www.elsevier.com/locate/ress

Moving beyond probabilities – strength of knowledge characterisations applied to security

Tore Askeland, Roger Flage, Terje Aven

PII: S0951-8320(16)30732-3
DOI: http://dx.doi.org/10.1016/j.ress.2016.10.035
Reference: RESS5684

To appear in: *Reliability Engineering and System Safety*

Received date: 4 April 2016
Revised date: 6 October 2016
Accepted date: 30 October 2016

Cite this article as: Tore Askeland, Roger Flage and Terje Aven, Moving beyond probabilities – strength of knowledge characterisations applied to security *Reliability Engineering and System Safety* http://dx.doi.org/10.1016/j.ress.2016.10.035

Draft 14.11.16

Moving beyond probabilities – strength of knowledge characterisations applied to security

Tore Askeland*, Roger Flage, Terje Aven
University of Stavanger, PO box 8600 Forus, 4036 Stavanger, Norway
tore.askeland@uis.no
roger.flage@uis.no
terje.aven@uis.no
*Corresponding author.

Abstract
Many security experts avoid the concept of probability when assessing risk and vulnerabilities. Their main argument is that meaningful probabilities cannot be determined and they are consequently not useful for decision-making and security management. However, to give priority to some measures and not others, the likelihood dimension needs to be addressed in some way; the question is how. One approach receiving attention recently is to add strength of knowledge judgements to the probabilities and probability intervals generated. The judgements provide a qualitative labelling of how strong the knowledge supporting the probability assignments is. Criteria for such labelling have been developed, but not for a security setting. The purpose of this paper is to develop such criteria specific to security applications and, using some examples, to demonstrate their suitability.

1 Introduction

In security contexts risk is commonly assessed through the triplet, threats, values and vulnerabilities, or threats, vulnerabilities and consequences (Cox 2008). Threat levels are judged by reference to capacity and intention, but explicit probability judgements are not commonly used. There is broad scepticism in the security community towards using probabilities. Many security experts think about probabilities as frequency probabilities, interpreted as the fraction of times an event would occur if the situation were repeated over and over again infinitely under similar conditions, and find this type of probability not to be meaningful for characterising the "chance" that a threat is realised. With such an interpretation, we would also avoid the probability concept in security risk and vulnerability assessments. However, the relevant interpretation of probability in security settings is not frequentist probabilities but subjective probabilities; sometimes also referred to as judgemental or knowledge-based probabilities, see e.g. Aven (2013a). Many professionals are not familiar with this type of probability, but it is the appropriate one to use for this type of application. Let A be the event that a specific type of attack occurs in a given country during the next week. Then an expert may assign a probability of this event occurring, given his/her background knowledge K, to be, say, 0.1. Mathematically we can write

$$P(A|K) = 0.1. \qquad (1)$$