Threat Modeling in Security Architecture – The Nature of Threats

Lukas Ruf, Consecom AG, Anthony Thorn, ATSS GmbH, Tobias Christen, Zürich Financial Services AG,
Beatrice Gruber, Credit Suisse AG, Roland Portmann, Hochschule Luzern
ISSS Working Group on Security Architectures

1 Introduction

For a proper risk assessment and management, the identification and understanding of threats are crucial: they are the starting point. Literature or the internet proposes various methods of modeling threats. Usually, they follow one of two approaches to identify threats. These approaches are either based on a catalogue or a step-by-step procedure that both help in detecting threats. However, they do not or only partly address the modeling aspect per se. Or the underlying models are not exposed. A concise threat model supports the risk manager in understanding the nature of threats.

This paper proposes a new threat model by a broader view on threat distinguishing criteria. Therewith, it improves the understanding of threats and alleviates the threat-categorizing. It addresses this problem by introducing a three dimensional model that alleviates the risk assessment by introducing three orthogonal dimensions of top-level threats.

The threat model presented in this document is based on discussions within the security architecture working group of ISSS, but is not the opinion of the ISSS, nor even a unanimous statement by the working group members.

1.1 Related Work

In the area of threat modeling, two categories stand out: one approach provides very extensive lists of threats, usually grouped according to vulnerabilities to which threats might be applied. The second approach defines threat modeling as a procedure of subsequent steps that are needed to identify the threats.

A predominant example of the first class is the list of threats by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) published as part of the BSI Grundschutz Gefährdungskataloge. In this list, an extensive exemplary overview of threats already applied to assets is provided. This list of threats is based on the model of five categories labeled *force Majeure organizational deficits, human spurious actions, technological failures*, and *deliberate actions.* The list of applicable threats is compiled based on this classification method.

In the second class, an elaborate example is provided by Microsoft's document on *Improving Web Application Security: Threats and Countermeasures*[1]. In this document, threat categories are implicitly addressed by a solution-based approach in which threats are presented together

[1] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan, Microsoft Corporation, *Improving Web Application Security: Threats and Countermeasures*, June 2003.

with the appropriate security services and an available, recommended solution. Specifically, threat modeling is understood there as a procedural approach to define the sequence of specific assessment steps to be applied while doing the threat identification and categorization.

While both approaches provide specific solutions, they do not explicitly address the issue of modeling threats in a broader sense: the former serves as one of *the* lookup-catalogues of threats-per-asset examples while the latter addresses solutions directly to improve security. Both approaches, thus, lack the desired orthogonal non-ambiguity to understand the nature of threats and alleviate therewith their mitigation by appropriate countermeasures.

We argue that a discussion of threats categories along with the proposal of an orthogonalized threat model contributes to the understanding of the nature of threats.

2 Threat Model

An orthogonal classification schema provides required means to support the understanding and to alleviate the investigation process in a structured way. Structured processes are important. In the context of threat identification, they are fundamental since threats span multi-lateral problem spaces since often, threats are created based on series and coincidences of preceding threats and vulnerabilities.

In multi-lateral problem spaces, orthogonality is difficult to achieve and not realistic if threats are created by series of preceding threats and vulnerabilities residing in various angles. However, the nature of threats, i.e. the origin of all subsequent threats, need to be understand for a comprehensive view and extensive risk management.

Realizing this need, we propose a fundamental separation of two types: first, a top-level class of threats, i.e. the origin or nature of threats, and second, the *mesh of threats* that results from the series and sequences of interdependent threats at lower levels. In this paper, we address primarily the first type, the top-level threats.

2.1 Threat Classification Method

For the classification of top-level threats, we propose to categorize the threat space into subspaces according to a model of three orthogonal dimensions labeled *Motivation, Localization and Agent.* Figure 1 provides a visualization of the orthogonal threat dimensions.

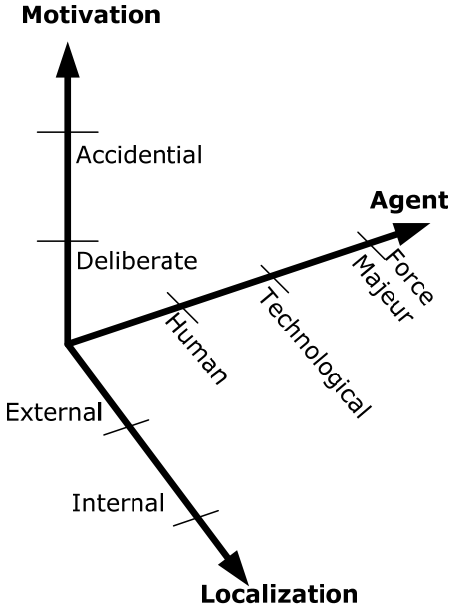

Figure 1: Threat Dimensions

The three dimensions are proposed to answer the following three fundamental questions[2]:

- **Who** is the agent?
- **Why** is the agent motivated?
- From **where** does the agent threaten the asset?

These three dimensions together with the specific criteria are discussed in the following subsections.

2.1.1 Threat Agent

The threat agent is the actor that imposes the threat on a specific asset. For the specific classification of the threat agent, three classes are identified as follows:

- Humans
- Technological
- Force Majeure

While the first class is pretty obvious and refers to threats caused by humans like for example users, attackers, auditors, the community or governmental bodies, the distinction and clear demarcation of the second and third classes need slightly more elaboration.

Technological threats are caused by physical and chemical processes on material. As an example of technological threats, aging processes are identified.

Threats by force Majeure agents are primarily environmental like for example earthquakes, lightning, wind or water but also due to animals and wildlife. While this threat agent provides a neat top-level threat, the top-level impact on technology most frequently creates a larger mesh of threats at lower levels. Examples are lightning strikes that caused trees pulling down power lines which then caused power outages due to grid-breakdowns.

2.1.2 Threat Motivation

The second dimension describes a categorization of threats along a binary classification that focuses on the motivation of this threat. This distinguishes between *deliberate* and *accidental*.

We argue that this top-level threat distinction is sufficient to classify all the threats along the motivation axis to answer the question 'why' a threat is created, For example combined with the agent dimension, a threat caused by a human threat agent is caused either by a deliberate intention or accidentally by carelessness. For the technological class, only accidental threats are conceivable/possible, since deliberate motivation is only possible for a human. The same applies to force Majeure.

2.1.3 Threat Localization

For the localization of threats, we also propose a binary classification of the origin. By this binary decision, we achieve completeness since the origin must always be located inside or outside the perimeter.

2.2 Threat Model Completeness

Our threat model is complete and spans the full space of top-level threats. The reason for this statement is based on the results of the subsequent analysis:

- An agent delivers the information on whom or what causes the threat. Our classification into *human, technological* and *force Majeure* covers there the full set of potential agents since we include humans on the first hand, second, chemical and physical reaction on hu-

[2] The reader may wonder where the 'What?' question is answered as the threat catalogues do: The threat per se (the 'what') resides in the sub-space spanned by the three dimensions.

man-made objects (technological), and, third, force Majeure for all those agents on which humans do not have any influence.

- By the motivation we answer the question why a threat is created. With our proposal of a binary classification schema of threats into *deliberately* and *accidentally* caused we cover all reasons why a threat is created since we abstract those threats that are caused by an agent without will as being accidentally created.
- For the problem to localize the origin of a threat, we define a binary classification schema as well that categorizes the origin into *internal* and *external*. This classification schema is sufficient to cover all origins for top-level threats since a threat is either caused from within an organization, system or architecture or from an external point of origin.

Following this line of argumentation, we argue that our threat model is complete and covers the full space. Moreover, since the aspect of time is reflected by the success probability of a threat being applied to a vulnerability of an asset, we explicitly exclude this fourth dimension from our threat model. In addition, we leave aside impact-based categories since they are not part of top-level threats. Analogously, we do not include threats caused by left-aside countermeasures.

2.3 Use of the Threat Model: Comparable Threat Vectors

Sub-spaces within an N-dimensional space are identified usually by an N-dimensional vector. Analogously, our threat model provides the foundations to define 3-dimensional threat vectors in a unified way along the three dimensions introduced above. However, for threat vectors it is particularly crucial to note that only the targeted sub-space is identified and neither its length nor its direction.

Irrespective of this particularity, threat vectors provide a suitable method to describe the specific threat exposure of an architecture or system. We propose to follow our threat model and to insert the specific values of applicable threats in the respective dimensions. We recommend not restricting effective threat values to the top-level threats but covering the mesh of threats by respective threat vector instances. By this method, the specific aspect of concern is represented specifically for a system under investigation.

By the implementation of this recommendation, the threat exposure of an architecture or system becomes comparable with other designs. This comparability of the threat exposure alleviates then the risk-based selection of suitable security architecture or the definition of a suitable security baseline.

3 Summary and Conclusion

In this paper, we have proposed and introduced a new threat model that, first, defines a complete, orthogonal model of top-level threats, and, second, alleviates the categorization of threats in a uniform way. Furthermore, we have shown its relation to the mesh of threats that is created by threats residing at a lower level.

We position this model in relation to existing threat models by asserting the benefit of orthogonality and completeness combined with its clear modeling focus rather than addressing process and procedural aspects. By leaving aside process and procedural aspects explicitly, our model provides therewith the foundations to come up with a comparability of threat exposures of different architectures and systems uniformly. We also left aside the threat strength as there is no consensus on how to quantify and threat strength is mostly qualified in relation to defense strength.

This comparability provides the means to alleviate the process of secure system design, implementation and deployment by a generally accepted method for comparing different approaches.