. The paper is completed by conclusions – Sect. 6.

2 Vulnerability Assessment According to Common Criteria

Vulnerability assessment (VA) is focused on the flaws or weaknesses in the TOE working in its operational environment. First, they should be identified and then assessed whether they can be exploited by threats agents of the defined capability, i.e. the attack potential sufficient to violate the SFRs.

The assessment embraces vulnerabilities possible to exploit by a huge number of attacks, which can be ordered by five main categories: bypassing, tampering, direct attack, monitoring and misuse [9]. Each category has its subcategories.

Bypassing embraces means which can be used by an attacker to avoid security enforcement done by TSFs. Bypassing may concern:

- inheriting privileges or other capabilities that would not be granted otherwise;
- exploiting the capabilities of TOE interfaces, or of utilities interacting with the TOE;
- getting access to sensitive data stored in or copied to inadequately protected areas, where confidentiality is a concern.

Tampering encompasses attacks focused on the behaviour of the TSF (i.e. corruption or deactivation), for example:

- forcing the TOE to deal with unusual or unexpected circumstances;
- disabling or delaying security enforcement;
- getting access to data whose confidentiality or integrity the TSF relies on;
- modifying the TOE in its physical aspect.

Direct attack covers the identification of penetration tests to check the strength of permutational or probabilistic mechanisms and other mechanisms to ensure they withstand a direct attack.

Monitoring attack is aimed at information related to the TOE operations, e.g.: information of internal TOE transfer or export from the TOE, information generated and passed to other user data or gained through monitoring the operations.

Misuse may be caused by:

- incomplete guidance documentation;
- unreasonable guidance;
- forced exception behaviour of the TOE;
- unintended misconfiguration of the TOE.

This classification has an open character and is refined to express specific technological issues related to the given IT product category.

The examples of vulnerabilities are:

- absence of the required security enforcement on interfaces or utilities,
- possibility to illicitly acquire privileges or capabilities of a privileged component,
- inadequately protected areas.

3 State of the Art in the Research Domain

The review embraces the following fields:

- methods and tools supporting the CC methodology processes, including evaluation,
- vulnerability assessment methods and tools.

Apart from the Common Criteria standard and the supplementing guidelines [2], the support given to the Common Criteria methodology developers and evaluators is rather poor and embraces only the following:

- general guidelines, like: ISO/IEC 15446 [10] for security targets and protection profiles elaboration, the BSI guide [11] for other evidences up to EAL5, and books, like [3, 4], however, they are focused on the Common Criteria methodology presentation, not on vulnerability assessment;
- a few software tools, like: Common Criteria (CC) ToolboxTM [12], GEST [13], Trusted Labs Security Editing Tool (TL SET) [14]; please note that these tools are focused on the ST preparation and do not support the elaboration of other evidences concerning the TOE design, life cycle, guidance, testing, vulnerability assessment, etc.; they do not deal with vulnerability assessment either;
- the CCMODE Tools [15] embraces full implementation of CEM, but omits vulnerability assessment details discussed in this paper;
- the extensive Information Assurance Technology Analysis Center (IATAC) [16] report encompasses detailed methods and tools focused on different kinds of vulnerability analyses designed for specific IT products or systems, like network scanners, host scanners, web application scanners, multilevel scanners, penetration test tools, vulnerability scan consolidators, etc.; they can be used on the lower layer of the software tool presented in this paper.

There are no specialized software tools supporting vulnerability assessment.

4 Methodology

During the vulnerability assessment a huge number of attack scenarios are assessed with respect to potential vulnerabilities. Some vulnerabilities are encountered during evaluation activities “by the way”, some of them are results of unstructured, focused or even methodical analyses. The rigour applied depends on the claimed EAL.

For all exploitable vulnerabilities the evaluator calculates the attack potential to determine whether the exploitation conditions are adequate to the level of the attack potential assumed for the attacker. The attack potential rises proportionally to the increasing motivation, resources and expertise of the attacker.

The attack potential (AP) sufficient to breach the TOE can be expressed as the sum of factors:

$$AP = ET + SE + KT + WO + EQ, \text{ where:} \tag{1}$$

ET – Elapsed Time, i.e. time taken to identify and exploit the vulnerability (Table 1);

SE – Specialist Expertise, i.e. the level of generic knowledge of the attacker (Table 2);

Table 1. Measures of the Elapsed Time (ET)

Elapsed time	ET	Elapsed time	ET
<=1 day	0	<=3 months	10
<=1 week	1	<=4 months	13
<=2 weeks	2	<=5 months	15
<=1 month	4	<=6 months	17
<=2 months	7	>6 months	19

Table 2. Measures of the Specialist Expertise (SE)

Specialist expertise	SE	Comments
Laymen	0	Has no particular expertise
Proficient	3	Is familiar with the security behaviour of the product or system type
Expert	6	Is familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and employed concepts of security, techniques and tools for defining new attacks, cryptography, classical attacks for the product type, attack methods, etc. – implemented in the product or system type
Multiple expert	8	On the expert level different fields of expertise are required for distinct steps of the attack

Table 3. Measures of the Knowledge of the TOE (KT)

Knowledge of the TOE	KT	Example
Public	0	Information gained from the Internet
Restricted	3	Knowledge controlled within the developer's organisation and shared with other organizations under a non-disclosure agreement
Sensitive	7	Knowledge that is shared between discreet teams within the developer's organisation. Only members of specified teams have access to it
Critical	11	Knowledge familiar only to a few individuals. The access to this knowledge is very strictly controlled on a strict-need-to-know basis and individual undertaking

KT – Knowledge of the TOE, i.e. dealing with the TOE design, operation (Table 3);
WO – Window of opportunity, i.e. considerable amounts of access to the TOE or the number of samples of the TOE that the attacker can obtain; related to ET (Table 4);
EQ – Equipment, i.e. IT hardware/software or other equipment required to identify or exploit the vulnerability (Table 5).

Table 4. Measures of the window of opportunity (WO)

Window of opportunity	WO	Example
Unnecessary/unlimited access	0	The attack does not need any kind of opportunity to be performed because there is no risk it will be detected during access to the TOE and one can access the number of TOE samples for the attack
Easy	1	Access is required for less than a day. Fewer than 10 TOE samples are required to perform the attack
Moderate	4	Access is required for less than a month. Fewer than one hundred TOE samples are required to perform the attack
Difficult	10	Access is required for at least a month. At least one hundred TOE samples are required to perform the attack
None	**	The attack path is not exploitable due to other measures in the intended operational environment of the TOE; the period during which the asset to be exploited is available or is sensitive is shorter than the opportunity period needed to perform the attack

Table 5. Measures of the equipment (EQ)

Equipment	EQ	Example
Standard	0	Is readily available to the attacker, either to identify a vulnerability or to attack. This equipment may be a part of the TOE as such (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser or simple attack scripts)
Specialised	4	Is not readily available to the attacker, but could be acquired without too much effort. This could include the purchase of some equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet), or development of more extensive attack scripts or programs. If distinct steps of an attack require clearly different test benches consisting of specialised equipment, this would be rated as bespoke
Bespoke	7	Is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the equipment is so specialised that its distribution is controlled, or even restricted. The equipment may be also very expensive
Multiple bespoke	9	Different types of bespoke equipment are required for distinct steps of an attack

Table 6. Attack potential and the TOE resistance

AP range	Attack potential required to exploit scenario	TOE resistant to attackers with attack potential of
0–9	Basic	No rating
10–13	Enhanced-Basic	Basic
14–19	Moderate	Enhanced-Basic
20–24	High	Moderate
=>25	Beyond high	High

All factors are measured using the predefined enumerative scales (Tables 1, 2, 3, 4 and 5).

The symbol specified in Table 4 "**" has special meaning and should not be seen as natural progression from the timescales specified in the preceding ranges associated with this factor.

The AP is assessed in the range 0 to 57 with special WO = None option. Table 6, based on CEM [9] (Annex B/Table 4), shows how these values are assigned to the enumeration values (second and third columns). For example, it means that if the minimal AP to exploit scenarios is 15, i.e. "Moderate", than the TOE is resistant to attackers with the attack potential of "Enhanced-Basic".

The above method, compatible with those specified in this annex, is sufficient to calculate the attack potential. This method does not go beyond the vulnerability assessment, e.g. towards risk assessment/management, though it is related to this issue.

5 Implementation and Validation

The ERM configurable software platform has been incrementally developed. Currently it contains the following risk assessment methods [17, 18] implemented:

- Consequences-probability matrix (called here TVC, because it is based on triples: threat-vulnerability-controls),
- Business impact analysis (BIA),
- Fault Tree Analysis (FTA),
- Event Tree Analysis (ETA).

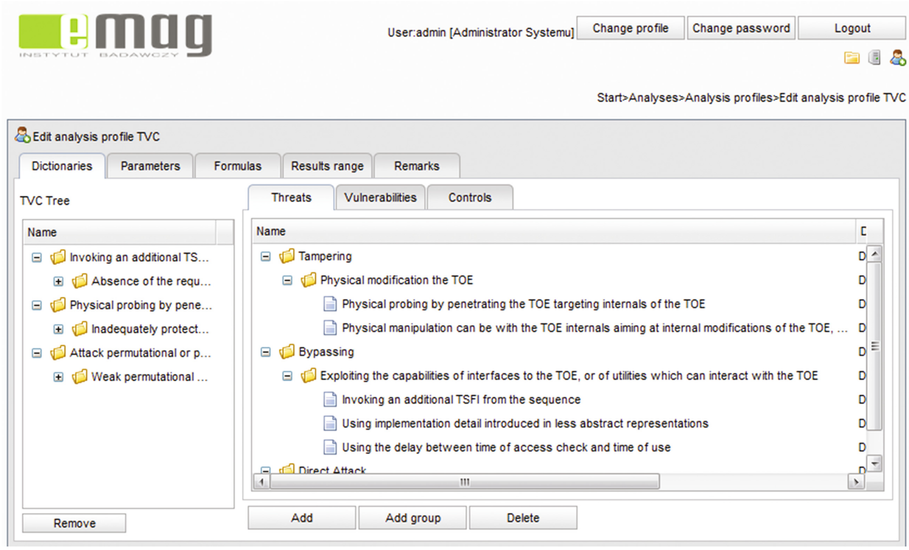
For each kind of analysis one or more analysis profiles can be defined, embracing dictionaries, formulas and configuration parameters. Using the given profile, one or more analyses can be provided, and based on the risk assessment results, new or improved security measures can be proposed (in this sense it is a risk management tool). This tool has an open character and it should be validated in different application domains. The paper [19] shows the tool and one of the first ERM applications.

Apart from the first aim, i.e. providing the ERM-based vulnerability assessment tool (ERM-VA) for Common Criteria evaluators, the second aim is to validate the ERM software itself to sample data for its future development. ERM-VA is based on the TVC method. The implementation embraces the profile elaboration and performing analyses. The goals of the implementation are the following:

- to manage the systematic and complex vulnerability assessment process,
- to calculate attack potentials for considered attack scenarios and to assess the TOE resistance to the attacks of the given potential.

5.1 TVC-VA Analysis Profile

The TVC-VA profile should consider the predefined threats and vulnerabilities discussed in CEM [9] (Annex B/Table 4). Analyzing this document, the lists of predefined threats and vulnerabilities are elaborated and introduced to the TVC-VA profile. The main categories and subcategories of threats and the list of vulnerabilities are presented in Sect. 2. No controls, i.e. security measures are needed for the vulnerability analysis. The dictionaries are open. They can be refined or supplemented for the assessed IT product to express its specific character. The right part of Fig. 1 shows a part of the global threat dictionary made according to CEM/Annex B including two main categories: bypassing and tampering with subcategories and particular threats. The left part shows three selected pairs threat-vulnerability for further analysis Fig. 2.

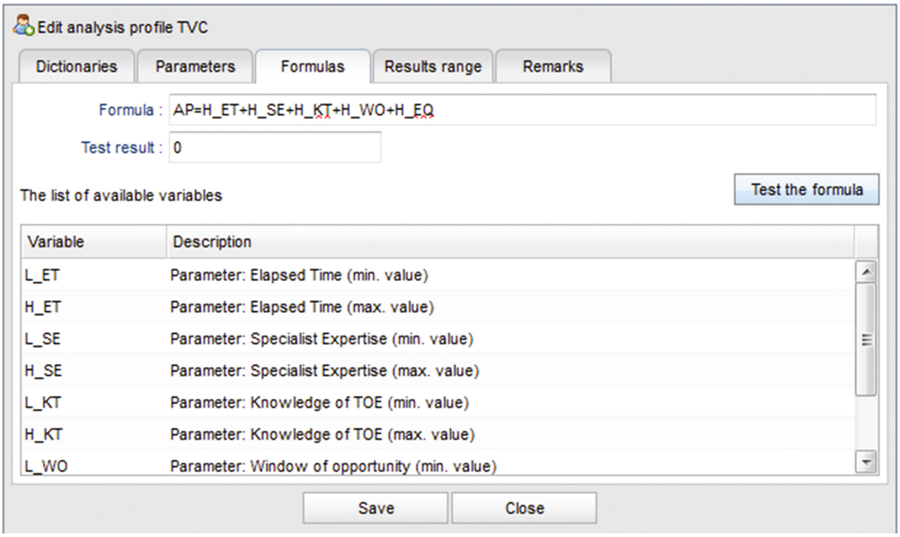


- Invoking an additional TS...
  - Absence of the requ...
- Physical probing by pene...
  - Inadequately protect...
- Attack permutational or p...
  - Weak permutational ...

- Tampering
  - Physical modification the TOE
    - Physical probing by penetrating the TOE targeting internals of the TOE
    - Physical manipulation can be with the TOE internals aiming at internal modifications of the TOE, ...
- Bypassing
  - Exploiting the capabilities of interfaces to the TOE, or of utilities which can interact with the TOE
    - Invoking an additional TSFI from the sequence
    - Using implementation detail introduced in less abstract representations
    - Using the delay between time of access check and time of use
- Direct Attack

Fig. 1. Threat dictionary – an example in the EMAG-ERM tool

Each pair represents an attack scenario (AS). For the given AS the attack potential should be calculated. Thus the basic formula (Eq. 1) used in Common Criteria is implemented in the tool. The ERM formulas and their variables are defined by the user. Each variable has minimal (L_VAR) and maximal (H_VAR) values to express uncertainties. For the discussed profile, uncertainties are not considered, both values are



Formula : AP=H_ET+H_SE+H_KT+H_WO+H_EQ

Test result : 0

The list of available variables

Variable	Description
L_ET	Parameter: Elapsed Time (min. value)
H_ET	Parameter: Elapsed Time (max. value)
L_SE	Parameter: Specialist Expertise (min. value)
H_SE	Parameter: Specialist Expertise (max. value)
L_KT	Parameter: Knowledge of TOE (min. value)
H_KT	Parameter: Knowledge of TOE (max. value)
L_WO	Parameter: Window of opportunity (min. value)

Fig. 2. Attack potential formula implemented in the TVC-VA profile in the EMAG-ERM tool

the same and only variables with prefixes "H_" are used. Each variable representing an AP factor has predefined measures according to Table 1 through Table 5.

Figure 3 shows an example of the factor measure configuration. It is an implementation of Table 5 concerning the threat agent equipment.

This way the TVC-VA profile is ready to use.

5.2 TVC-VA Analysis

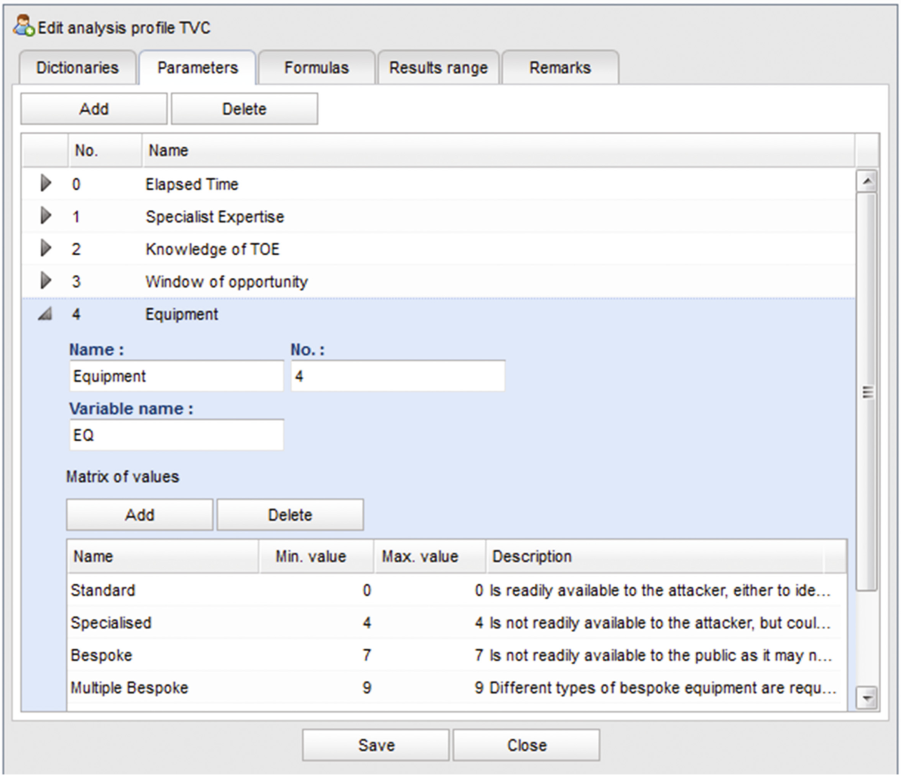
The vulnerability assessment is shown by an example embracing three attack scenarios (Fig. 4). The left part of the window presents these scenarios, the right part the assessment of particular factors with respect to the first AS:

- threat: "Invoking an additional TSFI from the sequence",
- vulnerability: "Absence of the required security enforcement on interfaces or utilities".

Each factor has basic and extended explanations helping the evaluator.

Figure 5 presents the results of the assessment. Different attack potentials are obtained, belonging to different enumerative values (please compare these results with Table 6).

Based on this table the following conclusion is possible. One of the attack scenarios has AP = 18. It means that the considered TOE can be exploited by an intruder of this attack potential, so the TOE is resistant to the attackers with attack potential of "Enhanced-Basic". Particular attack potentials are marked by different colours.



No.	Name
0	Elapsed Time
1	Specialist Expertise
2	Knowledge of TOE
3	Window of opportunity
4	Equipment

Name : Equipment

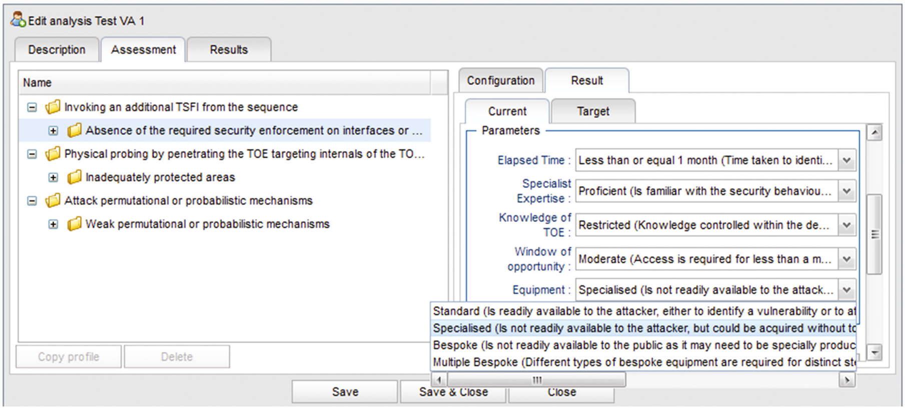
No. : 4

Variable name : EQ

Matrix of values

Name	Min. value	Max. value	Description
Standard	0	0	Is readily available to the attacker, either to ide…
Specialised	4	4	Is not readily available to the attacker, but coul…
Bespoke	7	7	Is not readily available to the public as it may n…
Multiple Bespoke	9	9	Different types of bespoke equipment are requ…

Fig. 3. Equipment (EQ) factor related to data in the TVC-VA profile in the EMAG-ERM tool



Name

- ⊟ Invoking an additional TSFI from the sequence
  - ⊞ Absence of the required security enforcement on interfaces or …
- ⊟ Physical probing by penetrating the TOE targeting internals of the TO…
  - ⊞ Inadequately protected areas
- ⊟ Attack permutational or probabilistic mechanisms
  - ⊞ Weak permutational or probabilistic mechanisms

Parameters

Elapsed Time : Less than or equal 1 month (Time taken to identi…

Specialist Expertise : Proficient (Is familiar with the security behaviou…

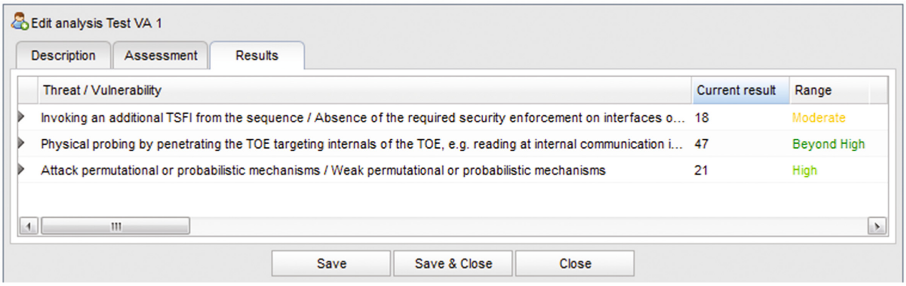
Knowledge of TOE : Restricted (Knowledge controlled within the de…

Window of opportunity : Moderate (Access is required for less than a m…

Equipment : Specialised (Is not readily available to the attack…

Standard (Is readily available to the attacker, either to identify a vulnerability or to at
Specialised (Is not readily available to the attacker, but could be acquired without to
Bespoke (Is not readily available to the public as it may need to be specially produc
Multiple Bespoke (Different types of bespoke equipment are required for distinct st

Fig. 4. Vulnerability assessment based on the TVC-VA profile in the EMAG-ERM tool



	Threat / Vulnerability	Current result	Range
▸	Invoking an additional TSFI from the sequence / Absence of the required security enforcement on interfaces o...	18	Moderate
▸	Physical probing by penetrating the TOE targeting internals of the TOE, e.g. reading at internal communication i...	47	Beyond High
▸	Attack permutational or probabilistic mechanisms / Weak permutational or probabilistic mechanisms	21	High

Fig. 5. Vulnerability assessment results in the EMAG-ERM tool

6 Conclusions

The paper is focused on two main goals:

- automation of arduous and difficult vulnerability assessment,
- sampling experience for further development of the Enhanced Risk Manager software.

Analyzing CEM, especially in the range of vulnerability assessment, a concise specification of the vulnerability assessment method is prepared, being an input for software implementation of the method on the open, fully configurable ERM risk manager. The implementation embraces the analysis profile definition according to the vulnerability assessment methodology, i.e. preparing dictionaries of threats and vulnerabilities, defining some attack scenarios for analysis, defining the formula and measures of the formula factors. For the given profile many analyses can be performed, including the one presented in the paper.

For each identified attack scenario, i.e. the pair threat-vulnerability, the attack potential is calculated and classified according to CEM as: "Basic", "Enhanced-Basic", "Moderate", "High", "Beyond High". It allows to determine the TOE resistance to attackers with the given attack potential.

The quantitative values of the attack potential are automatically translated to commonly used enumeration values and marked by colours. The validation shows that the complete vulnerability assessment can be performed using the ERM tool.

One issue was not properly implemented in the ready-made software. It concerns the "exception" in the Window of opportunity factor, i.e. WO = NONE. The possibility of the implementation exists, but needs extra, uncomplicated programming (introducing a special flag to mark this exception).

The threat and vulnerability dictionaries fully implement items extracted from CEM [9] (Annex B), but it should be noted that they have a generic character. They should be extended by IT products/technologies specific items or specified within the supporting guides and standards, like [20].

The discussed software support embraces the main management activities of vulnerability assessment. Please note that each attack scenario represents an experiment, sometimes very complex, long lasting and based on specialized equipment. The tool is able to manage results of these experiments, but particular experiments should be performed using the specific methods and tools (similar to these, owned by potential attackers). This range of automation seems to be enough. A good idea would be to integrate the Common Criteria evaluation tool existing in the CCMODE Tools [15] with the presented vulnerability assessment tool discussed in the paper.

References

1. Common Criteria for IT Security Evaluation, part 1–3, version 3.1 rev. 4 (2012). http://www.commoncriteriaportal.org/. Accessed 10 Mar 2017
2. Common Criteria Portal Home page. http://www.commoncriteriaportal.org/. Accessed 10 Mar 2017
3. Hermann, D.S.: Using the Common Criteria for IT Security Evaluation. CRC Press, Boca Raton (2003)
4. Higaki, W.H.: Successful Common Criteria Evaluation. A Practical Guide for Vendors. Copyright 2010 by Wesley Hisao Higaki, Lexington (2011)
5. Bialas, A.: Intelligent sensors security. Sensors **10**, 822–859 (2010)
6. Bialas, A.: Common criteria related security design patterns—validation on the intelligent sensor example designed for mine environment. Sensors **10**, 4456–4496 (2010)
7. Bialas, A.: Common criteria related security design patterns for intelligent sensors—knowledge engineering-based implementation. Sensors **11**, 8085–8114 (2011)
8. Bialas, A.: Computer-aided sensor development focused on security issues. Sensors **16**, 759. http://www.mdpi.com/1424-8220/16/6/759. Accessed 10 Mar 2017
9. Common Methodology for Information Technology Security Evaluation, version 3.1 rev. 4 (2012). http://www.commoncriteriaportal.org/. Accessed 10 Mar 2017
10. ISO/IEC TR 15446: Information technology—Security techniques—Guide for the production of Protection Profiles and Security Targets (2009)
11. Bundesamt für Sicherheit in der Informationstechnik. Guidelines for Developer Documentation according to Common Criteria, Version 3.1 (2007)
12. CC Toolbox. http://niatec.info/ViewPage.aspx?id=44. Accessed 10 Mar 2017
13. Horie, D., Yajima, K., Azimah, N., Goto, Y., Cheng, J.: GEST: a generator of ISO/IEC 15408 security target templates. In: Lee, R., Hu, G., Miao, H. (eds.) Computer and Information Science 2009. SCI, vol. 208, pp. 149–158. Springer, Heidelberg (2009). http://link.springer.com/chapter/10.1007%2F978-3-642-01209-9_14#page-1. Accessed 10 Mar 2017
14. TL SET. http://trusted-labs.com/security-consulting/tools-training/tl-set/. Accessed 10 Mar 2017
15. CCMODE: Common Criteria compliant, Modular, Open IT security Development Environment'. http://www.commoncriteria.pl/. Accessed 10 Mar 2017
16. Goertzel, K.M., Winograd, T.: (Contributor): Information Assurance Tools Report – Vulnerability Assessment. 6th edn. Information Assurance Technology Analysis Center (IATAC), USA (2011)
17. ISO 31000:2009, Risk management – Principles and guidelines
18. ISO/IEC 31010:2009 – Risk Management—Risk Assessment Techniques

19. Bagiński, J., Rogowski, D.: Software support for enhanced risk management. In: Rostański, M., Pikiewicz, P., Buchwald, P., Maczka, K. (eds.): Proceedings of the XI International Scientific Conference Internet in the Information Society, Publishing University of Dąbrowa Górnicza, Cieszyn, Poland, 22–23 September 2016, pp. 369–388 (2016)
20. ISO/IEC TS 30104 Information technology—Security Techniques—Physical Security Attacks, Mitigation Techniques and Security Requirements (2015)