Towards a UML Profile for Model-Based Risk Assessment

Siv Hilde Houmb[1], Folker den Braber[2], Mass Soldal Lund[2], Ketil Stølen[2]

[1] Telenor R&D, Norway, siv-hilde.houmb@telenor.com

[2] Sintef Telecom & Informatics, Norway, {fbr,msl,kst}@sintef.no

Abstract. The EU-funded CORAS project (IST-2000-25031) is developing a framework for model-based risk assessment of security-critical systems. This framework is characterised by: (1) A careful integration of aspects from partly complementary risk assessment methods. (2) Guidelines and methodology for the use of UML to support and direct the risk assessment methodology. (3) A risk management process based on AS/NZS 4360 and ISO/IEC 17799. (4) A risk documentation framework based on RM-ODP. (5) An integrated risk management and system development process based on UP. (6) A platform for tool-inclusion based on XML. This paper focuses on one specific aspect of the CORAS framework, namely the CORAS UML profile for risk assessment. In particular, it explains its role in the CORAS risk management process and demonstrates its use in the risk assessment of an e-Commerce system.

1 Introduction

The EU-funded CORAS project is developing a framework for model-based risk assessment. In connection with this, a UML profile for risk assessment is defined. CORAS aims for improved methodology and computerised support for precise, unambiguous, and efficient risk assessment of security-critical systems. CORAS addresses security-critical systems in general, but places particular emphasis on IT security. IT security includes all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of IT systems [6]. An IT system for CORAS is not just technology, but also the humans interacting with the technology, and all relevant aspects of the surrounding organisation and society.

The main result of the CORAS project is the CORAS framework. This framework is characterised by: (1) A careful integration of aspects from partly complementary risk assessment methods like HazOp[1] [10], FTA[2] [5], FMEA[3] [3], Markov analysis

[1] Hazard and Operability Analysis.
[2] Fault Tree Analysis.
[3] Failure Mode and Effects Analysis.

[18], and CRAMM[4] [2]. (2) Guidelines and methodology for the use of UML[5] [12] to support the risk assessment methodology. (3) A risk management process based on AS/NZS 4360 [1] and ISO/IEC 17799 [7]. (4) A risk documentation framework based on RM-ODP[6] [13]. (5) An integrated risk management and system development process based on UP[7] [9]. (6) A platform for tool-inclusion based on XML[8] [19].

An important aspect of the CORAS project is the practical use of UML to support the risk management process in general, and risk assessment in particular. Risk assessments are costly and time consuming and should not be initiated from scratch each time we assess a new or modified system. Documenting risk assessments using UML supports reuse of risk assessment documentation, both for systems that undergo maintenance and for new systems, if similar systems have been assessed earlier. The CORAS UML profile for risk assessment provides rules and constraints for risk assessment relevant system documentation.

One major challenge when performing a risk assessment is to establish a common understanding of the target of evaluation, threats, vulnerabilities and risks among the stakeholders participating in the assessment. The CORAS UML profile aims to improve the communication ability during risk assessments, by making the UML diagrams easier to understand for non-experts, and at the same time preserving the well-definedness of UML.

Requirements to security documentation and the demands to document security issues are increasing. This raises the issue of standards for ensuring and documenting the security of IT systems. The CORAS UML profile for risk assessment constitutes a contribution in this direction.

The remainder of the paper is divided into three main sections. Section 2 provides background on the CORAS model-based risk assessment methodology. Section 3 introduce and exemplifies the CORAS UML profile in a risk assessment of an e-Commerce system. Section 4 concludes and sums up the main results.

2 Background

As illustrated in Fig. 1, the CORAS risk assessment methodology is model-based in the sense that models are used for three different purposes: (1) To describe the target of evaluation at the right level of abstraction and to direct and guide the use of assessment methodology. (2) As a medium for communication and interaction between different groups of stakeholders involved in a risk assessment. (3) To document risk assessment results and the assumptions on which these results depend.

[4] British Government's Central Computer and Tele-communications Agency's (CCTA) Risk Analysis and Management Methodology.
[5] Unified Modeling Language.
[6] Reference Model of Open Distributed Processing.
[7] Unified Process.
[8] eXtensible Markup Language.

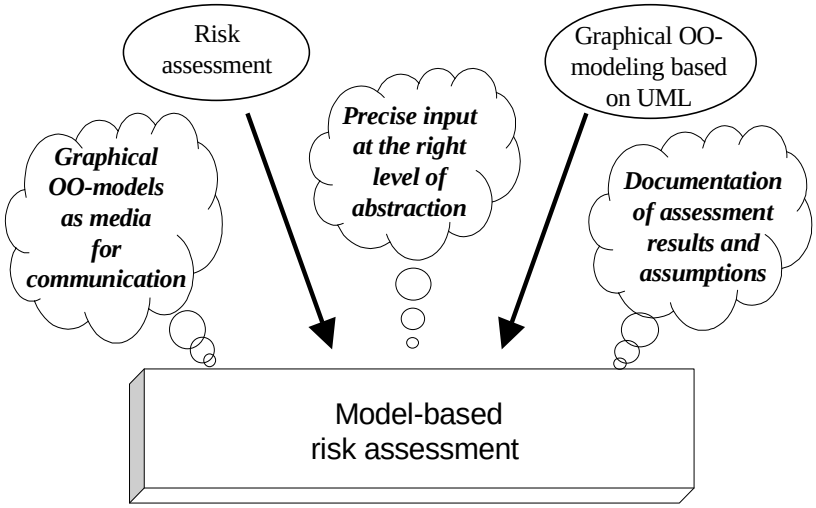

Fig. 1. Model-based risk assessment

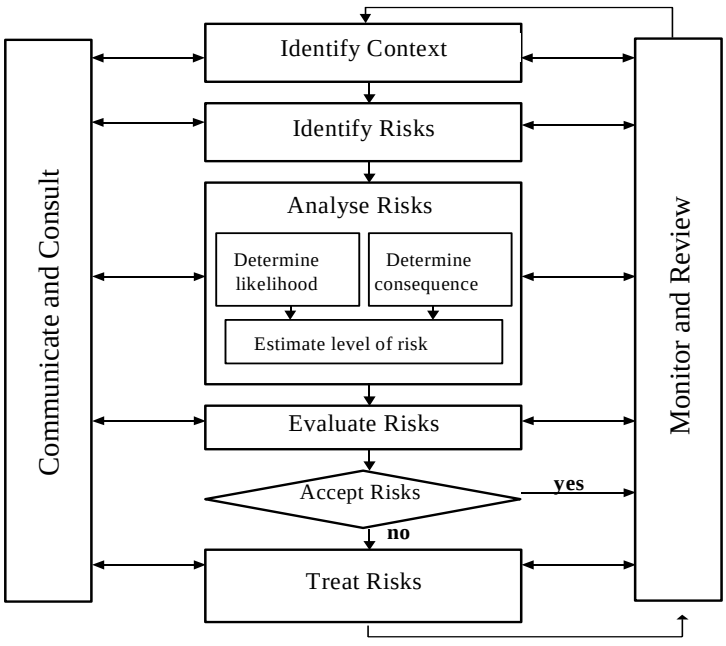

Fig. 2. The CORAS risk management process

As illustrated by Fig. 2, inspired by [1], the CORAS risk management process is sequenced into five sub-processes. In addition, there are two sub-processes, which are

running in parallel with the other five, and targeting communication and consultation as well as monitoring and reviewing.

The sub-processes for context identification, risk identification, risk analysis, risk evaluation and risk treatment are decomposed into activities as specified in Fig. 3.

Sub-process 1: Identify Context • Activity 1.1: Identify areas of relevance • Activity 1.2: Identify and value assets • Activity 1.3: Identify policies and evaluation criteria • Activity 1.4: Approval **Sub-process 2: Identify Risks** • Activity 2.1: Identify threats to assets • Activity 2.2: Identify vulnerabilities of assets • Activity 2.3: Document unwanted incidents	**Sub-process 3: Analyse Risks** • Activity 3.1: Consequence evaluation • Activity 3.2: Frequency evaluation **Sub-process 4: Risk Evaluation** • Activity 4.1: Determine level of risk • Activity 4.2: Prioritise risks • Activity 4.3: Categorise risks • Activity 4.4: Determine interrelationships among risk themes • Activity 4.5: Prioritise the resulting risk themes and risks **Sub-process 5: Risk Treatment** • Activity 5.1: Identify treatment options • Activity 5.2: Assess alternative treatment approaches

Fig. 3. Activities of the CORAS risk management process

To facilitate model-based risk assessment, a CORAS specific UML profile for risk assessment is under development. The profile defines UML stereotypes for communication and interaction among stakeholders involved in an assessment. It also defines more specialised kinds of UML diagrams, to support documentation of risk assessment results. Section 3 introduces and presents the concrete syntax of stereotypes and diagrams of the UML profile in an example-driven manner.

3 Using the CORAS UML Profile in the Assessment of an e-Commerce System

The CORAS UML profile for risk assessment is a refinement of the UML profile as defined in the UML Standard, version 1.4 [12]. The profile defines UML stereotypes and rules for specialized UML diagrams, for support of the model-based risk assessment process of the CORAS project. In order to increase the readability of the UML diagrams, most of the defined stereotypes are represented by intuitively understandable icons. The icons are introduced when they naturally occur in the examples in the following sections. At the moment the profile consists of six packages. (1) Actors Package, which defines actor stereotypes. (2) SWOT Model Package, which defines SWOT diagrams. (3) Asset Model Package, which defines asset diagrams. (4) Threat

Model Package, which defines threat diagrams. (5) State Analysis Model Package, which defines state analysis diagrams. (6) Treatment Model Package, which defines treatment diagrams.

In the following we demonstrate the use of the CORAS UML profile in the risk assessment of an e-Commerce system. Due to space limitations we can for obvious reasons only address a few of the many steps such an assessment involves. We will focus on the following:

- SWOT analysis under Activity 1.1 using SWOT diagrams.
- Identification and valuing of assets under Activity 1.2 using asset diagrams.
- Model-based threat and vulnerability identification under Activities 2.1 and 2.2 using threat diagrams.
- Model-based consequence and frequency evaluation under Activities 3.1 and 3.2 using state analysis diagrams.
- Model-based risk treatment under Activity 5.1 using treatment diagrams.

The diagrams mentioned above are all specialised UML diagrams, whose syntax is defined as part of the CORAS UML profile.

Before going into details on the risk assessment process, some background on SecureBuy, the e-Commerce system to be assessed, is required. The description is based on a specification provided in [4], which aims at developing a stochastic model for analysing risks of e-Commerce systems.

We assume that the system owner, the company Secure e-Commerce, has developed the system themselves. The SecurePay system is new, and security issues have not yet been addressed, which means that no security mechanisms are implemented prior to the risk assessment.

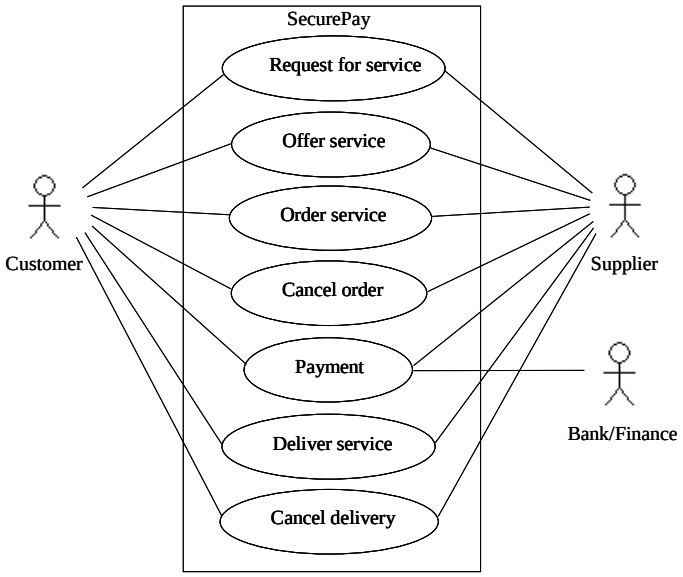

Fig. 4. Main stakeholders and services involved in the purchase process

The UML use case diagram in Fig. 4 focuses on the purchase process. It presents the main stakeholders and the main services of the SecureBuy system. The sequence diagram in Fig. 5 specifies an example-run addressing the use case “Payment” in Fig. 4 as an exchange of request (Req) and result (Res) messages.

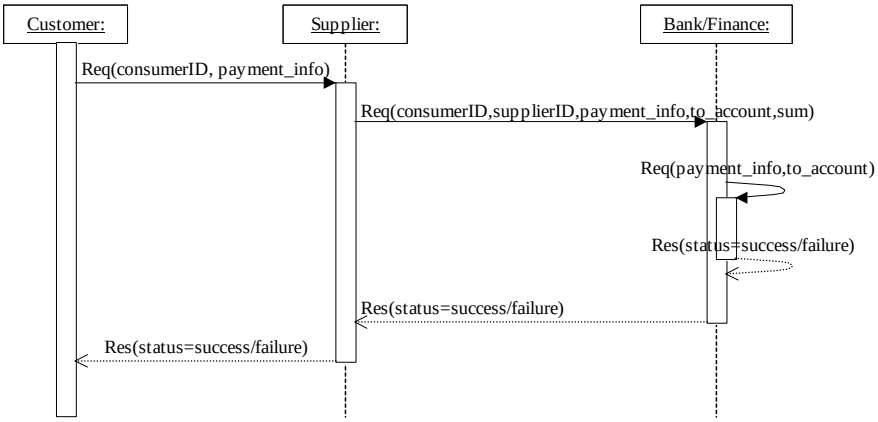

Fig. 5. Example-run addressing the use case “Payment”

3.1 SWOT Analysis under Activity 1.1

In the CORAS methodology a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis is used to define the relationship between the organisation within which the target of evaluation is situated and the environment of this organisation. The SWOT analysis identifies high-level strengths, weaknesses, opportunities and enterprise threats, and will often determine the general direction of the rest of the assessment.
A SWOT analysis of the organization Secure e-Commerce identified the following:
Strengths:
- Experience in developing and using e-Commerce systems

Weaknesses:
- Security issues not assessed during development process.

Opportunities:
- Employees with experience within the security domain.

Threats:
- Fraud.
- Denial of service (DOS).

The SWOT diagram in Fig. 6 documents these results. Strengths, weaknesses, opportunities and threats, as well as stakeholders and assets, are illustrated graphically by stereotypes defined by the CORAS UML profile. Each strength, weakness, opportunity and threat is associated with a stakeholder and an asset.

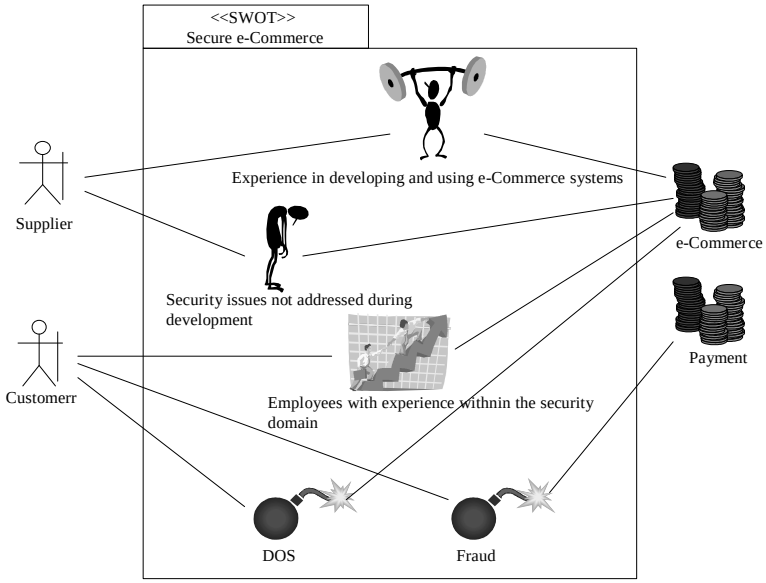

Fig. 6. SWOT results for the company Secure e-Commerce

3.2 Identification and Valuing of Assets under Activity 1.2

Identification and valuing of assets is a central element in the CORAS risk management process. If there are no assets there is nothing to protect, and no reason to worry about security. The CORAS risk management process is asset directed in the sense that the set of assets identified under Activity 1.2 strongly determines the following assessment activities. The results from the asset identification and valuing are documented in an asset table and an asset diagram.

Asset diagrams are specialized class diagrams. Assets are grouped in themes with the asset theme stereotype, and standard associations express the relationships between assets. The asset diagram also documents the assets values. The asset themes provide a classification of assets. CORAS distinguishes between six asset themes; human, physical, information, organizational, law and regulation and software assets.

Figure 7 presents an asset diagram for the company Secure e-Commerce with respect to the SecurePay system. The asset diagram specifies the identified assets, their values, and which asset theme they belong to. For the system SecurePay we use three asset themes and have identified four assets. The ownership stereotype is used to specify that the stakeholder Supplier, which represent the company Secure e-Commerce, owns all assets.

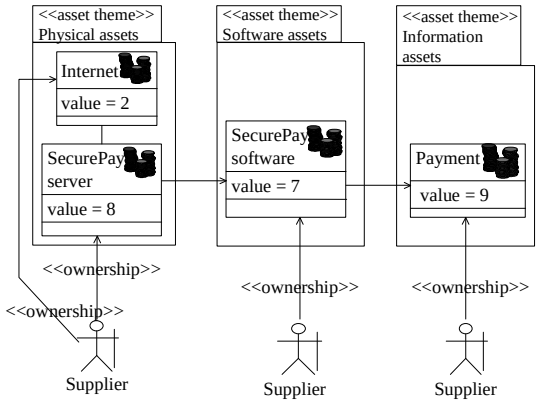

Fig. 7. Asset diagram for SecurePay

3.3 Threat and Vulnerability Identification under Activities 2.1 and 2.2

The risk identification sub-process consists of three activities of which the first two are complementary and may be carried out in any order. The third is performed first after the two others have been completed. Activities 2.1 and 2.2 address the identification of unwanted incidents from two different angles. Activity 2.1 focuses on identifying threat scenarios that may result in unwanted incidents causing loss in asset value, while Activity 2.2 focuses on identifying the vulnerabilities of assets that may be exploited by threats to cause unwanted incidents resulting in loss of asset values.

Activity 2.1 makes use of input from the SWOT, as well as the asset identification and valuation. The main strategy of the threat identification is to focus on the assets identified and valued by the stakeholders, and try to reveal threats exploiting vulnerabilities, or other threats that directly or indirectly reduce the value of an asset.

Threats and vulnerabilities are documented using threat diagrams. Threat diagrams are specialised use case diagrams, defined by the CORAS UML profile, inspired by [16]. As with use cases, threats are further specified using textual descriptions, sequence diagrams or activity diagrams.

Figure 8 present a threat diagram. The threats denial of service (DOS) and fraud, initially identified during SWOT, are represented by threat stereotypes. The consumer, which is an actor, is represented by a (human) user stereotype in the threat diagram. The attacker, which is an unauthorised user, is represented by a mis-user stereotype.

The operation identified as subject to exploitation is transfer_money. The attributes identified as potential vulnerabilities are no_authentication, and no_firewall. The threat diagram specifies the relationship between the identified threats, vulnerabilities and assets. Users and mis-users are included to specify who may cause these threats and whether or not they are authorised users or potential mis-users.

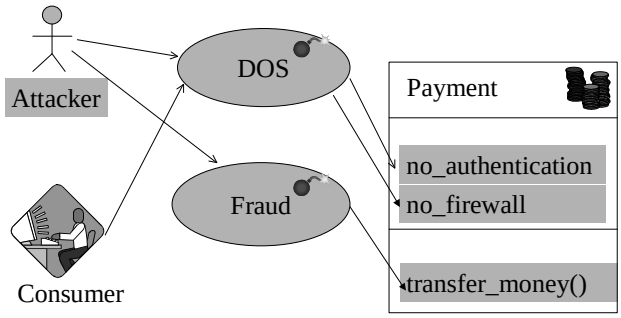

Fig. 8. Threat diagram for the system SecureBuy

3.4 Consequence and Frequency Evaluation under Activities 3.1 and 3.2

The objective of the consequence and frequency evaluation is to estimate and document the consequence and frequency values of unwanted incidents. Depending on the knowledge of the system among the members in the analysis team, frequencies may be expressed using qualitative values or quantitative values. The CORAS UML profile provides state analysis diagrams to support consequence and frequency evaluation.

Fig. 9 provides an example of a state analysis diagram for the purchase scenario, for which the scenario in Fig. 4 is part of.

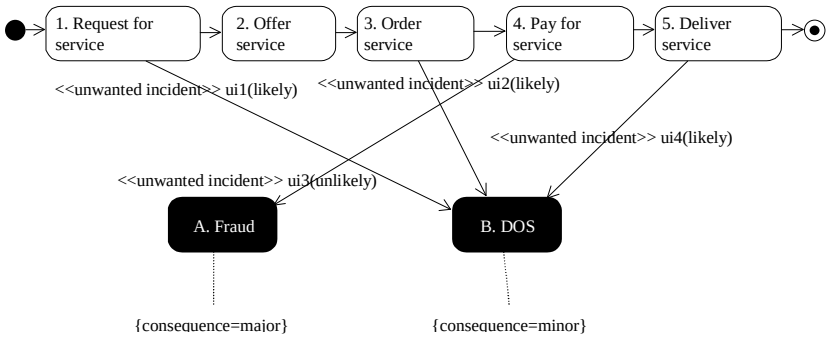

Fig. 9. State analysis diagram for the purchase scenario

State analysis diagrams are extended UML statechart diagrams inspired by [4]. A state analysis diagram specifies the undesired, as well as the desired, behaviour of the system. In addition to the desired states and desired transition describing the normal behaviour, a state analysis diagram also describes the undesired transitions and states, describing potential mis-behaviour. An undesired transition is always triggered by an unwanted incident. Unwanted incidents are represented by event stereotypes defined

in the CORAS UML profile. (An unwanted incident is in other words modelled as a specialization of the UML concept event). An undesired state can only be reached by the means of an undesired transition, and an undesired state may not have any outbound transitions.

The identified unwanted incidents – "Unauthorised transfer of money from Consumer's account" (ui1), "Request for service is prevented" (ui2), "Offer of service is prevented" (ui3) and "Delivery of service is prevented" (ui4) become triggers of transitions to undesired states – are shown as trigger events in the diagram of Fig. 9, with frequency values as parameters. Consequence values are attached to the undesired states to document the effects of the unwanted incidents.

To / From	0	1	2	3	4	5	A	B
0	0	P_{01}	0	0	0	0	0	0
1	0	0	P_{12}	0	0	0	0	P_{1B}
2	0	0	0	P_{23}	0	0	0	0
3	0	0	0	0	P_{34}	0	0	P_{3B}
4	0	0	0	0	0	P_{45}	P_{4A}	0
5	0	0	0	0	0	0	0	P_{5A}
A	0	0	0	0	0	0	0	0
B	0	0	0	0	0	0	0	0

Fig. 10. State probability matrix

A state analysis diagram may be used to generate a state probability matrix for further analysis using Markov-analysis or simulation. Fig. 10 exemplifies a state probability matrix for the state analysis diagram in Fig. 9, where P_{xy} is the probability (i.e., the frequency) of transition between state *x* and state *y*. It is not always easy or even possible to obtain quantitative values. In such cases qualitative values can be used providing they are converted to appropriate quantitative values before inserted into the state transition matrix, or if the analysis technique are capable of handling qualitative input values.

3.5 Identify Treatment Options under Activity 5.1

An important part of the risk treatment is to identify and document possible treatments and their effects. Identified treatments are documented in treatment diagrams defined by the CORAS UML Profile. Treatment diagrams are threat diagrams extended with specialised use cases representing treatments. The prevent relationships in the treatment diagrams specify which threats the different treatments are intended to treat. Option relationships in the treatment diagrams specify the assets involved and

the kind of treatment being used. The options are reduce likelihood, reduce consequence, transfer consequence and avoid consequence. Fig. 11 provides an example of a treatment diagram from the assessment of the system SecurePay. The treatment diagram documents a possible treatment for the threat denial of service (DOS).

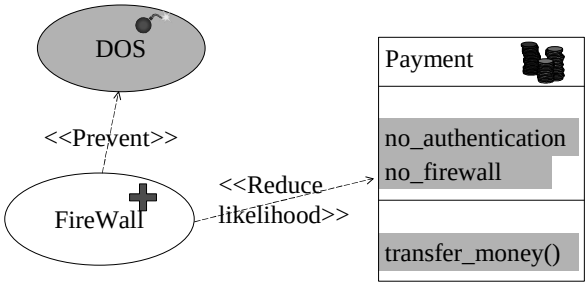

Fig. 11. Treatment diagram for the threat denial of service (DOS)

4 Conclusions

This paper has introduced the CORAS UML profile for risk assessment exemplified in an assessment of an e-Commerce system. The CORAS UML profile is motivated by several factors:

- Risk assessment benefits from correct descriptions of the target of evaluation, its context and security issues. CORAS UML profile extends the precision of such descriptions, and this is likely to improve the quality of risk assessment results.
- The graphical style of the CORAS UML profile facilitates communication and interaction between stakeholders involved in a risk assessment. This may improve the quality of risk assessment results, and reduce the danger of wasting time and resources on misconceptions.
- The CORAS UML profile facilitates a more precise documentation of risk assessment results and the assumptions on which their validity depends. This is likely to reduce maintenance costs by increasing the possibilities for reusing and updating assessment results when the target of evaluation is maintained.

To assess the impact of the CORAS methodology and guide the CORAS R&D work, six trials have been planned for the CORAS project; three within e-commerce (one of which has already been completed; see [14], for preliminary results) and three within telemedicine (one of which has already been completed; see [17] for preliminary results).

Acknowledgements

The CORAS consortium consists of eleven partners from four countries: CTI (Greece), FORTH (Greece), IFE (Norway), Intracom (Greece), NCT (Norway), NR (Norway), QMUL (UK), RAL (UK), Sintef (Norway), Solinet (Germany) and Telenor (Norway). Telenor and Sintef are responsible for the administrative and scientific coordination, respectively. The results reported in this paper have emerged through the joints efforts of the CORAS consortium.

References

1. AS/NZS 4360:1999 Risk management (1999).
2. Barber, B., Davey, J., The Use of the CCTA Risk Analysis and Management Methodology CRAMM in Health Information Systems, in MEDINFO 92, Lun, K.C., Degoulet, P., Piemme, T.E., Rienhoff, O. (eds.), North Holland Publishing Co, Amsterdam (1992), 1589 –1593.
3. Bouti, A., Ait Kadi, D., A state-of-the-art review of FMEA/FMECA. International Journal of Reliability, Quality and Safety Engineering 1 (1994), 515-543.
4. Houmb, S. H., Stochastic Models and Mobile E-Commerce: Are stochastic models usable in the analysis of risk in mobile c-commerce? Master's Thesis, Østfold University College, Faculty of Computer Sciences (2002).
5. IEC 1025:1990 Fault tree analysis (FTA) (1990).
6. ISO/IEC TR 13335-1:2001 Information Technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security (2001).
7. ISO/IEC 17799:2000 Information technology – Code of practise for information security management (2000).
8. Jacobson, I., Rumbaugh, J., Booch, G. The unfied software development process. Addison-Wesley (1999).
9. Krutchten, P., The Rational Unified Process, An introduction. Addison-Wesley, 1999.
10. Leveson, N. G., SAFEWARE, System, Safety and Computers, Addison-Wesley (1995), ISBN: 0-201-11972-2.
11. Littlewood, B., A reliability model for systems with Markov structure. Appl. Stat. 24 (1975), 172-177.
12. OMG, Unified Modeling Language Specification, version 1.4 (2001).
13. Putman, J. R., Architecting with RM-ODP, Prentice-Hall (2000).
14. Raptis, D., Dimitrakos, T., Gran, B. A., and Stølen, K., The CORAS Approach for Model-based Risk Management applied to e-Commerce Domain, CMS-2002 (2002).
15. Rumbaugh, J., Jacobson, I., Booch, G., The Unified Modeling Language, Reference manual. Addison-Wesley (1999).
16. Sindre, G., and Opdahl, A.L., Eliciting Security Requirements by Misuse Cases. In Proc. TOOLS-PACIFIC 2000. Los Alamitos, CA: IEEE Computer Society Press Sydney, Australia (2000), 120-131.
17. Stamatiou, Y. C., Henriksen, E., Lund, M. S., Mantzoranis, E., Psarros, M., Skipenes, E., Stathiakis, N. and Stølen, K., Experience from using model-based risk assessment to evaluate the security of a telemedicine application, TICD-2002 (2002).
18. Storey, N., Safety-critical computer systems, Addison-Wesley (1996), ISBN: 0-201-42787-7.
19. World Wide Web Consortium, eXtensible Markup Language (XML) v1.0, W3C Recommendtion, Second Edition (2000).