ACTA IMEKO
ISSN: 2221-870X
June 2019, Volume 8, Number 2, 12 - 20

Applying heuristics to the selection and prioritisation of security assessment items in software assessment: the case of ISO/IEC 27001

Ferrucio de Franco Rosa[1,2], Mario Jino[2], Paulo Marcos Siqueira Bueno[1,2], Rodrigo Bonacin[1,3]

[1] *CTI Renato Archer, Campinas SP, Brazil*
[2] *FEEC-UNICAMP, Campinas SP, Brazil*
[3] *UNIFACCAMP, Campo Limpo SP, Brazil*

ABSTRACT
Security standards are essential instruments for security assessment. To create security assessment designs with suitable assessment items, we need to know the security aspects that are covered by a particular standard. We propose an approach to the selection and prioritisation of security assessment items. Assessment heuristics are proposed, aiming to increase the coverage of assessment dimensions and security characteristics in assessment designs. The main contribution of this paper to the field is the set of security assessment heuristics. Our approach can be applied to security standards in order to select or to prioritise assessment items with respect to 11 security properties and 6 assessment dimensions. The approach is flexible and allows the inclusion of security dimensions and properties. Our proposal is applied herein to a well-known security standard, ISO/IEC 27001, and its assessment items were analysed. The proposal is intended to support (i) the generation of high-coverage assessment designs, by including security assessment items with assured coverage of the main security characteristics and (ii) the evaluation of security standards with respect to the coverage of security aspects.

Section: RESEARCH PAPER

Keywords: assessment; security; standard; software; assessment dimension; security property; heuristics; coverage; ontology

Citation: Ferrucio de Franco Rosa, Mario Jino, Paulo Marcos Siqueira Bueno, Rodrigo Bonacin, Applying heuristics to the selection and prioritisation of security assessment items in software assessment: the case of ISO/IEC 27001, Acta IMEKO, vol. 8, no. 2, article 3, June 2019, identifier: IMEKO-ACTA-08 (2019)-02-03

Section Editor: Emiliano Sisinni, University of Brescia, Italy

Received July 13, 2018; **In final form** June 11, 2019; **Published** June 2019

Funding: This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001

Corresponding author: Ferrucio de Franco Rosa, e-mail: ferrucio.rosa@cti.gov.br

1. INTRODUCTION

Nowadays, cars are also computers on wheels. Smartphones have become bank agencies, replacing even wallets and credit cards. Interconnected devices have massively increased in prevalence. The new industrial revolution is characterised by strong automation based on artificial intelligence. In this environment of complexity and ubiquity, we are faced with serious attacks on important infrastructures that make use of smart devices [1]-[3]. Fraud related to information security is commonplace. Nevertheless, security receives increased attention only after software has been developed or even deployed [4], [5].

In this context, information security is a critical issue. Security standards are essential instruments in the security assessment process [6], [7]. Key questions to overcome security issues remain open, such as: which test cases are the most effective for security assessment? How can the effectiveness of a security assessment be verified? How can security assessments be made to be less dependent on human skills and intuition?

Systematic approaches based on quantitative analysis to support security assessment activities are needed to deal with current IT complexity. Coverage measures are important instruments in quantifying key security aspects in software testing.

We propose the identification of security properties (e.g. confidentiality and availability) and assessment dimensions (e.g. business logic and system in runtime) covered by assessment items (e.g. test cases) from sources such as security standards, by using a security assessment ontology [8], [9].

A set of heuristics can be applied to the analysis, selection, and prioritisation of items from security assessment designs

(ADs). This systematic and measurable approach has the purpose of developing security ADs, which aim to be comprehensive and low time-consuming. In this sense, this article proposes a set of security assessment heuristics to support the generation of high-coverage ADs and the evaluation of the coverage of security standards.

Our proposal is intended to be applied in the context of measurable security assessments (encompasses test and verification) in measurable applications. We have applied it here to the well-known security standard (SS) ISO/IEC 27001 [10].

2. LITERATURE REVIEW AND RELATED WORK

A literature review has been carried out. Articles were selected from the main research databases following known systematic review methods [11], [12]. Related works with characteristics or objectives similar to the proposed approach were selected. A more extensive view of the related works and conceptual foundations can be found in [5], [9].

An integrative security knowledge model and a heuristic approach to security requirements is presented in [13]. A method based on natural language analysis is proposed to refine and adapt security knowledge. The approach aims to identify vulnerabilities in natural language requirements based on reported security incidents. The approach has two parts: (1) security assessment and (2) extraction of security knowledge. This work focuses on the identification of known vulnerabilities and their variations in natural language requirements. Although the focus is technical aspects of security, the approach is also capable of incorporating aspects related to humans. Important studies and their main security concepts are presented. However, the success of the approach depends on the quality of the security knowledge.

A quantitative method of assessing and prioritising security is presented in [14], aiming to evaluate a specific security aspect (authenticity) for access control in web applications. The analytic hierarchy process is used as a mathematical tool to transform intangible measures into tangible measures. The main objective is to assess the security aspect authenticity for access control in web applications i.e. to evaluate the authentication process of a system in test runtime. The method does not consider other assessment dimensions or security issues, such as the operating environment, network, business rules, source-code analysis, availability, and integrity. Security requirements for access control are presented by means of a checklist, and they can be used to support the security assessments of banking systems.

A methodology for the automatic generation of IT security metrics based on ISO 27001 is presented in [15], aiming to enable organisations to assess compliance with information SSs and the effectiveness of control implementations. It is based on the security ontology presented in [16].

A method of mapping the information security knowledge of the French standard EBIOS [17] and the German manual Grundschutz [18] for a security ontology is presented in [19]. Knowledge provided by these standards is transformed into web ontology language (OWL) code. The proposed method allows for the reusing of information security knowledge bases (KBs) and for the mapping thereof to standardised data structures. According to the authors, although there are information security ontologies, no method has been proposed to map best practice guidelines or information SSs to an ontology. The proposed approach is based on the NIST handbook [20]. To simplify the mapping process, top-level threats (e.g. data disclosure, data tampering, and data loss) that affect security attributes (e.g. confidentiality, integrity, and availability) have been defined.

The open source security testing methodology (OSSTMM) is proposed in [21] and aims to characterise operational security by examining and correlating test results consistently. An OSSTMM audit is an operational level security measure. A secondary objective is to provide guidelines to ensure that (i) the test has been conducted completely; (ii) the test includes all the necessary channels; (iii) the test complies with the law; (iv) the results are measurable; (v) the results are consistent and repeatable; and (vi) the results contain only facts derived from the tests. The risk assessment value (RAV) is a scale measure of an attack surface. It is calculated by the quantitative equilibrium between limitations and controls. On this scale, 100 RAV is a perfect balance; less than 100 represents a lack of control (or countermeasures) and therefore a large attack surface. More than 100 RAV shows more controls than are needed, which can be a problem because controls often add interactions within a scope. There are also complexity and maintenance issues.

Our proposal, which is described in the next section, provides a feasible and systematic approach based on measurable coverage of security properties.

3. HCAPP-SEC – HEURISTICS AND A CRITERIA-BASED APPROACH TO THE SELECTION AND ANALYSIS OF SECURITY ASSESSMENT ITEMS

When there is a large quantity of tests to do, assessment may become inaccurate, laborious, and expensive. Clear criteria are required for the selection and prioritisation of assessment items according to the relevant security requirements. HCApp-Sec is an approach to the selection and prioritisation of security assessment items, devised to support the development of security ADs in a systematic, comprehensive, quantifiable way. It is rooted in assessment heuristics. Measured diversity (from coverage measures) is ensured by considering security properties and possible perspectives (dimensions) in a security assessment.

3.1. Security assessment ontology

The approach makes use of conceptual formalisation by means of the security assessment ontology (SecAOnto) [8], [9]. The main objective thereof is to represent and formally structure the knowledge on security assessments. Further information about SecAOnto can be found in [9], [22].

The essential concepts used in the context of this paper are described. We consider knowledge sources (KS) as either SSs or other documents that can be used in security assessments. A KS is composed of a set of assessment items (AIs) that can be treated as unities of knowledge.

The 11 security properties (PPs) initially considered are: availability; integrity; confidentiality; authenticity; non-repudiation; traceability; privacy; auditability; legality; resilience; non-retroactivity.

The six assessment dimensions (DMs) considered are: business logic; system architecture; process; system in runtime; source-code structure; and operating environment. An AI is said to cover a PP or a DM if it explicitly evaluates that PP or DM. SecAOnto is applied to determine which PPs and DMs a given AI covers.

3.2. Coverage measures

The assessment results indicate that in most situations high-diversity sets achieve more efficiency and a larger coverage than those obtained by randomly generated sets of the same size [23].

We propose an approach for quantifying the coverage of security properties and assessment dimensions of each AI of security KSs. It is used as the basic input to define the security assessment heuristics. By measuring the coverage of each AI, our approach enables the application of systematic and quantifiable heuristics, aiming at the development of comprehensive and low time-consuming security ADs. For instance, an AI that covers *availability, integrity,* and *confidentiality* is more comprehensive than one that only covers *integrity*.

The process of defining heuristics begins with coverage calculus. Coverage calculus considers the diversity of the assessment scope (the DMs) and the diversity of security aspects (PPs), as well as their conceptual distances, proposed in adjacency matrices (i.e. distances between DMs and distances between PPs). These distances (the degree of diversity) were initially proposed by a security expert based on a previous literature review and their professional experience, and they were refined by four system analysts and security experts. Their values range from 0.0 to 1.0. The aim of the adjacency matrices is to model the conceptual distances between pairs of the security concepts: pairs of PPs and pairs of DMs. For example, the property *confidentiality* has a distance value from *authenticity* and *authenticity* has a distance value from the *integrity* property.

The rationale is that a greater diversity (and therefore the assessment comprehensiveness) is achieved when concepts are semantically dissimilar. For example, *confidentiality* and *availability* are distinct and distant concepts, whereas *privacy* and *confidentiality* are closer concepts, since *privacy* is *confidentiality* of personal information. The proposed assessment coverage measures, based on the distances between security properties and assessment dimensions, are:

(i) Coverage of DMs (CovDM) is a measure concerning the DMs addressed by the AI. In equation (1), the numerator is the sum of the conceptual distances (or diversity) of all pairs of DMs, and *c* is the total number of DMs covered by the AI. The alpha constant (α) represents the total number of DMs (equal to 6). Hence, CovDM is a value between 0 and 1. It is greater if more DMs are covered, weighted by the diversity of covered DMs.

(ii) Coverage of PPs (CovPP) is a measure concerning the PPs addressed by the AI. In equation (2), the numerator is the sum of the conceptual distances (or diversity) of all pairs of PPs, and *c* is the total number of PPs covered by the AI. The beta constant (β) represents the total number of PPs (equal to 11). Hence, CovPP is a value between 0 and 1. It is greater if more PPs are covered, weighted by the diversity of the covered PPs.

(iii) Local coverage of AIs (CovLOC) is a measure of the coverage of the AI, taking the average between CovDM and CovPP. In equation (3), the numerator is the sum of the previous coverage values for the AI. Therefore, CovLOC combines CovDM and CovPP.

(iv) Global coverage of KS (CovGLO) is a measure of the coverage of the KS, taking the average of CovLOC for all AIs of the KS. In equation (4), the numerator is the sum of the coverage of all AIs of a given KS; *n* is the total number of AIs in KS. Therefore, CovGLO is the average coverage of the AIs in the KS.

(v) Total coverage of ADs (CovTOT) is a measure of the coverage of the AD, taking the average of the CovLOC of all selected AIs (SAIs) of KSs. In equation (5), the numerator is the sum of the coverage of all AIs in a specific AD; *n* is the total number of AIs in the AD. Therefore, CovTOT is the average coverage of the AIs in the AD.

We propose three classes of coverage measures, each class with a different application. Measures (1), (2), and (3) refer to AIs and can be used for the prioritisation and selection of AIs that will be used. Measure (4) characterises a KS and can be used for choosing KSs according to the organisation security goals. Measure (5) characterises an AD and can be used for choosing ADs.

$$\mathrm{CovDM(DM)} = \frac{\sum_{i=1}^{c-1}\sum_{j=(i+1)}^{\mathrm{c}} \mathrm{D}(dm_i, dm_j)}{a} \qquad (1)$$

$$\mathrm{CovPP(PP)} = \frac{\sum_{i=1}^{c-1}\sum_{j=(i+1)}^{c} \mathrm{P}(pp_i, pp_j)}{\beta} \qquad (2)$$

$$\mathrm{CovLOC(AI)} = \frac{(\mathrm{CovDM} + \mathrm{CovPP})}{2} \qquad (3)$$

$$\mathrm{CovGLO(KS)} = \frac{\sum_{i=1}^{n} \mathrm{CovLOC}(AI)}{n} \qquad (4)$$

$$\mathrm{CovTOT(AD)} = \frac{\sum_{i=1}^{n} \mathrm{CovLOC}(SAI)}{n} \qquad (5)$$

3.3. Heuristics for selecting the AIs of SSs

Heuristics are methods of solving problems. Heuristic reasoning is good, but we cannot say it is suitable for rigorous proofs [24]. Heuristics, in general, do not guarantee that the resulting set is the best set or even the smallest set; rather, this set has a high probability of being efficient concerning the requirements. The prioritisation techniques of test cases (AIs) are typically heuristics [25]. The role of heuristics in the context of exploratory software assessment is discussed in [26]. According to the authors, every decision of an evaluator is made under conditions of uncertainty and insufficient knowledge. Therefore, all decisions have some probability of being incorrect, and this probability means that we cannot mechanically choose the next thing to do. Instead, since each decision brings an element of risk, we can use heuristics. Even the process of evaluating a heuristic for its applicability can be an extremely useful process to help an evaluator think about what they are trying to achieve from different viewpoints and help them find a good solution to the problem [26].

In this work, we detail and apply the heuristics proposed in [27]. Our heuristics have low computing costs for effective solutions, given that they consider the diversity of security aspects. In the context of this work, the term ‘assessment heuristics’ encompasses both test heuristics and verification heuristics.

Each heuristics process is an approximation to an objective. The proposed heuristics aim to select or prioritise (i) *n* better AIs by considering CovDM; (ii) *n* better AIs by considering CovPP; (iii) *n* better AIs, by considering CovLOC; (iv) *n* better KSs by considering CovGLO; (v) *n* better ADs (selected AIs) by considering CovTOT; (vi) *n* better AIs by considering coverage (CovDM, CovPP, or CovLOC) above average; (vii) *n* better AIs by considering higher coverage with a lower amount of AIs; and (viii) *n* better AIs by considering CovDM and CovPP concurrently.

With these objectives in mind, the following security assessment heuristics are proposed.

Coverage of AD heuristics (H-CovDM) aims to select AIs with more diversity in CovDM. This heuristics method determines AIs with a high range of DMs by addressing at least one pair of DMs among those with highest distance of a KS. H-CovDM relies on CovDM. This coverage is based on the diversity of the AI. If the AI addresses only one DM, the coverage value will be 0, but if it is more than one DM, its coverage value will depend on the distances between DMs. The larger the distance, the greater the diversity of DMs, and the higher the coverage value is. An example is 'Select the ten best AIs by considering CovDM'.

Coverage of PP heuristics (H-CovPP) aims to select the AIs with greater diversity in CovPP. This heuristics method determines the AIs with high range of PPs by addressing at least one pair of PPs among those with highest distance of a KS. H-CovPP relies on CovPP; this coverage is based on the diversity of the AI. If the AI addresses only one PP, the coverage value will be 0, but if it is more than one PP, its coverage value will depend on the distances between PPs. The larger the distance, the greater the diversity of PPs, and the higher the coverage value is. An example is 'Select the ten best AIs by considering CovPP'. In this case, there would be a cut line, and the ten AIs with the higher CovPP values would be selected. In this context, it is not guaranteed that the resulting set is the best set; rather, this is a set that is efficient and considers the diversity of PPs.

Local coverage heuristics (H-CovLOC) aims to select the AIs with the higher average of the sum of CovDM and CovPP (i.e. CovLOC). This heuristics method determines the AIs among those with the highest arithmetic mean of CovDM and CovPP. Consider three AIs (a, b and c) with the following values: (a) CovDM=0.450, CovPP=0.450, then CovLOC=0.450. (b) CovDM=0.900, CovPP=0.0, then CovLOC=0.450. (c) CovDM=0.450, CovPP=0.800, then CovLOC=0.625. In this case, AI (c) will be selected. An example is 'Select the first ten AIs by considering CovLOC'. In this case, there would be a cut line, and the ten AIs with the highest CovLOC values would be selected. In this context, it is not guaranteed that the resulting set is the best set; rather, it is a set that is efficient and considers the diversity of ADs and PPs.

Global coverage heuristics (H-CovGLO) aims to select the KSs with the highest average of the sum of the CovLOCs of all AIs. This heuristics method determines the KSs with the higher values of CovGLO. An example is 'Select the first two KSs by considering CovGLO'. In this context, it is not guaranteed that the resulting set is the best set; rather, it is a set that is efficient and considers the average of the CovLOCs of each KS (CovGLO) of the database.

Total coverage heuristics (H-CovTOT) aims to select the ADs with the higher values of CovTOT. As an AD is composed of SAIs of KSs, this heuristics method selects the ADs that have, in their set of AIs, the highest average of the sum of CovLOCs (CovTOTs). An example is 'Select the first two ADs by considering CovTOT". In this case, the two ADs with the highest CovTOT values will be selected. In this context, it is not guaranteed that the resulting set is the best set; rather, this is a set that is efficient and considers the average of the CovLOCs of each AD (CovTOT) of the database. This heuristics method can be interesting, for example, when we want to reuse designs that have proven efficient in a certain context. In addition, experienced and robust ADs may be candidates for becoming KSs.

Above average heuristics (H-AboveAvg) aims to select or prioritise AIs that are above average by considering CovDM, CovPP, or CovLOC of all the AIs from a specific KS. This heuristic is an approximation to the objective of identifying *n* AIs that have higher coverage values by considering the average of one of the coverages (CovDM, CovPP, or CovLOC) as the cut line. Some examples of using the heuristics method are 'Select all AIs with above-average CovDM values'; 'Select all AIs with above-average CovPP values'; 'Select the top five AIs with above-average CovDM, CovPP, and CovLOC values'. In these cases, AIs with higher coverage values are selected. In this context, it is not guaranteed that the resulting sets are the best possible sets; rather, they are efficient (based on the coverage, either CovDM, CovPP, or CovLOC) and consider the average as a cut line. This heuristics process can be useful, for example, when we need to create efficient designs in a certain context by considering the average.

Pareto percentage heuristics (H-ParetoPercentage) aims to select the AIs among those with the best CovLOC of a KS. This heuristics process selects a set of AIs among those with highest CovLOC and a lowest quantity of AIs by disregarding the average (CovGLO), and it considers the total sum of the CovLOCs of all AIs of a KS. Examples are 'Select the AIs that represent 40 % of the sum of the CovLOCs of a KS' and 'Select all AIs up to the optimum point of the sum of the CovLOCs of a KS'. In these cases, the AIs with the higher values of CovLOC would be selected. In this context, it is not guaranteed that the resulting set is the best set; rather, it is efficient and considers the sum of all the CovLOCs of a KS of the database.

Pareto frontier heuristics (H-ParetoFrontier) aims to select the AIs with the higher values by considering CovPP and CovDM. This heuristics process selects a set of AIs among those with the best values of CovDM and CovPP concurrently (bi-objective). Consider two AIs (a and b) with the following values: (a) CovDM=0.450, CovPP=0.450, then CovLOC=0.450. (b) CovDM=0.900, CovPP=0.0, then CovLOC=0.450. In this case, AI (a) will be selected or prioritised.

Some examples of scenarios are 'Select the AIs with CovDM and CovPP > 0', 'Select the AIs with CovDM and CovPP > 0.400', and 'Select the AIs with CovDM > 0.200 and CovPP > 0.350'. In these scenarios, the AIs with higher values of CovDM and CovPP at the same time would be selected.

In this context, it is not guaranteed that the resulting set is the best set; rather, it is an efficient set and considers the values of CovDM and CovPP pairs of a certain KS of the database.

In Table 1, we present a synthesis of the proposed security assessment heuristics.

Table 1. Synthesis of the proposed security assessment heuristics.

Heuristics	*Objective*
H-CovDM	*n* better AIs, by considering CovDM.
H-CovPP	*n* better AIs, by considering CovPP.
H-CovLOC	*n* better AIs, by considering CovLOC.
H-CovGLO	*n* better KSs, by considering CovGLO.
H-CovTOT	*n* better ADs (selected AIs), by considering CovTOT.
H-AboveAvg	*n* better AIs, by considering coverage (CovDM, CovPP, or CovLOC) above average.
H-ParetoPercentage	*n* better AIs, by considering higher coverage with lower amount of AIs.
H-ParetoFrontier	*n* better AIs, by considering CovDM and CovPP at the same time.

4. APPLYING HEURISTICS TO ISO/IEC 27001

In this section, we present a case study of an application of HCApp-Sec to the selection and prioritisation of AIs for ADs.

Among the well-known and accepted information security KSs, ISO/IEC 27001 [10] was selected (identified as KS1). The proposed heuristics were applied to KS1. The complete dataset can be found in [28].

Concerning usage examples of the heuristics, we expect (i) to verify the possibility of selecting better AIs and (ii) analyse how heuristics can be used in selection or prioritisation based on the measures of coverage of DMs and PPs.

Table 2 presents an example of the application of the H-CovDM heuristics, which resulted in the five best AIs and the five worse (informative) AIs of the KS1 dataset, according to the proposed heuristics. This heuristics attains higher diversity with respect to DMs, based on CovDM.

Table 3 presents an example of application of the H-CovPP heuristics, which resulted in five best AIs and the five worse (informative) AIs of the KS1 dataset, according to the proposed heuristics. This heuristic attains high diversity with respect to PPs, based on CovPP.

Table 4 presents an example of an application of H-CovLOC heuristics and values for CovDM and CovPP, which resulted in the five best AIs and the five worse (informative) AIs of the KS1 dataset, by considering CovLOC. This heuristics method attains high diversity with respect to DMs and PPs, based on the average of CovDM and CovPP.

H-CovGLO (Table 5) aims to select or prioritise KSs that attain the highest value of CovGLO i.e. it aims to select the KSs that are the most comprehensive by considering the average CovLOC values for all the AIs.

Table 2. Application of H-CovDM to KS1.

KS	*AI*	*CovDM*	*Obs.*
1	11.6.2	0.967	Better
1	12.3.2	0.850	
1	11.7.1	0.650	
1	11.5.6	0.650	
1	10.3.1	0.650	
-	-	-	-
1	6.1.8	0.000	Worse
1	8.2.1	0.000	
1	8.2.2	0.000	
1	8.3.1	0.000	
1	6.1.7	0.000	

Table 3. Application of H-CovPP to KS1.

KS	*AI*	*CovPP*	*Obs.*
1	10.10.1	1.000	Better
1	15.1.3	1.000	
1	13.2.3	1.000	
1	15.1.5	1.000	
1	9.2.4	0.982	
-	-	-	-
1	10.10.2	0.018	Worse
1	13.1.2	0.018	
1	10.8.4	0.018	
1	10.8.5	0.018	
1	6.1.7	0.000	

CovGLO for KS1, used in this study case, is 0.252. We intend to compare this value with other KSs in future works. This comparison can be useful for choosing, for example, which KSs should be used in certain compliance assessments.

One example of the heuristics process is 'Select the three of the best KSs by considering H-CovGLO'.

In Table 5, a simulation of a selection of all the sources of the database is presented. In this hypothetical situation, we present the selected KSs, highlighted based on H-CovGLO.

The CovGLO values of the KSs are simulated to demonstrate the use of the heuristics, with the exception of KS1, which presents the real value.

H-CovTOT aims to select or prioritise the ADs that attain high CovTOT (the average of the values of CovLOC for the selected AIs).

An example of an application of the above is 'Select the three best ADs for considering CovTOT'. Table 6 shows all three ADs prioritised for CovTOT by using the CovLOC valuesH-AboveAvg aims to select or prioritise among the most comprehensive AIs of a KS by considering the AIs with values above the average of CovLOC, CovDM and CovPP.

An example of the heuristics process is 'Select the AIs with values above the average, by considering CovPP'. Table 7 presents all the AIs selected according to the H-AboveAvg heuristics by using CovPP; additionally, H-AboveAvg can be used to select AIs by using CovDM and CovLOC.

For KS1, the averages are: CovDM = 0.220; CovPP = 0.284; and CovLOC = 0.252.

H-ParetoPercentage aims to select the smallest set of AIs of a KS, which achieves high comprehensiveness percentage. The

Table 4. Application of H-CovLOC to KS1.

KS	*AI*	*CovDM*	*CovPP*	*CovLOC*	*Obs.*
1	12.3.2	0.850	0.673	0.761	Better
1	10.10.1	0.483	1.000	0.742	
1	15.1.3	0.483	1.000	0.742	
1	14.1.3	0.483	0.900	0.692	
1	11.6.2	0.967	0.336	0.652	
-	-			-	-
1	6.1.8	0.000	0.045	0.023	Worse
1	8.2.1	0.000	0.045	0.023	
1	8.2.2	0.000	0.045	0.023	
1	8.3.1	0.000	0.045	0.023	
1	6.1.7	0.000	0.000	0.000	

Table 5. Application of H-CovGLO: selection of 3 KSs of the database.

ID	*KS*	*CovGLO*
<8>	***<FIPS (NIST) (140-2)>***	**<0.397>**
<5>	***<SANS Critical Security Controls>***	**<0.373>**
<4>	***<OWASP Testing Guide>***	**<0.295>**
2	ISO/IEC 15408	0.277
6	SBIS/CFM MOEA	0.276
1	*ISO/IEC 27001*	0.252
12	SLTI/MPOG ePing-Security	0.245
11	BACEN/STN Manual de Segurança da RSFN	0.234
7	PCI/DSS	0.211
13	CSA/CAIQ	0.198
9	SOX *Audit Checklist*	0.194
10	*Cybersecurity Capability Maturity Model* (C2M2)	0.144
14	MED-Sec-AWA Checklist	0.128
3	MITRE *Ten Strategies of a CSOC*	0.110

goal is to achieve improved completeness, but with less effort (the number of selected AIs).

Table 8 presents an example of an application of this process, which selects AIs such that the sum of CovLOC values reaches 40 % of the total for KS1".

In Figure 1, an application of H-ParetoPercentage to the KS1 dataset (CovLOC) is presented. As shown therein, after sorting the AIs by considering the individual CovLOC values of all AIs, a cut point can be identified i.e. a point at which a smaller number of AIs presents a certain percentage of CovLOC, among all the AIs of KS1.

H-ParetoFrontier aims to select or prioritise AIs considering both CovDM and CovPP at the same time (bi-objectively). After obtaining the sum of distances between DMs and PPs, values of CovDM and CovPP are obtained.

Table 9 presents an example of an application of the above, which selects AIs that have CovDM and CovPP values that are greater than 0.430.

Table 7. AIs Selected by Considering H-AboveAvg (CovPP).

ID	*CovPP*	*ID*	*CovPP*
10.10.1	1.000	12.2.1	0.518
15.1.3	1.000	14.1.5	0.491
13.2.3	1.000	9.1.4	0.473
15.1.5	1.000	9.2.1	0.473
9.2.4	0.982	6.2.3	0.464
14.1.3	0.900	7.1.2	0.445
15.3.2	0.900	12.4.3	0.409
8.1.3	0.855	11.4.4	0.409
12.2.2	0.845	10.1.3	0.409
11.4.5	0.818	12.4.2	0.364
10.4.2	0.745	15.1.1	0.364
12.3.2	0.673	8.1.2	0.364
10.9.2	0.673	9.2.3	0.355
10.7.3	0.645	9.2.6	0.355
15.2.1	0.636	11.6.2	0.336
10.8.3	0.591	11.5.4	0.336
10.9.1	0.591	11.7.1	0.318
12.5.5	0.573	11.4.1	0.318
15.1.6	0.573	7.2.1	0.309
10.2.2	0.573	8.1.1	0.309
10.4.1	0.518	15.1.4	0.309
10.6.1	0.518	12.5.4	0.300
10.9.3	0.518	10.2.1	0.300

In Figure 2, we present a visualisation of the AIs of KS1, with the values of CovDM and CovPP. In Figure 2, we can see all of the KS1 AIs plotted in the graph. The X-axis of the graph (values from 0 to 1) represents CovPP. The Y-axis of the graph (values from 0 to 1) represents CovDM.

In this view, we identify the points that can be selected or prioritised because they simultaneously achieve improved results by considering two coverage objectives (CovDM and CovPP).

For example, in Figure 2, the AIs in the upper-right quadrant are more adequate when we consider the values of CovDM and CovPP at the same time.

In [29] we detail the implementation of coverage calculus algorithms that calculate the coverage of security characteristics. This is an important step in the generation of security assessment criteria. We shared it in the GitHub Repository [30]. This

Table 6. ADs Selected or Prioritised by Considering H-CovTOT.

AD	*AI*	*KS*	*CovDM*	*CovPP*	*CovLOC*	*CovTOT*
3	12.3.2	1	0.850	0.673	0.761	0.718
3	10.10.1	1	0.483	1.000	0.742	
3	15.1.3	1	0.483	1.000	0.742	
3	14.1.3	1	0.483	0.900	0.692	
3	11.6.2	1	0.967	0.336	0.652	
-	-	-	-	-	-	-
2	10.10.1	1	0.483	1.000	0.742	0.680
2	15.1.3	1	0.483	1.000	0.742	
2	13.2.3	1	0.283	1.000	0.642	
2	15.1.5	1	0.283	1.000	0.642	
2	9.2.4	1	0.283	0.982	0.633	
-	-	-	-	-	-	-
1	12.3.2	1	0.850	0.673	0.761	0.528
1	11.6.2	1	0.967	0.336	0.652	
1	11.7.1	1	0.650	0.318	0.484	
1	11.5.6	1	0.650	0.173	0.411	
1	10.3.1	1	0.650	0.018	0.334	

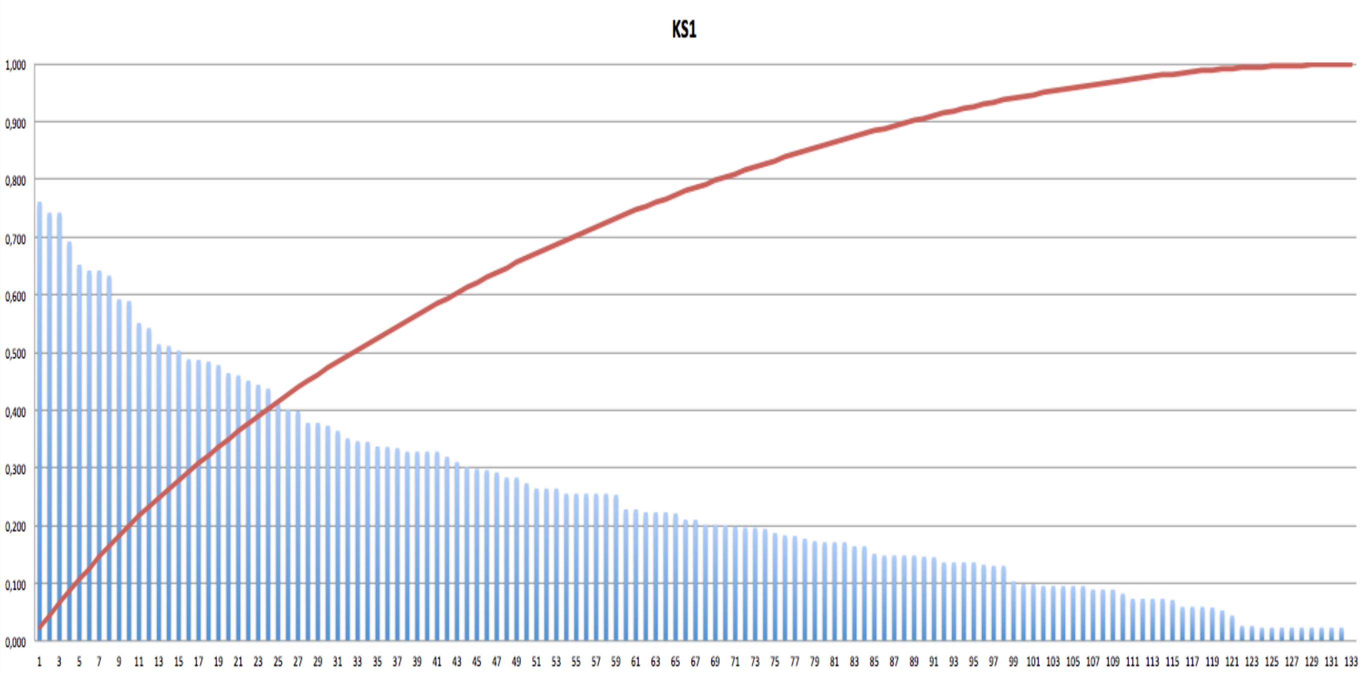

Figure 1. Application of H-ParetoPercentage to the KS1 Dataset.

implementation needs low computational resources, once the algorithms have quadratic time complexity (polynomial) considering a relatively small input (from the computational point of view) of words representing DM and PP.

5. DISCUSSION OF THE RESULTS

By using the well-known SS (ISO/IEC 27001), we observed that the proposed approach is pragmatic and realistic, and it can be useful in real-world situations of security assessments.

Table 8. AIs Selected Considering H-ParetoPercentage.

ID	CovLOC	%
12.3.2	0.761	2.27 %
10.10.1	0.742	4.49 %
15.1.3	0.742	6.71 %
14.1.3	0.692	8.77 %
11.6.2	0.652	10.72 %
13.2.3	0.642	12.64 %
15.1.5	0.642	14.55 %
9.2.4	0.633	16.44 %
15.3.2	0.592	18.21 %
10.4.2	0.589	19.97 %
11.4.5	0.551	21.62 %
10.4.1	0.542	23.24 %
12.2.2	0.514	24.77 %
12.5.5	0.511	26.30 %
15.1.6	0.503	27.80 %
12.4.3	0.488	29.26 %
14.1.5	0.487	30.71 %
11.7.1	0.484	32.16 %
10.9.2	0.478	33.59 %
10.7.3	0.464	34.97 %
15.2.1	0.460	36.34 %
10.6.1	0.451	37.69 %
8.1.3	0.444	39.02 %
10.8.3	0.437	40.32 %

The H-CovDM heuristics process attains high diversity with respect to DMs. As shown in Table 2, the best set of five AIs by following H-CovDM is: 11.6.2, 12.3.2, 11.7.1, 11.5.6, and 10.3.1.

The H-CovPP heuristics process attains high diversity regarding PPs. As shown in Table 3, the best set of five AIs by following H-CovPP is: 10.10.1, 15.1.3, 13.2.3, 15.1.5, and 9.2.4.

As shown in Table 4, by using H-CovLOC, it is possible to select the five best AIs from the KS1 dataset based on the average of CovDM and CovPP. The best set of five AIs by following H-CovLOC is: 12.3.2, 10.10.1, 15.1.3, 14.1.3, and 11.6.2.

H-CovGLO attains a high CovGLO by considering the average of CovLOC values for all the AIs. CovGLO for KS1 is 0.252. In Table 5, the CovGLO values of the KSs are simulated to demonstrate the use of the heuristics, with the exception of KS1.

H-CovTOT aims to select the AIs with the highest CovTOT of an AD, i.e. the average of the values of CovLOC for the selected AIs. As shown in Table 6, three ADs were prioritised for CovTOT by using the CovLOC values.

H-AboveAvg aims to select or prioritise AIs by considering the AIs with values above the average of CovLOC, CovDM, or CovPP. In Table 7, all AIs selected are presented according to the H-AboveAvg heuristics by using CovPP. For KS1, the

Table 9. AIs Selected by Considering H-ParetoFrontier.

ID	*CovDM*	*CovPP*
10.10.1	0.483	1.000
15.1.3	0.483	1.000
14.1.3	0.483	0.900
10.4.2	0.433	0.745
12.3.2	0.850	0.673
12.5.5	0.450	0.573
15.1.6	0.433	0.573
10.4.1	0.567	0.518
14.1.5	0.483	0.491

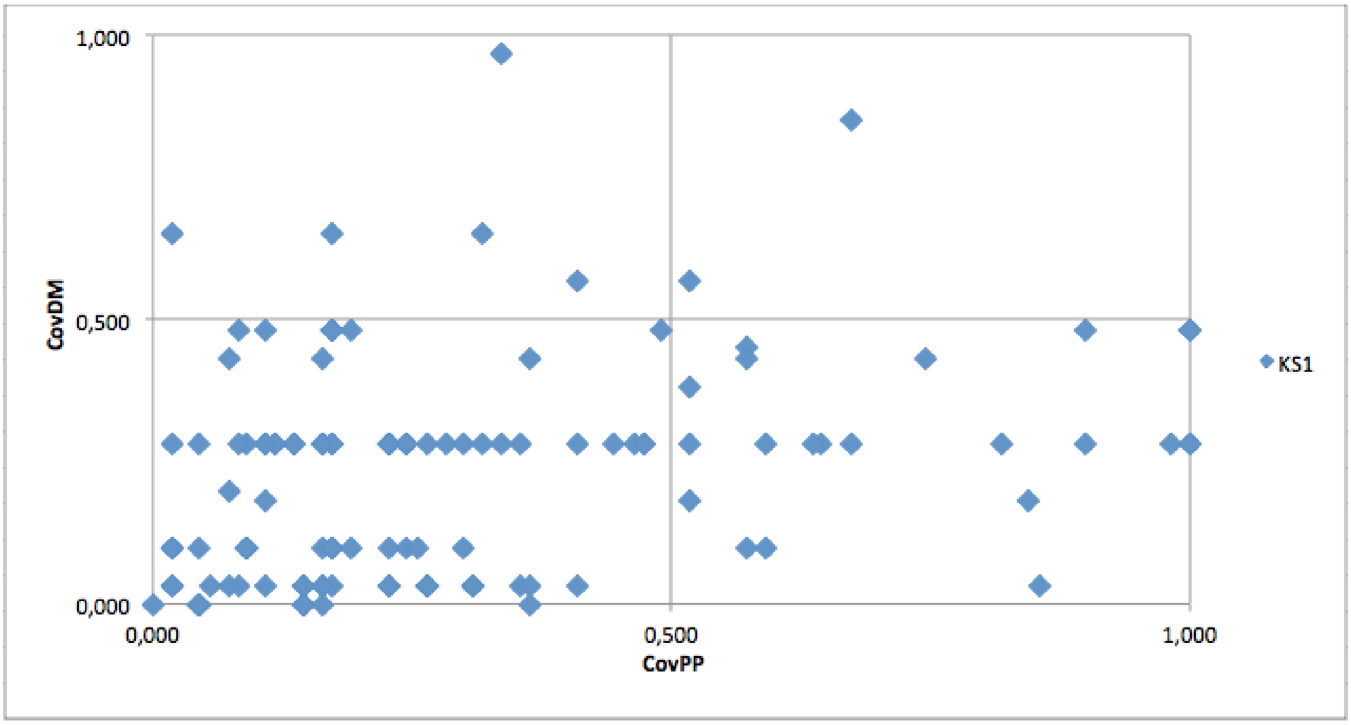

Figure 2. Visualisation of the AIs of KS1 (CovDM and CovPP).

average CovPP is 0.284. Therefore, 46 AIs were selected because the CovPP values thereof are higher than the average.

H-ParetoPercentage aims to achieve improved completeness, but with less effort. In Table 8, we present the AIs such that the sum of CovLOC values reaches 40 % of the total for KS1. As shown in Table 8, by including the AI 10.8.3, we achieved the objective of 40 % (40.32 %).

H-ParetoFrontier aims to select or prioritise AIs considering both CovDM and CovPP at the same time (bi-objectively). Table 9 presents the AIs that have CovDM and CovPP values that are greater than 0.430. As shown in Table 9, the best set of AIs by following H-ParetoFrontier is: 10.10.1, 15.1.3, 14.1.3, 10.4.2, 12.3.2, 12.5.5, 15.1.6, 10.4.1, 14.1.5.

6. CONCLUSION

In this article, we presented the HCApp-Sec coverage heuristics for selecting and prioritising AIs. Our proposal focuses on applying heuristics to make the use of SSs systematic, ensuring that security characteristics are covered by the security ADs; in this way, a small number of AIs can be selected for testing a comprehensive set of security characteristics. Our proposal can be applied to the selection and prioritisation of the AIs of any SS. We considered 11 PPs and 6 DMs. Other PPs or DMs can be included by making the additional conceptual formalisations and by defining the semantic distances from the new concepts to those already defined.

HCApp-Sec was applied to a well-known security KS (ISO/IEC 27001 – KS1). We characterised KS1 by identifying which DMs and PPs that their 133 AIs addressed. We also presented the quantities of dimensions and properties addressed by all AIs. All the proposed heuristics were exercised in the selection or prioritisation of the AIs of security ADs, thus demonstrating the feasibility of the application of our proposal.

The approach proposed herein can assist security researchers in the generation of ADs with assured coverage of key security characteristics and a priori assessment of security KSs with respect to scope and security. Specifically, the proposal can support (i) the selection or prioritisation of items with respect to the coverage and comprehensiveness of PPs and DMs; (ii) the selection of items that combine specific PPs or DMs; (iii) coverage analysis of items in an AD for more than one objective (scope or security); (iv) analysis of a source of security knowledge with respect to the coverage of important scope and security characteristics.

In future work, we hope to include PPs related to e-Voting domains, such as anonymity, uniqueness, transparency, and non-coercibility [31]. Since heuristics are approximations of objectives, one can think of replacing them with exact solutions that, for example, select the best set of 10 AIs or one of the smaller sets of AIs covering 80 % of the PPs. Our proposal is to develop algorithms to improve the selection of AIs. For example, meta-heuristic methods can be applied to indicate sets of viable solutions.

REFERENCES

[1] S. Mertl, 'How cars have become rolling computers', *The Globe and Mail*, 05.03.2016.

[2] BBC News, '"Smart" home devices used as weapons in website attack", 22.10.2016.

[3] The Tesla Team, 'A tragic loss', 30.06.2016.

[4] C.P. Barros, F. de F. Rosa, and A. F. Balcão Filho. "Software testing with emphasis on finding security defects." IADIS-The 12th International Conference on WWW/Internet. 2013, pp. 226–228.

[5] F. de F. Rosa, M. Jino, and R. Bonacin, 'The security assessment domain: a survey of taxonomies and ontologies', Technical Report, Renato Archer Information Technology Center (CTI), Campinas/SP, Brazil, 2017, Report number: PRJ04.35 – H1 14/01088 TRT0049417. DOI: 10.13140/RG.2.2.12437.73441.

[6] M. Felderer, M. Büchler, M. Johns, A.D. Brucker, R. Breu, and A. Pretschner, Security testing: a survey, Advances in Computers, Vol. 101 (2016) pp. 1–51. Elsevier.

[7] L.O. Duarte, A. Montes Filho, A.C. Guerra, and F. de F. Rosa, 'Característica segurança em qualidade de produto de software',

2010, pp. 221–228. Proceedings of IADIS Conferencia Ibero-Americana WWW/Internet, Algarve, Portugal, 2010. ISBN: 978-972-8939-34-2.

[8] F. de F. Rosa, M. Jino, and L.A.L. Teixeira Junior, 'Security assessment ontology - SecAOnto', 2017. [Online] Available: https://github.com/ferruciof/Files/blob/master/SecAOnto/SecAOnto_V4.owl. [Accessed: 12.01.2017]

[9] F. de F. Rosa, M. Jino, and R. Bonacin, 'Towards an ontology of security assessment: a core model proposal', in: Information Technology – New Generations. Advances in Intelligent Systems and Computing, vol. 738. S.Latifi (editor.) Springer, Cham, Las Vegas, 2018, pp. 75–80. DOI: 10.1007/978-3-319-77028-4_12. ISBN: 978-3-319-77028-4.

[10] ISO/IEC, ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, 2013.

[11] B.Kitchenham, Procedures for performing systematic reviews, Keele Univ., UK, 33(TR/SE-0401) (2004) p. 28.

[12] J. Biolchini, P.G. Mian, A.C.C. Natali, & G.H. Travassos (2005). Systematic review in software engineering. System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES, 679(05), pp 165-176.

[13] S. Gärtner, T. Ruhroth, J. Bürger, K. Schneider, & J. Jürjens (2014, August). Maintaining requirements for long-living software systems by incorporating security knowledge. In 2014 IEEE 22nd International Requirements Engineering Conference (RE) (pp. 103-112). IEEE.

[14] R. M. T. Colombo (2014). Proposta de uma metodologia de medição e priorização de segurança de acesso para aplicações WEB (Doctoral dissertation, Universidade de São Paulo). DOI: 10.11606/T.3.2014.tde-23122014-142055.

[15] S. Fenz (2010, March). Ontology-based generation of IT-security metrics. In Proceedings of the 2010 ACM Symposium on Applied Computing. pp. 1833-1839. ACM.

[16] S. Fenz, & A. Ekelhart (2009, March). Formalizing information security knowledge. In Proceedings of the 4th international Symposium on information, Computer, and Communications Security (pp. 183-194). ACM.

[17] DCSSI, EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), 2016. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m%7B_%7Debios.html. [Accessed: 12.01.2017]

[18] BSI, BSI Standard 100-2 IT-Grundschutz Methodology Version 2.0, 2008.

[19] S. Fenz, T. Pruckner, & A. Manutscheri. (2009, April). Ontological mapping of information security best-practice guidelines. In International Conference on Business Information Systems (pp. 49-60). Lect. Notes Bus. Inf. Process., 21, LNBIP. Springer, Berlin, Heidelberg.

[20] Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: a guide for managers. In NIST Special Publication 800-100, National Institute of Standards and Technology.

[21] ISECON, OSSTMM 3 – The Open Source Security Testing Methodology Manual, 2010, p. 213. [Online]. Available: http://www.isecom.org/mirror/OSSTMM.3.pdf.

[22] F. de F. Rosa, M. Jino, R. Bonacin, & L.A.L Teixeira Junior. (2018). An Ontology of Security Assessment. International Journal of Web Portals (Submited), 19. ISSN: 1938-0194.

[23] P. M. Bueno, M. Jino, & W. E. Wong (2014). Diversity oriented test data generation using metaheuristic search techniques. Information Sciences, 259, pp 490-509.

[24] G. Polya, How to Solve It: A New Aspect of Mathematical Method, Princeton University Press, 1973. ISBN: 0-691-02356-5.

[25] G. Rothermel, R. H. Untch, C. Chu, & M.J. Harrold (1999). Test case prioritization: An empirical study. In Proceedings IEEE International Conference on Software Maintenance-1999 (ICSM'99).'Software Maintenance for Business Change'(Cat. No. 99CB36360) (pp. 179-188). IEEE.

[26] A. Tinkham, & C. Kaner, Exploring exploratory testing. In STAR East conference, pp. 1-9, 2003.

[27] F. de F. Rosa, R. Bonacin, P.M.S. Bueno, M. Jino, 'Coverage-based heuristics for selecting assessment items of security standards: a core set proposal', Proc. of the IEEE International Workshop on Metrology for Industry 4.0 and IoT, 2018.

[28] F. de F. Rosa, M. Jino, L.A.L. Teixeira Junior, Dataset of KS1 (ISO/IEC 27001) – assessment items, 2017. [Online]. Available: https://github.com/ferruciof/Files/tree/master/Dataset-KS1. [Accessed: 12.01.2017].

[29] F. de F. Rosa (2018). HCAPP-SEC: seleção e análise de itens de avaliação de segurança baseadas em heurísticas e critérios= HCAPP-SEC: selection and analysis of security assessment items based on heuristics and criteria (Doctoral dissertation, Universidade Estadual de Campinas). [Online]. Available: http://repositorio.unicamp.br/handle/REPOSIP/332221. [Accessed: 06.06.2019]

[30] F. de F. Rosa, M. Jino, L.A.L. Teixeira Junior, and A. F. Balcão Filho, Framework para Geração de Conjunto de Critérios de Teste de Segurança de Software, 2016. [Online]. Available: https://github.com/ferruciof/Files. [Accessed: 12.01.2017]

[31] P. Salini, S. Kanmani, A knowledge-oriented approach to security requirements engineering for e-Voting system, International Journal of Computer Applications, 49(11) (2012) pp. 21–25.