Reliability Engineering and System Safety 119 (2013) 229–234

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts

Terje Aven

University of Stavanger, Norway

ARTICLE INFO

Article history:
Received 14 March 2012
Received in revised form
26 May 2013
Accepted 26 June 2013
Available online 6 July 2013

Keywords:
Subjective probabilities
Intentional acts
Imprecise probabilities
Risk management
Threat classification

ABSTRACT

In security applications probabilities are commonly avoided – it is said that they are impossible to determine and that they are of little interest as a tool to support the decision making and the risk management. Often qualitative assessments are performed on the basis of judgments of actors' intentions and capacities, without references to a probability scale. An example of such a structure is the grading done by the Norwegian Police Security Service (PST), which defines for example a moderate threat level as "One or more parties have the intention and capacity to strike at specific interests. There is an unspecified threat". In this paper we carry out an in-depth analysis of the meaning of the concept probability in a setting with intentional acts, the main aim being to provide new insights on the scope and use of probabilities in such situations. Comparisons are made with qualitative structures as the PST grading. We question if probabilities have in fact a role to play in security management. The paper concludes that the security field cannot and should not do without judgments of uncertainties using some scale of likelihood or confidence, but such judgments need to be supplemented by other approaches which highlight the background knowledge (including assumptions) that these judgments are based on.

1. Introduction

The Norwegian Police Security Service (PST) has defined four categories of threat levels [14]:

1) Low: The likelihood of a terrorist attack is low. One or more parties may have the intention of, but are not thought to have the capacity to strike at specific interests.
2) Moderate: The likelihood of a terrorist attack is moderate. One or more parties may have the intention of and capacity to strike at specific interests.
3) High: The likelihood of a terrorist attack is significant. One or more parties have the intention and capacity to strike at specific interests. There is an unspecified threat.
4) Extreme: The likelihood of a terrorist strike is extremely high. One or more parties have the intention to strike at specific interests. There is a specific threat. No further warnings are to be expected before a strike is carried out.

Similar systems exist in other countries, for example the UK Government uses the five categories: low – an attack is unlikely, moderate – an attack is possible but not likely, substantial – an attack is a strong possibility, severe – an attack is highly likely, and critical – an attack is expected imminently [16].

These levels refer to likelihood, in the sense that the likelihood is said to be low, moderate, significant and extremely high (or that the attack is unlikely, not likely, highly likely), but without any reference to the quantitative scale of [0,1] normally used for probabilities. In the PST system the categories are linked to some conditions concerning parties' capacities and intentions to strike some interests. These examples are not uncommon in the security community. There is a skepticism about the use of probabilities in the normal sense. The issue is discussed by for example [11], see also [12]. These authors point to some of the problems raised:

a) Security failures are deliberate and thus not open to probabilistic analysis and modeling. The attackers know what they are doing so where are the uncertainties?
b) Probability is difficult to use because of the essentially unrepeatable nature of the key events.

As commented by [11], the system owner and the defenders will not normally have the knowledge available when the attacker will act and in what way, there are uncertainties. And as probability is a tool for representing or expressing uncertainties, probability enters the scene also in such contexts. The events considered are often on–off situations which excludes frequentist

E-mail address: terje.aven@uis.no

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.06.044

probabilities – but subjective (also referred to as judgmental or knowledge-based) probabilities can always be used.

But why then do we see so seldom subjective probabilities used in security contexts? Are there special problems in using them in security settings or is their absence just a result of the security environment not knowing what these probabilities represent and how to apply them? These are the main issues we discuss in the present paper. Two hypotheses that initiated the present paper were that (i) the security community rejects the use of probabilities as their reference is frequentist probabilities, and (ii) there is a potential for meaningful use of subjective probabilities (including also interval subjective probabilities) in such settings provided that these probabilities are adequately defined and interpreted.

The latter hypothesis is the main focus in this paper. How should we understand and use such probabilities in practice? A well-known problem with specifying (subjective) probabilities in security contexts is that they are so linked to the risk management responses (see e.g. [5]): the analysts may for example assign a high probability number for an attack against some specific facility, the result being that some protective measures are implemented. This action may however cause potential attackers not to consider these facilities as suitable targets, and hence the probability of an attack needs to be reduced.

The example demonstrates clearly how important it is to be precise on what is the background knowledge that the subjective probabilities are based on. In the paper this issue is analyzed in detail: is it possible by proper structuring of the background knowledge to still use such probabilities in a meaningful and useful way? In the paper we also question if it is possible to reformulate qualitative statements such as (1)–(4) above by means of such probabilities? Before we go into the discussion a brief summary of fundamental ideas and definitions related to probability are given.

2. Fundamental ideas and definitions related to probability

The most general interpretation of a probability is simply to say that a probability is a measure for representing or expressing uncertainty, following the rules of probability calculus. However, this is not sufficiently precise, as the measure is not defined, and, depending on the measure, we are led to completely different perspectives. Basically, as noted for example by [4], there are two alternative interpretations that could be used; a probability of an event A is either:

i) A frequentist probability, expressing the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed. We denote this probability by $P_f(A)$. This concept is a model concept (a parameter of a probability model), and as $P_f(A)$ is unknown – it has to be estimated. Hence we get a distinction between the underlying concept $P_f(A)$ and its estimate $P_f(A)^*$ (say), or;
ii) a subjective (knowledge-based, judgmental) probability. This probability is a subjective measure of uncertainty conditional on some background knowledge K (the Bayesian perspective) [9,10]. The probability is interpreted with reference to an uncertainty standard, for example an urn: if the assessor assigns a probability of an event A equal to say 0.1, it means that the assessor compares his/her uncertainty about the occurrence of the event A with drawing at random a specific ball from an urn that contains 10 balls. To show the dependency of the background knowledge K (data, models, assumptions) that the probabilities are based on, we write $P(A|K)$. For other ways of interpreting a subjective probability and related discussions of suitability of these interpretations, see e.g. [15].

We will also mention imprecise probabilities. The theory of imprecise (interval) probability generalizes probability by using an interval $[\underline{P}(A),\overline{P}(A)]$ to represent uncertainty about an event A, with lower probability $\underline{P}(A)$ and upper probability $\overline{P}(A)$, where $0\leq\underline{P}(A)\leq\overline{P}(A)\leq 1$. The imprecision in the representation of the event A is defined by $\Delta P(A)=\overline{P}(A)-\underline{P}(A)$. To interpret these intervals we can use the reference to the urn standard: consider the subjective probability $P(A)$ and say that the analyst states that his/her assigned degree of belief is greater than the urn chance of 0.10 (the degree of belief of drawing one particular ball out of an urn comprising 10 balls) and less than the urn chance of 0.5. The analyst is not willing to make any further judgments. Then the interval [0.1, 0.5] can be considered an imprecision interval for the probability $P(A)$. Considerable research has been conducted in recent years to establish theories and calculation rules for dealing with imprecise probabilities (see e.g., [7,6,3]), two main directions being imprecision intervals based on the theories of possibility and evidence (formally, possibility theory can be seen as a special case of the evidence theory).

3. Discussion of the meaning and use of probabilities in a security context using some examples

We discuss a context for the probabilities where a set of attacks A may occur, leading to some consequences C, with respect to something that humans value, for example economic values, health and the environment. The type of the events may be known to varying degree. We distinguish between three types of unforeseen and surprising events [1,2]:

I) Events that were completely unknown to the scientific environment (strict unknown unknowns).
II) Events that were not on the list of known events from the perspective of those who carried out a risk analysis (or another stakeholder) (unknown unknowns in the weak sense).
III) Events on the list of known events in the risk analysis but found to represent a negligible risk

For short we refer to all these events as black swans, and the two first as unknown unknowns. It is tacitly understood that they have a potential for severe consequences.

Subjective probabilities are considered used to represent or express the uncertainties concerning the occurrence of these events A.

If it has become known that for a specific event A', for example an intrusion in a data system, the consequences, C, will be severe, we speak of a security hole. Intruders may try to exploit the hole intensively until the hole is fixed. In cases of security holes, the probability of the event A' is close to one and further assignment analysis is not required.

To be prepared for possible attacks, the defender will of course think protection and try to avoid such holes. The system designed and operated are made robust/resilient to protect the values of interest. However, in practice there will always be economic limitations – a balance has to be made between cautionary measures and costs. The issue is then to what extent (subjective) probabilities can support the decision making.

Consider a situation where we face three sources (1, 2 and 3) for an attack (actors carrying out the attack) within a specified period of time (absolute time or for a time of exposure). The first two are known and can lead to attacks A_1 and A_2, respectively, whereas the third is unknown and can lead to attack A_3 (being unknown means that the event will be of category I or II) using the above categorization, i.e. an