APPLYING DECISION THEORY TECHNIQUES TO INFORMATION SECURITY RELATED DECISIONS

Cezar VASILESCU

Regional Department of Defense Resources Management Studies, Brasov, Romania

***Abstract**: Software designers and security specialists can improve their selections if they choose to apply decision theory techniques to reduce the uncertainty involved. In case of security technology selection decisions, decision theory is attractive because it provides a methodology to cope with the uncertainty and multi-objective nature of these decisions. This paper defines the information security technologies selection problem and tries to present different alternatives to be employed when quantifying the benefits of security countermeasures in correlation with the consequences of successful computer-based attacks. Moreover, it presents the sources of uncertainty underlying the process of taking decisions related to what security technology to use.*

***Keywords**: decision theory, information security, countermeasures, information system.*

1. INTRODUCTION

Information Technology software projects and their implementation during the lifecycle contain a certain percentage of uncertainty in the objectives and in the selection of the appropriate ways to fulfill them. Software designers and security specialists can improve their selections if they choose to apply the power of decision theory to reduce the uncertainty of their success. This involves relying on somebody else's specialized expertise that leads to a very important question: how to apply decision theory techniques to information security related issues and deal with the challenges that could appear. There are several selection methods and methodologies recommended to be used to solve the security technology selection problem [1]. Using decision theory in choosing software security technologies is very challenging and usually the specialist may have to address two decisions:

- If the final goal is to replicate another's security manager security selections or to improve them;
- The appropriate level and detail of information necessary to make reasonable selections.

Both issues impact the structure of the selection method and the source of information used to make security technology decisions. To better understand how to respond to these challenges, we first need to examine the nature of decision theory and its standard methods of application.

Using decision theory we could provide answers to four main questions [2]:

1. *What is a decision?* We can define a decision as "*a conclusion or resolution reached after consideration*" [3]. Another definition that is close to our goals states that *"a decision is a choice made by some entity of an action from some set of alternative actions"* [2].

2. *What makes a decision good?* A decision is good when it identifies an alternative that the decision maker believes will be as effective as other alternative actions.

3. *How should one formalize evaluation of decisions?* Good decisions are formally characterized as actions that maximize expected utility. Decision theory formalizes this notion in stages:

- It first presumes an association of a set of outcomes with each action. A stands for the set of all outcomes identified with the actions or alternatives.

A = action $\rightarrow$ outcome.

- Then, it presumes a measure U of outcome value that assigns a utility $U(\omega)$ to each outcome $\omega \in \Omega$. Ω stands for the set of all outcomes identified with any actions (the union of those associated with each action). The outcomes must be identified so as to have some determined value or utility of the decision under consideration. This is to ensure that a single outcome cannot come about in ways that differ in value.
- Then it presumes a measure of the probability of outcomes conditional on actions, where $P_r(\omega \mid a)$- probability that outcome ω comes about after taking action $a \in A$ in the situation under consideration.
- Using these elements, the expected utility $EU(a)$ of an action a as the average utility of the outcomes associated with the alternative, weighting the utility of each outcome by the probability that the outcome results from the alternative,

$$EU(a) = \int_{\Omega} U(\omega) P_r(\omega \mid a) d\omega \qquad (1)$$

4. *How should one formulate the decision problem confronting a decision maker?* Alternatives, outcomes, probabilities and utilities are identified through an iterative process of hypothesizing, testing and refining sequences of formulations. By using knowledge of the situation and through direct queries, alternatives and outcomes can be identified.

In the case of security technology selection decisions, decision theory is attractive because it provides a methodology to cope with the uncertainty and multi-objective nature of these decisions. If the consequence of actions/decisions (the result) is uncertain, decision theory calls them risky decisions.

Risky decisions can also have multiple objectives, each having an attribute that is the degree to which a given decision objective has been attained.

The value of each alternative is computed and ranked based on the objective attributes. Probability distributions can be associated with each attribute to reflect the expectations of decision makers. The power of decision theory is that it provides a systematic way to consider tradeoffs among attributes, which can be used to make decisions.

2. INFORMATION SECURITY RELATED DECISIONS

We can define Information Security technologies selection problem as *"the task of selecting the best set of security countermeasures for an information system"*.

The biggest challenge in this respect is to quantify the benefits of security countermeasures and the consequences of successful computer-based attacks. The degree to which a security countermeasure stops an attack (or deals with the consequences of it) determines its usefulness.

Making decisions during the development or updating the information system security architecture is one of the most challenging tasks for a security analyst.

Specifically, it is a flexible, systematic and repeatable process that prioritizes threats and helps select countermeasures to clarify the best investments for the organization's objectives.

The process of taking decisions regarding which security technology to use has a certain degree of uncertainty, given by three key elements:

- the attack itself, because most security designers have little data concerning the frequency of attacks and which attacks are more likely to occur (that determines the appropriate selection of countermeasures);
- the outcome of a successful attack, because once the computer system is breached there are many potential action paths an attacker could follow;
- the benefit from countermeasures, because the effectiveness of a countermeasure in protecting or detecting an attack can only be estimated.

Another source of uncertainty came from the fact the security designer/administrator must also balance multiple objectives when selecting security technologies. Consequences of successful attacks must be balanced with:

- performance constraints;
- budget limitations;
- other design considerations.

This will add complexity to the application of decision theory techniques on information security related decisions. The selection process of the appropriate security technology could take advantage of the power of decision theory techniques, because possible outcomes from successful attacks (i.e. productivity loss) can be viewed as objectives. After the levels of outcomes are determined, reasonable alternatives can be generated from probability distributions.

3. IMPROVING DECISIONS BY USING DECISION THEORY TECHNIQUES

The application of decision theory techniques in the software design decision process improvement may result in an improved decision, but with a degree of uncertainty. If it does not rely on sufficient information (expertise), it could easily lead to a poor decision. For example, the information security technology selection process relies on countermeasure expertise to improve the selection of countermeasures. This expertise (the risk analysis consisting of the likelihood of attacks and their potential outcomes) is used to realistically represent the impact of a countermeasure to a specific computer-based attack. After the risk analysis is done, an outcome distribution for each relevant attack results. When a countermeasure is used, the outcome distribution graphs might be different. For example, when anti-virus software is used, the frequency of successful virus attacks is reduced or the amount of revenue lost is reduced. The outcome distribution graphs might shift when an anti-virus technology is used (Fig. 1, 2).

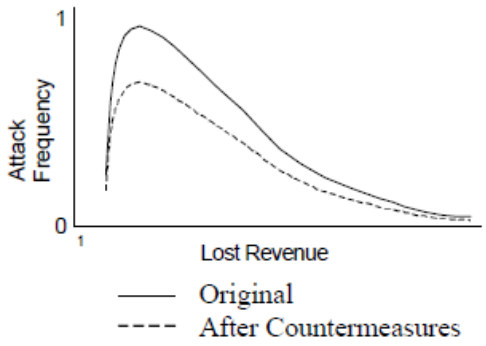

Fig. 1 Virus attacks - frequency mitigation

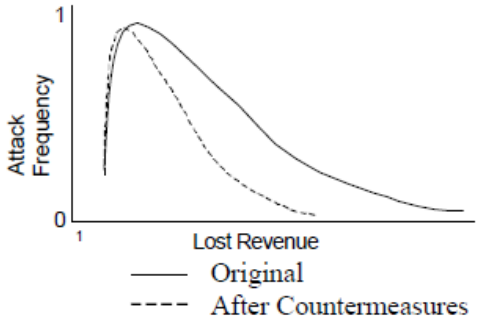

Fig. 2 Virus attacks - outcome mitigation

Generally speaking, if expertise is available, then decision theory techniques can be used to improve security design decisions. In order to use statistically analyzed attack frequencies information, threat data must be available.

In our days, one of the greatest challenges is to acquire reliable countermeasure expertise. Because this could affect their prestige, very few organizations report security incidents, and there is little reliable statistical data about attack frequencies. For example, even if 49% of the companies that took part in a survey said that their primary security concern was data leakage (such as employee or customer information), and 29% of them were in fact confronted with the problem in 2007, only 11% actually reported the incidents [4].

Another important consideration in the application of decision theory to design problems is the level and detail of the information used in the decision process. If the information is too detailed, it will result in a large amount of data that are extremely difficult to be reassembled into meaningful recommendations. There are more than 18 different types of computer-based attacks (from Denial-of-service (DoS) Attacks to TCP SYN or TCP ACK Flood Attack) [5], over 40 security countermeasures [6], and at least half a dozen possible outcomes [7].

Each class of outcomes may be associated with different attributes. A distribution curve may be also established for each outcome. For example, for each outcome of a computer-based attack three values could be provided: low, high, and expected.

In order to take information security related decision by using decision theory, an

important step is to determine a way to reduce the possible combinations of attacks, outcomes and countermeasures. The most efficient way to reduce the possible combinations is to focus on the most important. This technique eliminates aspects of the decision process that do not contribute significantly to the final selection. In this respect, we must focus on information about the top 3-4 outcomes and also on the countermeasures that provide a moderate level of protection.

In conclusion, the essence of the problem is to combine the information regarding the attack with mitigation information, so that countermeasures can be selected. There will be lots of different outcome distributions, each distribution adjusted to several countermeasures that are also weighted based on their overall contribution to outcomes mitigation.

4. CONCLUSION

So far I have described a few issues that must be taken into consideration when trying to apply decision theory techniques to information security decision problems.

Decision theory can be a significant tool in information security practice. However, it typically involves issues like *uncertainty, complexity, high-risk consequences, multiple alternatives* (each with its own set of uncertainties and consequences).

With these difficulties in mind, the best way to make a complex decision is to use an effective process. Clear processes usually lead to consistent, high-quality results, and they can improve the quality of our information security related decisions.

REFERENCES

1. Butler S., Chalasani, P., Jha S., Shaw M., *The Potential of Portfolio Analysis in Guiding Software Decisions*, June 2000;
2. Doyle, J., Thomason R. H., *Background to Qualitative Decision Theory*, 1999;
3. *** *Oxford English Dictionary*, Oxford Corpus, 2009;
4. http://news.softpedia.com/news/Only-11-of-Security-Incidents-are-Reported-91335.shtml;
5. http://www.unp.co.in/f140/types-of-attacks-63305/;
6. Norman, Th.L., *Risk Analysis and Security Countermeasure Selection*, CRP Press, 2009;
7. Jürgenson, A., Willemson J., *Computing Exact Outcomes of Multi-parameter Attack Trees*, Springer Berlin / Heidelberg, 2008.