Extended eTVRA vs. Security Checklist: Experiences in a Value-Web *

Ayşe Morali
University of Twente
ayse.morali@utwente.nl

Emmanuele Zambon
University of Twente
emmanuele.zambon@utwente.nl

Siv Hilde Houmb
Telenor R&I Trondheim
and University of Twente
Siv-Hilde.Houmb@telenor.com

Karin Sallhammar
Telenor R&I Trondheim
Karin.Sallhammar@telenor.com

Sandro Etalle
Eindhoven Technical University
and University of Twente
s.etalle@tue.nl

Abstract

Security evaluation according to ISO 15408 (Common Criteria) is a resource and time demanding activity, as well as being costly. For this reason, only few companies take their products through a Common Criteria evaluation. To support security evaluation, the European Telecommunications Standards Institute (ETSI) has developed a threat, vulnerability, risk analysis (eTVRA) method for the Telecommunication (Telco) domain. eTVRA builds on the security risk management methodology CORAS and is structured in such a way that it provides output that can be directly fed into a Common Criteria security evaluation.

In this paper, we evaluate the time and resource efficiency of parts of eTVRA and the quality of the result produced by following eTVRA compared to a more pragmatic approach (Protection Profile-based checklists). We use both approaches to identify and analyze risks of a new SIM card currently under joint development by a small hardware company and a large Telco provider.

1. Introduction

ISO 15408:2007 Common Criteria for Information Technology Security Evaluation [10], here referred to as the Common Criteria, is tailored for industrial purposes and is the result of the experience and recommendations of researchers and experienced developers both within the military sector and from industry. Common Criteria evaluates the security level of IT products using a hierarchy of predefined evaluation classes called Evaluation Assurance Levels (EAL). There are seven such EALs, where EAL 7 provides highest assurance. The EALs and associated guidelines take an evaluator through a well-formulated and structured process of assessing the security of specific parts of (or the complete) IT product to gain confidence in the security controls of the system.

Common Criteria security evaluation is considered a healthy approach for tackling the security issues of an IT product, as it gives detailed guidelines about the procedure to carry it on and it describes the activities that developers and security experts involved (e.g. evaluator) should undertake to ensure that all relevant security aspects have been addressed. However, a Common Criteria security evaluation is both costly and time and resource demanding. Hence, not many companies set aside budget and time to take their IT products through such a formal evaluation process. Furthermore, the security guidelines are not easily accessible for non-security experts (and security experts are a scarce resource). For this reason, the Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) program at European Telecommunications Standards Institute (ETSI), a major European Telecommunication (Telco) standardization organization with world-wide influence, developed a threat, vulnerability, risk analysis (eTVRA) method to support Telco companies in a Common Criteria security evaluation. eTVRA builds on CORAS [11] and is structured to provide output that can be directly fed into a security evaluation thus easing the evaluation process.

In this paper we evaluate eTVRA by comparing it to a more pragmatic approach based on Protection Profile checklists. We perform the comparison in terms of time, resource efficiency and quality of the results. We also evaluate the efficiency of eTVRA in a value-web context, to

*This research is supported by the research program Sentinels (http://www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

identify and analyze risks of a new SIM card currently under development in collaboration between a small hardware company and a large Telco provider. The goal for the new SIM card is to comply with EAL 4 or 4+ according to Common Criteria. Finally, we report on lessons learnt from applying an extended version of eTVRA. Based on experience from earlier assessments at ETSI [18], we extended eTVRA by adding to it a sub-process of the CORAS methodology to compensate the fact that eTVRA does not include context identification activities. Context identification is critical to produce precise risk assessment results.

The paper is structured as follows: in Section 2 we provide background information on CORAS, eTVRA and value-webs. In Section 3 we give the industrial context. In Section 4 we describe the methodology that we used to identify and analyze risks to the new SIM technology. In Section 5 we present the pragmatic approach based on checklists, and in Section 6 we compare it with the extended eTVRA methodology. In Section 7 we draw the lessons learned by using eTVRA in a value-web context. Finally, in Section 8 we conclude the paper and give directions for future work.

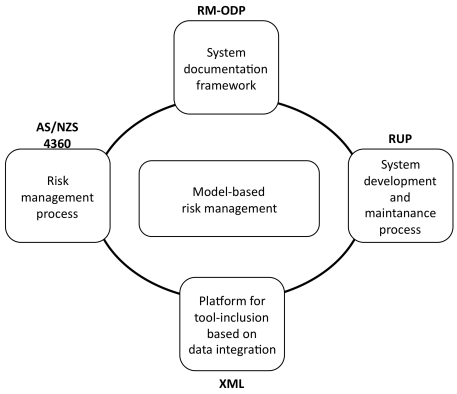

Figure 1. The five main components of the CORAS framework.

2. Background information

2.1. CORAS

CORAS [11] is a framework for model-based risk assessment of security critical systems. It consists of four main components as shown in Figure 1: (1) a risk documentation framework based on RM-ODP [1]; (2) a risk management process based on the AS/NZS 4360 [14]; (3) an integrated risk management and system development process based on the Unified Process [13] and (4) a platform for tool inclusion based on data-integration using XML. [11]

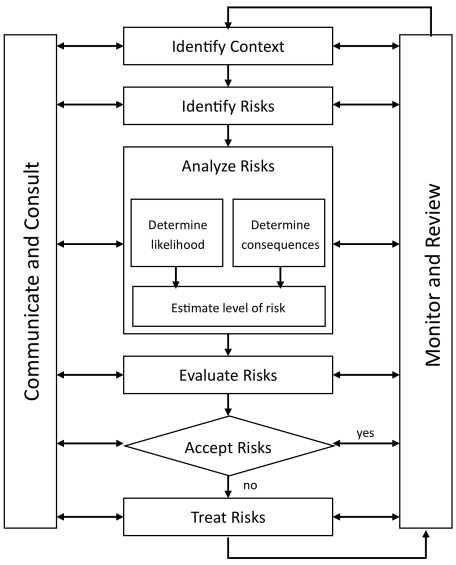

Figure 2. CORAS sub-processes

The CORAS framework is model-based in the sense that it gives detailed recommendations for modeling both the system and the risk, as well as security controls identified during the risk assessment using UML. Furthermore, CORAS is asset-driven, which means that the identification of assets is the driving task of the risk assessment process [11].

The CORAS risk management process comprises five sequential risk assessment sub-processes and two management sub-processes running in parallel (see Fig. 2).

2.2. eTVRA

Threat, Vulnerability and Risk Assessment (eTVRA) [16] is based on component 2 of CORAS and refines the risk management process developed by ETSI for risk assessment of Telco standardization projects.

The process of eTVRA consists of 7 steps [17]:

1. Identify security objectives
2. Identify security requirements
3. Inventory of assets
4. Identification and classification of vulnerabilities, threats and unwanted incidents
5. Quantifying the occurrence likelihood and impact of threats
6. Establishment of risk
7. Identification of countermeasures framework

eTVRA aims at analyzing the threats, identifying the best set of countermeasures and reduce the overall risk. The process starts with identification of the security objectives of a system or a system component, out of which security requirements are extracted. Later an inventory of the assets in the system is drafted. The purpose of using the eTVRA is to be able to identify vulnerabilities that exist in the system. Therefore, after identifying assets and their vulnerabilities, threats that exploit those vulnerabilities and cause incidents are determined. The security requirements and the threats are then extended according to threats and vulnerabilities. Then, the occurrence likelihood of the threats and their impact is analyzed and quantified. This is used in the following step to calculate the risk. Consequently, the countermeasures for treating the risk are identified. This process is applied iteratively, until the risk of unwanted incidents is reduced to an acceptable level, or whenever there are changes in the environment [16].

eTVRA encapsulates the relevant parts of Common Criteria and aims at producing high-quality input to a Common Criteria Security Evaluation. Below we provide more details on this.

eTVRA is developed mainly for security standardization. Therefore, it considers only the technical vulnerabilities and countermeasures: the business impact of security breaches is as usual outside the scope of the standards.

2.3. Value Webs

A value-web [5] consists of a set of profit and loss responsible actors that cooperate to realize a common goal. The actors can be independent companies or even business units of an holding. A value-web produces either a product or a service of some value. Some of the most commonly build value-webs are marriages, outsourcing, insurance and contractor relationships.

The main challenge of constructing and protecting value-webs is that the web should be profitable for each of the actors.

To evaluate the effects of value-webs on a risk assessment, the following evaluation criteria should be considered: (1) goal of each actor, (2) available resources, (3) confidentiality of business critical information, (4) communication of confidential information, and (5) coordination of the responsibilities of the actors.

3. Industrial context

The industrial context in this paper consists of two European companies, which collaborate as a value-web in the Telco domain. Together, they have developed the world's first GSM SIM card with embedded radio capabilities (802.11b). The two companies are a small hardware producer, which is new to the Telco market, and a large European Telco provider that is already a major player in the field. The distribution of responsibility within the development project is that the hardware producer designs and produces the (Integrated Circuit) IC technology and its firmware, while the large Telco company implements the software layer between the firmware and the operating system (OS) as well as the value-added service running on top of the OS.

One of the possible application areas for this new SIM card is automatic meter reading (AMR). AMR refers to the technology used for automatically collecting data from metering devices (e.g. water, gas, and electricity) and transferring readings to a central database for billing and analysis. In this context, a SIM card with wireless capabilities will reduce the number of terminals necessary to report the readings, hence saving a substantial amount of money. To limit the scope of the assessment and to make it feasible to do an evaluation between eTVRA and a checklist-based approach, we focused on the security of the new SIM technology in the context of AMR and on how to produce high-quality input to a future Common Criteria evaluation.

4. Methodology

We evaluated the efficiency and result quality of two risk assessment approaches; (1) extended eTVRA and (2) Protection Profile-based checklists, as input to Common Criteria security evaluation. Here, we describe the two approaches and document the changes we made to eTVRA and the risk identification and risk analysis methods that we used to support the relevant activities of eTVRA, as eTVRA does not give concrete guidelines as such.

Fig. 3 gives an overview of the extended eTVRA. The main changes we made consist in adding the context identification step taken from CORAS as well as concrete guidelines for methodologies to use for risk identification and risk analysis. The figure illustrates, besides the process flow, the information we used as input to the different steps involved, the information delivered as output of the steps and the methodologies that we used as support in producing the outputs. The extensions made to eTVRA come as a response to the deficiencies of eTVRA that are identified during earlier case studies.

4.1. Step 1: Context Identification

Earlier case studies of eTVRA at ETSI have shown that "context identification" is critical for producing more precise results. As eTVRA does not include any specific context identification activities, we extended eTVRA with the context identification sub-process of CORAS. The aim of

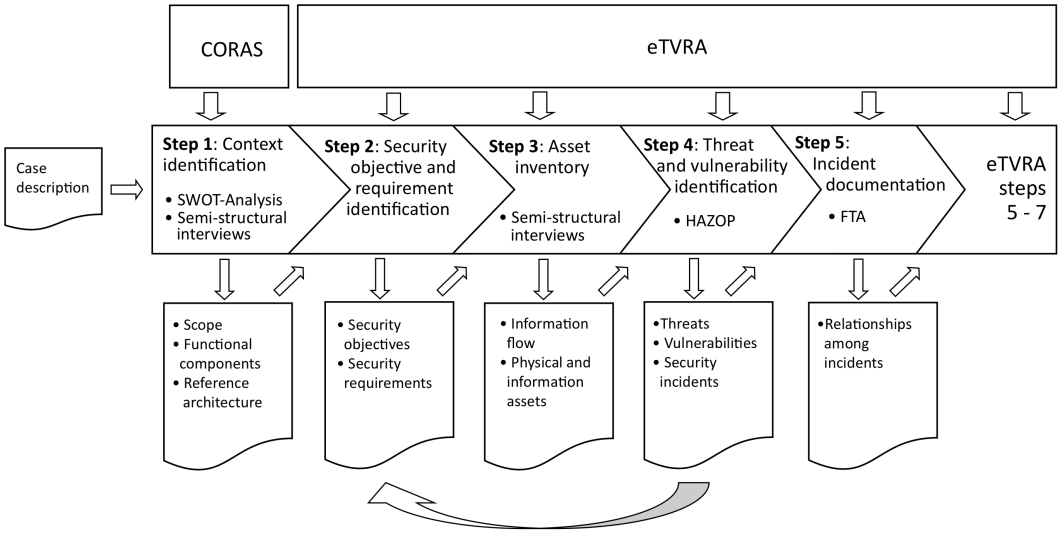

Figure 3. Extended eTVRA and the supporting methodologies that we used with input and output documents.

this sub-process is to describe the IT product to be assessed and its environment.

We used a Strengths Weaknesses Opportunities and Threats (SWOT) analysis [6] as information gathering tool to identify the scope of the risk assessment and to ensure that the two stakeholders involved agreed on the goal and the objective of the assessment.

To prepare for and to carry out an effective SWOT session we referred to the case scenario documentation. Then, we (the risk analysts), together with the product owner (the two stakeholders in the value-web), went through the current case scenario document and made sure that we had a common understanding of the assessment context and of the role of the SIM card in an AMR setting.

The SWOT analysis helped us to determine the scope of the assessment and to focus the following assessment activities. In addition to SWOT, we carried out semi-structured interviews with both stakeholders. During the semi-structured interviews we agreed with the stakeholders on the functional components of the AMR deployment scenario which we previously extracted from the case scenario documentation.

The result of this step is documented in a context identification document, which consisted of the *case description* (including the deployment scenario), the *functional components*, the *reference architecture* and the *scope* of the assessment.

4.2. Step 2: Security Objective and Requirement Identification

The first step of eTVRA is the specification of security objectives and the identification of security requirements. From this step on, we used the eTVRA process as described in [17].

To establish the security objectives we based ourselves on the output of the previous step; namely the SWOT-Analysis and the semi-structured interviews, as reported in the context identification document.

We divided the *security objectives* of the new SIM technology into security objectives of the assets and security objectives of the environment. We then combined them and defined new security objectives for the desired level of confidentiality, integrity, availability, authentication and authorization for the assets involved.

These security objectives were high-level, e.g. “The new SIM technology should ensure continuous and correct operation of its core functionality and availability to authorized use upon request.”, so for operability reasons they had to be refined into *security requirements*. Security requirements describe the details of how the security objective will be achieved.

We listed the security objectives in a Target of Evaluation (ToE) document. At that time we did not have enough information to detail security requirements, so we postponed this activity to a further step. This document was then extended with the context identification descriptions from the previous step and given to the two stakeholders for approval.

4.3. Step 3: Asset Inventory

In this step we used the information gathered in Step 1 and 2 as input. First, we had to complete the draft-list of assets that came out of the semi-structural interviews with the two stakeholders as described in Section 4.1.

For the interview with the large Telco company we used the reference architecture as input and we obtained a list of assets relevant for the information flow in the AMR case. These were assets at a high-level of abstraction (e.g. the concentrator functionality on the SIM card).

The interview with the hardware developer was carried out as a functional architecture walk-through. This resulted in assets on the physical and logical layer. We then compared these assets with the information flow assets and modeled their internal relations (e.g. dependency and containment relationships). The result of this activity was given as output of Step 3.

4.4. Step 4: Threat and Vulnerability Identification

eTVRA includes activities to identify threats and vulnerabilities but does not provide how-to guidelines (i.e. it does not provide any method/tool to systematically extract threats and vulnerabilities). We therefore used the guidelines provided in CORAS to assist us in Step 4. In particular, we used Security-HazOp [23] (in CORAS Security-HazOp is referred to as HazOp) and Fault Tree Analysis (FTA) [15].

Security-HazOp

A Hazard and Operability (HazOp) study [3] is a systematic analysis of how deviations from intended use of system components can arise, and whether these deviations can result in hazards. A hazard is defined in FAA Order 8040.4 [22] as a "Condition, event, or circumstance that could lead to or contribute to an unplanned or undesirable event."

Although HazOp has been developed for safety rather than security, i.e. for industrial processes, notably the chemical, petrochemical and nuclear industries, experiences over the years have shown that the basic principle is applicable in different contexts, such as systems containing programmable electronics [9]. Security-HazOp [23] is a security specific refinement of HazOp which includes security specific constructs.

In general, HazOp is performed by defining a set of guide-words and attributes and combining them with each other. The result can be used to describe generic deviations which help in identifying specific safety related deviations. Security-HazOp differs from HazOp in the chosen guidewords and attributes.

Srivatanakul et al. [21] criticize Security-HazOp and claim that the recommended guidewords are not flexible enough to bring out the analysts' creativity. They propose to apply guidewords to elements of a case by interpreting the guidewords for the attributes of each element of the case that is subject to deviation.

Furthermore, we took some of the recommendations given in CORAS for Security-HazOp and used as input the high-level threats and vulnerabilities discovered during the SWOT-Analysis and from relevant Smart Card Protection Profile [8].

By determining and associating the guidewords we used the following approach. First, we listed the actors, associations and elements of the AMR case. Second, we constructed a list of guidewords for the attributes of each of these main elements, as recommended by Srivatanakul for increasing the creativity of the analyst. Third, considering that more than one guideword may apply to an asset at one time, we grouped the guidewords as *pre-guide-words* and *post-guide-words* as recommenced in Security-HazOp. Last, we used the following notation to generate possible security incidents: `<pre-guideword> <attribute>` of `<component>` due to `<post-guideword>`. In this notation, *Pre-Guidewords* are the possible causes of inadequate security attributes, e.g. *deliberate*, *unintentional*.

Attributes are obtained by negating the security objectives, e.g. manipulation, denial and disclosure. *Components* are physical and information assets; and *Post-guide-words* are the possible threats, e.g. technical failure or outsider.

In this way, we obtained a list of 5400 possible incidents, e.g. *"Deliberate disclosure of meter readings due to technical failure"*. As it is not time and resource efficient to cover all of these incident in one HazOp-session, we preprocessed and eliminated impossible incidents using the security objectives identified in Step 2 as filter. The incidents space sub-set derived from this consisted of 88 possible incidents.

We organized two structured brainstorming sessions: (i) one session with the large Telco company and (ii) one session with both stakeholders. During these HazOp sessions, the RA-leader moderated the debate by using a set of "fault-statements" derived from the incident sub-set, e.g. unsorted *"How is it possible to deliberate disclose meter readings due to technical failure?"*, to motivate the attendees to structured thinking. In all cases where potential hazards were detected, the RA leader followed up by asking questions directed towards gathering information on its likelihood and its potential business impacts. Furthermore, to brighten the perspective of the attendees but remain passive in generating threats, we also used a light-weight role-play.

The output of Step 4 was an unstructured list of vulnerabilities, threats and potential security incidents.

4.5. Step 5: Incident Documentation

The list produced in Step 4 was taken as input to Step 5, where the list was structured in terms of cause-consequence relationships. We used FTA [15] to support us in this activity.

FTA

According to [14], a "fault" is an abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function. FTA is a system engineering method, which is mainly used in the safety domain. It represents, from the system point of view, the logical combinations of various system states, faults, and possible causes which can contribute to a top event (specified event). Security techniques, such as Threat Trees and Attack Trees originates from FTA [15].

We used the Fault Trees to illustrate at high-level threat-vulnerability pairs. Furthermore, we linked the incidents to each other with respect to their dependencies, e.g., if an incident a is a precondition for an incident b then we inserted incident a below incident b and indicated the relation with an arrow. Moreover, we differentiated between AND and OR causal relations.

Finally, we communicated the fault tree and the derived incident scenarios to the asset owners. The goal of this activity was to communicate and consolidate our findings and to gather additional information on the likelihood and consequence evaluation.

Currently, we are in the process of gathering likelihood and consequence of the identified threats. This activity is carried out by the two stakeholders in the value-web. The remaining processes (Steps 5, 6 and 7 of eTVRA) are going to be carried out when the likelihood and consequence evaluation is finished at the end of 2008.

5. Alternative methodology: Security Checklists from SmartCard Protection Profiles

In parallel to analyzing risks according to the extended eTVRA, we employed a more pragmatic (i.e. less time consuming) approach. We call this the PP-based approach or the security checklist from relevant PPs. This approach requires almost no interaction with the main stakeholders for threat identification as the possible threats are extracted from an existing `Common Criteria PP for SmartCards` [8]. The approach consists of four steps:

1. Description of the risk assessment object and its security environment.
2. Specification of the security functional requirements.
3. Identification of the threat-vulnerability pairs and their impact.
4. Risk analysis, prioritization and documentation.

Steps 1 and 2

Step 1 of this approach is similar to Step 1 of the extended eTVRA described in the previous section.

The security environment of the new SIM card for the AMR scenario includes (1) the assets to be protected and (2) the threat agents with their abilities to reach and exploit the assessment object or/and its environment during a reasonable product life-time (which is from product release to major natural update). To describe the security environment in this approach, we used the documentation provided in Step 1 of the extended eTVRA. According to the results of the semi-structured interviews, we classified the components of the new SIM card in the context of the AMR scenario into physical and logical components. We further classified physical components according to how they interact with the external environment (e.g. wireless connection, serial connection, etc.). This classification is useful to clarify the main attack points of each component (e.g. a certain component may be attacked only through the wireless interface).

Step 3

The third step in this approach is performed off-line, that is without interacting with the stakeholders.

We made a selection of the threats enumerated in the relevant Common Criteria PP [8]. The selection criteria we adopted were based on: (i) whether the threat agent fits in the usage scope of the new SIM card (e.g. terrorism is not a credible threat agent for the AMR scenario) and (ii) whether the threat can be perpetrated by means of the components of the new SIM card (i.e. if it exists a component in the new SIM card which can be targeted by the threat). As the new SIM card also contains several components which are not part of a standard SmartCard (e.g. a wireless interface), the threat list provided in [8] covers only partly the range of possible threats. To fill this gap we included additional threats collected during a literature search [4, 12, 2, 20, 7].

Following [8] threats are characterized by a threat agent, a threat scenario, a set of vulnerabilities enabling the threat and one or more assets targeted by the threat. The threat list can be summarized as follows:

- Threats associated with physical attacks
- Threats associated with logical attacks
- Threats associated with access control

- Threats associated with unanticipated interactions
- Threats regarding cryptographic functions
- Threats of information monitoring
- Threats addressed by the operating environment
- Miscellaneous threats

To be able to build a hierarchy among the threats, which in turn is needed to prioritize threats in the fourth step of this approach, we additionally grouped threats according to the relevant security properties confidentiality, integrity and availability. The five resulting threat categories are: (1) unauthorized disclosure of assets, (2) theft or unauthorized use of assets, (3) unauthorized modification of assets, (4) unauthorized disclosure of assets and (5) unauthorized modification of assets.

Step 4

Step four is concerned with calculating the risk level of the threats and thereby prioritizing risks. The list of prioritized risks was submitted to the main stakeholders as an addition to the earlier described ToE document. (This step has not been finalized yet.)

6. Comparison of the two approaches

The main goal of the risk assessment for both stakeholders in the value-web was to produce information that could be used, preferably directly, as input to a Common Criteria evaluation. This puts some constraints on the expected outcome of the risk assessment, and influenced how we carried out some of the steps of the extended eTVRA. This is also the reason why we decided to compare eTVRA with a more pragmatic approach of security checklists derived from existing Protection Profiles (PP).

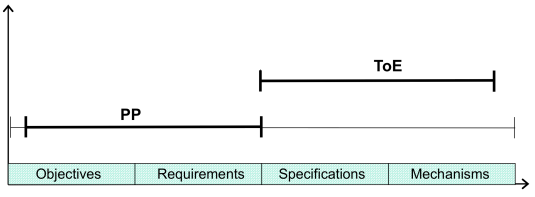

Figure 4. ST/ToE and ST/PP activity chart.

Common Criteria recognizes two types of evaluations: (1) ST/ToE evaluation and (2) ST/PP evaluation. ST denotes the Security Target. In case of an ST/ToE evaluation, specific parts of the concrete IT product are defined into a Target of Evaluation (ToE). On the other hand, PP is an implementation-independent version of a particular IT product type, such as SmartCards. This means that a PP can be looked upon as a template for a type of IT products. Figure 4 shows the different activities involved when carrying out ST/ToE and ST/PP evaluations. The two types of evaluations are not orthogonal as the output of ST/PP can serve as input for ST/ToE.

To enable reuse, Common Criteria offers a registry where IT product owners can chose to store documents from successful PP or ST/ToE evaluation. It is from the PP registry that we found the SmartCards PPs that we used for the alternative methodology (PP-based methodology) described in the previous section.

In our case, the goal is to assess the ST/ToE to reach EAL 4 or 4+. Ideally, if the SmartCard PP [8] covered all aspects of our IT product, it could have been used as a template to produce the ST/ToE documents of the object in question. However, as one always has to produce the ST-part and as the ST is ToE dependent, there is always at least some adaptation work needed, also in our case. To investigate the amount of adaptation work and the quality of the output produced, we performed a structured evaluation of the distance between the results produced and the needed input for an ST/ToE evaluation. This evaluation was done for both methodologies. Before we discuss the result of this evaluation, we list the ST/ToE requirements, which we use as evaluation criteria.

According to Common Criteria Part 1 [10], the mandatory content of an ST/ToE is the following:

- *ST introduction*, containing three narrative descriptions of the ToE on different levels of abstraction.
- *Conformance claim*, showing whether the ST claims conformance to any PPs and/or packages (e.g. threat lists), and if so, to which.
- *Security problem definition*, showing the threats, security policies and assumptions that must be countered, enforced and upheld by the ToE and its operational environment (also referred to as security environment).
- *Security objective*, which includes the security objectives for the ToE and the security objectives for the operational environment of the ToE.
- *Extended components definition*, where new components (i.e. not included in Common Criteria Part 2 [10] or Common Criteria Part 3 [10]) may be defined. These new components are needed to define extended functional and extended assurance requirements.
- *Security requirements*, where a translation of the security objectives for the ToE into a standardized language is provided. That is, standardized according to the recommendations in Common Criteria: security requirements should clearly specify the security functions, to

a level where it is possible to directly check that these security functions are actually implemented as specified and to argue that they fulfill the security objective they address.

- *ToE summary specification*, showing how the security functions specified are implemented in the ToE.

The PP-based approach (described in Section 5) produced a checklist of threat categories relevant for SmartCards. In addition, we added threat categories relevant for the wireless interface. Provided that the chosen PP has a good coverage of the IT product (new SIM card in the context of the ARM scenario), this approach should reduce at least the time, the resources and possibly the cost needed to produce high quality results in terms of usable input to ST/ToE evaluation according to Common Criteria EAL 4 and 4+. The same can be said for the extended eTVRA, as it has been developed and tailored to produce information directly usable as input to a ST/ToE evaluation, except for the EAL level. However, which of the two approaches is more efficient (that is, offers an more efficient underlying process) and which produces the highest quality result in terms of coverage and match to the ST/ToE evaluation information requirements is not clear and will be examined in the sequel. Note that we do not discuss the quality of the result in terms of is ability to pass an EAL 4 or 4+ evaluation, as the evaluation has not been performed yet.

6.1. Evaluation of result quality for the PP-based approach

To simplify the evaluation of the PP-based approach, we assumed full coverage and relevance for our IT-product. A PP document has the same basic structure as a ST/ToE document. However, the PP introduction is narrative and does not provide the information necessary for a ST/ToE introduction. Thus, this part had to be completely re-written in the form. For the remaining parts, we had to add information for the wireless interface and to tailor the contents of the PP document to fit our IT product. We did so by adding new parts and by re-formulating text for the conformance claim, the security problem definition, the security objectives, the extended components definition, and the security requirements. As a PP document does not include a ToE summary specification, this part had to be made from scratch. We could reuse a substantial amount of the existing PP text (about 40%) and we also got help in putting together the security controls necessary for the new SIM card.

We believe that this result holds in general whenever there is a close match between an existing PP and the IT product. Therefore, if those conditions are met, it is more time and resource efficient to follow the alternative approach described in Section 5. Otherwise the PP-based approach is not more efficient that extended eTVRA. We based this last consideration on the experience we gained from the AMR case study, without a formal evaluation. In addition, the PP-based approach did not identify any of the added security challenges (e.g. the public key functionalities or the key management protocol issues) which needed extra attention from the management perspective, as the roles of the two actors were not clearly defined.

Table 1. Comparison of the methodologies

	Extended eTVRA	PP-based approach
KPI(1): n. of threats	77	48
KPI(2): n. of abstraction layers	6	2
KPI(3): man-hours employed	310	68
KPI(4): re-written chapters of CC certification document	6/7	2/7

6.2. Evaluation of result quality for the extended eTVRA

The extended eTVRA produced most of the underlying information needed for the ST/ToE document. However, the output had to be re-formulated to fit the ST/ToE document requirements. Step 1 of extended eTVRA produced the goal and scope statements, which could easily be reused in a ST/ToE evaluation. Furthermore, it also identified which EAL to target and the ToE boundaries, that is, which parts of the IT product were in the scope. The SWOT and the semi-structured interviews in Step 1 also brought to light cross-organizational challenges due to the value-web configuration. Finally, the ToE document in Section 4.1, produced as output from Step 1, is at a level that made it easy to formulate the necessary ToE abstraction levels required for the ST/ToE introduction.

6.3. Summary of evaluation results

To summarize, the extended eTVRA produced richer information, but the output was not as tailored and directly reusable as that produced by the PP-based approach. However, we identified more threats using the extended eTVRA. To make a comparison which encompassed both the result quality and process efficiency, we identified four Key Performance Indicators (KPIs): (i) number of relevant threats identified during the risk assessment, (ii) number of abstraction layers in the threat hierarchy built during the risk assessment, (iii) number of man-hours employed to carry out the risk assessment and (iv) number of re-written chapters of CC certification document. KPIs (i) and (ii) express the quality of the results in terms of *result quality* and *result presentation quality*, while KPI (iii) and (iv) measures the efficiency of the underlying process of each approach in terms of *invested resources* during the assessment and for elabo-

rating the results of the assessment. Table 1 summarizes the methodology comparison.

By calculating the KPI (iii) we assumed a working day of 8 hours. Furthermore, the chapters of CC certification document are respective to the mandatory content of an ST/ToE presented in Section 6.

The results of the comparison indicates that a risk assessment following the extended eTVRA delivers better results ($\sim$37%) than the PP-based approach in that it produces a richer and more product-specific result. The main reason for this is that by using the extended eTVRA, and the supporting risk identification and analysis methods as described in Section 4, we can benefit of the creativity of the risk analyst and the stakeholders involved. This most often means that the risk identification is attacked from several viewpoints.

Moreover, in the presentation of the results produced from the PP-approach we only used two levels of abstraction. This is in contrast with the six-layer incident hierarchy resulting from the extended eTVRA. In general, having more layers is not always beneficial. However, for the critical components of an IT product, more layers ease the evaluation job of the Common Criteria evaluator: the six layers in the fault tree gives a deeper knowledge into how incidents may arise and thus also in how incidents can be prevented. On the other hand, such detailed results may not be necessary for less critical components or assets and is both time and resource demanding. At present, there is no consensus on when a richer layer is beneficial.

Considering the time spent on identifying threats, the PP-based approach is five times more efficient than the extended eTVRA methodology. This makes the former more favorable than the latter in cases where time, resources and budget are limited or when the market window is relatively short in time. Additional instructions in which the PP-approach works better is, when a limited ST/ToE is sufficient (only small parts of the IT product are evaluated), when targeting a low EAL (EAL 2 or 3) or when the PP is not used to support a ST/ToE evaluation but merely as domain knowledge.

What should also be noted is the effort spend to adapt the methodologies to cover the mandatory contents of an ST/ToE according to Common Criteria Part 1, which is indicated with KPI (iv). As the Extended eTVRA allocates only the "ST introduction" and "Security Problem Definition" Chapters, the PP-based approach requires re-writing only the "ST introduction" and "ToE Summary Specification" Chapters. Hence, the latter requires three time less re-writing, and is therefore, more result oriented.

7. Lessons Learned

The lessons learnt from the AMR case are many. They are both related to the result quality and process efficiency as discussed in the previous section and to how the extended eTVRA enables the communication needed in each step and whether it produced the information required as input for the next step in the methodology. This is particularly challenging in a value-web context. We have discussed the former in the previous section, so here we report on (i) communication and (ii) information on a value-web context.

7.1. Communication

The industrial context with two relatively different companies collaborating in a value web affected the quality of the communication throughout the assessment. One of the companies was a relatively small hardware producer new on the Telco market. Its goals with the development project was thus naturally rather different than that of the second stakeholder: the large Telco company. A small company usually has limited monetary and human resources and when such a company is new to a market, the essence is to produce a good quality product and to get penetration in the new domain. A big international player with many years in the market could care less about time and market penetration issues, as it does not depend on a single product for market visibility and cash flow. However, the two stakeholders have a common goal in the development project and that is to produce a high quality product.

We experienced some communication difficulties that we believe are due to the configuration of the value-web. First, it seems that there was no clear agreements, neither internal to each stakeholder or across the two organizations, regarding which information was company internal, company confidential or open to everybody involved in the value-web. This made it somewhat challenging to carry out assessment sessions where both stakeholders were involved. Also, the distribution of assignments within the development project seemed to have been shifted a bit since the start-up of the project due to technical difficulties.

We also experienced that it was much easier to get the communication flowing when interacting with each stakeholder separately, than it was in sessions where both were present. This could be due to the tight deadline phase that the project was in at the time of the assessment, but it could also be a general observation that is valid outside of the AMR case.

What worked well were the semi-structured interviews in Step 1 of the extended eTVRA and the separately executed risk identification sessions in Step 3. The common brainstorming sessions was less successful. We have identified two main reasons for this: (i) unspoken communication restrictions and (ii) possible unsuitability of Security-HazOp for risk identification in a value-web context.

Un-spoken communication restrictions refer to the first evaluation criteria listed in Section 2.3. Both stakeholders

had unspoken goals and expectations, that out of strategic reasons where kept hidden even though they would help clarifying some of the security challenges that were discussed.

Additional communication difficulties arose from poor management of tacit knowledge, and poor alignment between own vision of role and others' expectations [19]. This is further explored in Section 7.2.

When it comes to Security-HazOp and whether the method is efficient for risk identification in a value-web context, we made some observations that deserve further investigation. In particular, brainstorming sessions with all involved stakeholders were not effective due to the reasons mentioned above: hidden goals, assumptions and expectations. However, we believe it should be possible to adapt Security-HazOp to allow tacit information to be revealed in a non-threatening manner so that relevant stakeholders do not feel unconformable. Furthermore, confidential information should always remain secret, even if its disclosure is in the best interest of the project. We believe this issue deserves further investigation before any conclusion can be drawn.

7.2. Information

Information is crucial for the quality of risk assessment results and for the efficiency of risk assessment methodologies. If information is missing or if there are problems in interpreting it, the results produced will be poor.

As always in development projects, not much information is available in the early stages of the development. That was also true for the AMR case. In particular, information is often not made explicit at these early stages and people are not often aware of the knowledge they possess or how it can be valuable to others. Tacit knowledge is considered more valuable because it provides context for people, places, ideas, and experiences. Effective transfer of tacit knowledge generally requires extensive personal contact and trust. For risk management it is necessary to gain some understanding of the deployment scenarios to make security decisions, so it is important to extract the hidden knowledge.

In the AMR case, we extracted tacit knowledge through the semi-structural interviews. That is, we first made guesses based on the scarce information available and then asked the stakeholders their opinion on our guesses as a kick-off for the semi-structured interview. Then we tried to use the stakeholders feedback to structure our own thoughts and to arrive at a preliminary understanding of the intended behavior and deployment of the new SIM card for the AMR scenario.

The reference architecture and the functional components of the new SIM card that was given us during Step 1 of the extended eTVRA methodology is an example of implicit information. The diagram in itself did not give the risk analysts much information, as they did not have the required domain knowledge. The added information given in the semi-structured interview ensured that the diagram made sense, and could be used to articulate the security objectives. In a similar manner, we used at Step 4 of the extended eTVRA methodology the list of assets combined with our knowledge about the information flow to transfer the implicit knowledge on the threats and vulnerabilities into explicit knowledge.

8. Conclusions

This paper presented an extension of eTVRA and compared it with a more pragmatic PP-based approach on a concrete test-case as tools for producing quality results for a ST/ToE Common Criteria evaluation. The two approaches were evaluated in terms of result quality and process efficiency. The result of the evaluation is that if a suitable PP exists and if the ToE has a rather limited scope, the PP-based approach is at least more time effective, maybe also more resource and cost effective. However, it produces a more narrative result than that of the extended eTVRA approach. We argue that which of the two approaches is more suitable for a particular case depends on the goal of the risk assessment and possibly on the targeted EAL in case of a ST/ToE evaluation.

We have extended eTVRA with a context identification step. The decision on this extension was based on previous experience with eTVRA in which we show that without context definition it is hard to keep threat identification sessions, and in particular brainstorming sessions, targeted and focused.

We also extended eTVRA with methodology recommendations for threat identification and incident documentation borrowed from Security-HazOp and FTA. Security-HazOp is a security specific adoption of HazOp, which has been in use in the safety domain for several decades. HazOp is well tested and well structured and, when adequate guide-words are selected, proved to be an effective threat identification brainstorming tool. The same can be said for FTA, which showed to produce an adequate set of abstraction levels.

Future work includes finalizing the risk assessment of the new SIM card in the context of the AMR scenario, carry out more risk assessments using the extended eTVRA to get a better overview of the efficiency of the underlying process of the methodology and to give more detailed recommendations on how to produce high-quality results. The latter refers to the degree that the output can be used directly in a ST/ToE document for a ST/ToE evaluation according to Common Criteria. We also plan to investigate how value-webs introduce challenges in risk assessments and how con-

tracts can be used to cope with them.

References

[1] A. Vallecillo. *DINTEL Edition on Software Engineering. No. 3.*, chapter RM-ODP: The ISO Reference Model for Open Distributed Processing, pages 69–99. DINDEL, 2001.

[2] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. *Security Protocols*, 1361/1998:125–136, 1998.

[3] C. I. Association. A Guide to HAzard and Operability Studies, 1992.

[4] E. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In *Proceeding of the 3rd International Conference on Security in Pervasive Computing*, pages 104–118, 2006.

[5] P. Bowen, J. Hash, and M. Wilson. *Information Security Handbook: A Guide for Managers*. NIST Special Publication 800-100, 2006.

[6] BSI. *BS IEC 61882:2001 : Hazard and operability studies (HAZOP studies). Application guide*. British Standards Institute, 2001.

[7] F. C. B. Certificat. Common Criteria For Information Technology Security Evaluation: Smart Card Integrated Circuit Protection Profile (PP/9806), 1998.

[8] F. C. B. Certificat. Common Criteria For Information Technology Security Evaluation: Protection Profile Smart Card Integrated Circuit With Embedded Software (PP/9911), 1999.

[9] M. Chudleigh and J. Catmur. Safety Assessment of Computer Systems Using HAZOP and Audit Techniques. In *SAFECOMP '92: Proc. of Safety of COmputer Control Systems*, pages 285–292. Pergamon Press, 1992.

[10] ISO 15408:2007 Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, CCMB-2007-09-001, CCMB-2007-09-002 and CCMB-2007-09-003, September 2007.

[11] F. den Braber, T. Dimitrakos, B. A. Gran, M. S. Lund, K. Stolen, and J. O. Aagedal. The CORAS methodology: model-based risk assessment using UML and UP. pages 332–357, 2003.

[12] K. Eagles, K. Markantonakis, and K. Mayes. A Comparative Analysis of Common Threats, Vulnerabilities, Attacks and Countermeasures Within Smart Card and Wireless Sensor Network Node Technologies. *Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems*, pages 161–174, 2007.

[13] L. Favre, editor. *UML and the Unified Process*. IGI Publishing, Hershey, PA, USA, 2003.

[14] J. T. C. OB-007. Risk Management: AS/NZS 4360:2004, 2004.

[15] N. Roberts, W. Vesely, D. Haasl, and F. Goldberg. *Fault Tree Handbook*. System and Reliability Reseach Office of U.S. Nuclear Regulation Commition, 1981.

[16] J. Rossebø, S. Cadzow, and P. Sijben. eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope. In *AReS '07: Proceedings of the The Second International Conference on Availability, Reliability and Security*, pages 925–933. IEEE Computer Society, 2007.

[17] RTS/TISPAN-07006-TECH. Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and Protocols; Part 1: Method and Proforma for Threat, Risk, Vulnerability Analysis. Technical Report TS 102 165-1 V4.2.1, European Telecommunications Standards Institute, 2006.

[18] K. Schneider, S. Houmb, J. Jürjens, and J. Rossebø. Systematic Reuse of Experience in Security Requirements Elicitation. Technical report, ETSI, 2008. Submitted to ICSE 2009 Software Engineering in Practice Track.

[19] M. Schotten and E. Scherer. Design of co-ordination schemes in the networked enterprise. In *Proc. of IEEE International Conference on Systems, Man, and Cybernetics*, volume 1, pages 313–318. IEEE Computer Society, 1998.

[20] G. Selimis, N. Sklavos, and O. Koufopavlou. Crypto processor for contactless smart cards. In *Proc. of the 12th IEEE Mediterranean Electronical Conference*, volume 2, pages 803–806. IEEE Computer Society, 2004.

[21] T. Srivatanakul, J. Clark, and F. Polack. Effective Security Requirements Analysis: HAZOP and Use Cases. In K. Zhang and Y. Zheng, editors, *Information Security*, volume 3225 of *Lecture Notes in Computer Science*, pages 416–427. Springer, 2004.

[22] U.S. Department of Transportation - Federal Aviation Administration. Appendix G: FAA Order 8040.4, 1998.

[23] R. Winther, O.-A. Johnsen, and B. Gran. Security Assessments of Safety Critical Systems Using HAZOPs. In *SAFECOMP '01: Proc. of the 20th Int. Conf. on Computer Safety, Reliability and Security*, pages 14–24. Springer-Verlag, 2001.