Behavior Risk: the Indefinite Aspect at the Stuxnet Attack?

Wolfgang Boehmer
Technische Universität Darmstadt
Email: wboehmer@cdc.informatik.tu-darmstadt.de

***Abstract*—In 2009, the Stuxnet virus was first observed in the wild and was considered as a novelty among the viruses. The Stuxnet virus is classified as a *game changer* and so we denote it *causa Stuxnet*. For the critical infrastructures, it was inconceivable, that a specific virus has been developed for industrial systems. Besides this novelty, the infection path was different from the typical patterns of attack and infection in the field of office communication. In this article, we focus only on the infection path of Stuxnet. We use the Game Theory to analyze the infection path. We found that the infection path is one game in a complex multi-layer game. As a result, based on a Nash equilibrium, a cooperative solution is proposed to arm the existing IT security concepts against such infections. Nevertheless, the existing IT security concepts are not useless, but the behavioral risk has to be taken into account.**

***Index Terms*—Event risks; behavioral risks; trust/investor game; IT security concept; industrial control system**

I. Introduction

In the past, the focus was placed on attacks and countermeasures on purely IT systems in the business community or, better, in the field of office communication. However, it had also previously been attacks on industrial facilities, such as D. Denning analyzed in the article [1]. In their article, a comprehensive analysis and categorization of attacks on industrial facilities has been done. The Stuxnet virus was called a *game changer* in their article,

In 2009, as N. Falliere et. al. from Symantec wrote [2], the Stuxnet virus was first observed in the wild and was considered as a novelty among the viruses. For the critical infrastructures, it was hitherto unthinkable that a specific virus has been developed for industrial control systems. Besides this novelty, the route of infection was different from the typical patterns of attack and infection in the field of office communication.

Typically, an attack on IT systems is analyzed and described by so-called attack trees. Attack trees are a good way to detect possible attacks or mimic attack routes in advance.

In 1994, Edward Amoroso's book Fundamentals of Computer Security Technology described threat trees, a tree structure very similar to attack trees. By the late 1990s, papers were beginning to appear describing the attack tree analysis process in some detail. For instance, in the 1998 paper Toward a Secure System Engineering Methodology [3] the authors describe a mature, attack tree-based approach to analyzing risk. One of the first who dealt systematically with this type of technical attacks was Bruce Schneier. In 1999, he published the idea of *attack trees*, which were directed towards technical systems [4]. The idea was taken further and improved by the company Amenaza Tech. Ltd.

Game theory considered – very roughly speaking – conflict situations between one or more Individuums. Fiona Carmichael [5] wrote in her book (2005) on page 3: the idea of Game Theory is to analyze situations where two or more Individuums (or institutions) the outcome from action by one of them depends not only on the particular action taken by the individuums but also on the action taken by the other (or others). In these circumstances the plans or strategies of the individual concerned will be dependent on expectations about what the other is doing. Thus, Individuums in these kinds of situations are not making decisions in isolation, instead their decisions making is interdependently related.

In essence, game theory is primarily not used for the analysis of attacks [5] page 4. However, a certain relationship exists between an attack tree and game theory in a particular form of play (zero-sum game) of two players. In the article by Kordy et al. [6] it was shown in a comparison that an attack-defense tree and a strategic zero-sum game of two players to their binary information are equivalent in the extensive form. The extensive form denotes a game tree. In this context, a strategic game is a scenario or situation where, for two or more Individuums, their choice or behavior has an impact on the other (or others). A Player is participant in a strategic game and a strategy is a player's plan of action for the game. If only one player exist in a game, then this game is called a game against nature, which is generally called decision theory (rather than game theory). We will come back to this issue later on.

Another type of attack has been perfected, e.g., by Kevin D. Mitnick [7]. This type is classified as a social engineering attack and has been discussed multiple times in the literature.

From attack-trees, insights are gained and then countermeasures are designed to be armed for future attacks. However, the mere development of measures is not very helpful for an organization. These measures must be incorporated into a security concept and coordinated with other measures.

Security concepts have always been established for safeguarding companies and industrial plants. It can be shown that a good security concept cannot be reduced to a simple list of measures. However, the measures listed in the security concept must always result from a procedure or methodology. In the literature, there are numerous articles on the development of security concepts. But the objectives in the security

 ISBN: 978-1-61208-298-1

concepts discussed in the literature are often very different. This paper addresses three protection goals, pursued from different perspectives. However, security concepts based on the standards (e.g. ISO 27001) address three main protection targets (availability, confidentiality, integrity).

The relationship between security objective, systems and the security concept can be produced with the following definition:

Def. 1: A security concept includes measures $\mathfrak{M}$ to ensure the security objectives of confidentiality, availability and integrity of a system (ψ) aligned to a predefined level.

The three protection goals (*confidentiality, availability and integrity*) behave as random variables in a probability space and can counteract the risk of protection violation or deviation of the predefined level through appropriate security concepts. The *predefined level* is directly correlated with the risk appetite of a company (see Figure 1). The reader should note that the risk appetite must be defined for each of the protection goals. The risk appetite levels are set by the management for different activities or parts of the organization.

However, the different types of risks that may lead to a protection violation must be analyzed separately, because risks can be divided into state risks, behavioral risks, and hybrid risks (see Figure 2). Furthermore, not only the types of risks, but also the underlying systems ($\psi \in \Psi$) are to be differentiated in a security concept.

In general, for the term risk in this paper, we follow the definition from the Circular 15/2009: Minimum Requirements for Risk Management (MaRisk) issued by the Federal Financial Supervisory Authority (BaFin).

Def. 2: Risk is understood as the possibility of not reaching an explicitly formulated or implicitly defined objective. All risks identified by the management present a lasting negative impact on the economic, financial position or results of the company may have to be considered as much as possible.

The research contribution results from the analysis of the infection path of the Stuxnet virus [8] and combats it with methods of Game Theory. The result evident from the analysis is that only cooperative behavior between software manufactures for SCADA systems (e.g. Siemens, ABB, AREVA) and the software users (operator of the power plant) is sufficient for a Nash equilibrium. For a Nash equilibrium it is characteristic that actors cannot obtain a better position, if they deviate from their strategy. The cooperation (Nash equilibrium) will cause the software manufacturer for the SCADA systems, as a first step, to generate a signature in advance using the software and provide the signature to the power plant operator in advance, before any service technician arrives at the power plant. The signature makes it possible to uncover an evolution of the software (virus infection) in the IT equipment of service technicians as a second step with only a little effort. This constructive solution to this type of behavioral risk is already in the implementation stage at one power supplier in Germany.

It is also clear from the game analysis that the (current) practice of disinfecting the infected systems retroactively only represents the second best solution, because it is not ruled out that modifications of the Stuxnet virus could infect the sensitive control systems of industrial plants in the future. Moreover, conventional virus scanners in SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS) Systems are generally hardly used. This preventive solution then enables, if the software manufacturer for SCADA systems cooperates, future modifications of the Stuxnet virus or a variant of a Stuxnet virus to be uncovered effectively.

The rest of the article is divided into four sections. In the next section, the underlying model equations are explained. In the third section, case studies are discussed for the different types of risks; for example, hybrid risk analysis (see Fig. 2, no. (2)). In better security concepts, this approach can be found in the development of security measures. According to, e.g., the ISO 27001 and ISO 27005, a scenario analysis is required to create a security concept (*statement of applicability*). Subsequently, behavioral risks are discussed on the example of the Stuxnet virus. Such risks are based only on the misbehavior of Individuums. These are marked with the no. 3 in Fig. 2. With the Game Theory, the Causa Stuxnet is analyzed. Here, the route of infection is analyzed as a partial game in a complex multi-layered game. A Nash equilibrium is achieved, the knowledge of which can eliminate general routes of infection preemptively. However, measures derived from the analysis of behavioral risks have rarely been included in the security concepts. Also, methods of Game Theory, which consider behavioral risks, have not previously been included in any standard.

In the fourth section, we discuss the related work and in the last section, there is a brief summary and an outlook on further research. This article is an extended version of [9].

II. The model

In essence, we will deal in this article with hybrid risks described in Figure 2, number (2) and the behavioral risks, number (3) for analyzing the Stuxnet virus.

An IT/Inf.-Security concept reflects the complementary relationship between security and risk for a system $\psi \in \Psi$. This complementary relationship is that the lower the security ($\mathcal{S}ec$), the higher the risk ($\mathcal{R}$) of a violation for a system ψ of the three control objectives (*cf.* Definition 1); therefore risk and security are negatively correlated.

Figure 1 illustrates this relationship qualitatively for the protection goal availability.

To illustrate this negative correlation, risk and security *simplified* are normalized by the interval $[0, 1]$, with

$$\mathcal{S}ec = 1 - \mathcal{R}. \tag{1}$$

The risk ($\mathcal{R}$) in the sense of operational risk is obtained as the probability (Pr) of an event (E) on the impact on a system, e.g., on an open system (ψ_1), as a value chain with a negative outcome ($Loss, L$) in monetary units (euro), in $\mathbb{R}^+$ [10]. This relationship can be expressed as follows

$$\mathcal{R} = Pr_E \times L\ [\mathbb{R}^+]. \tag{2}$$

 ISBN: 978-1-61208-298-1

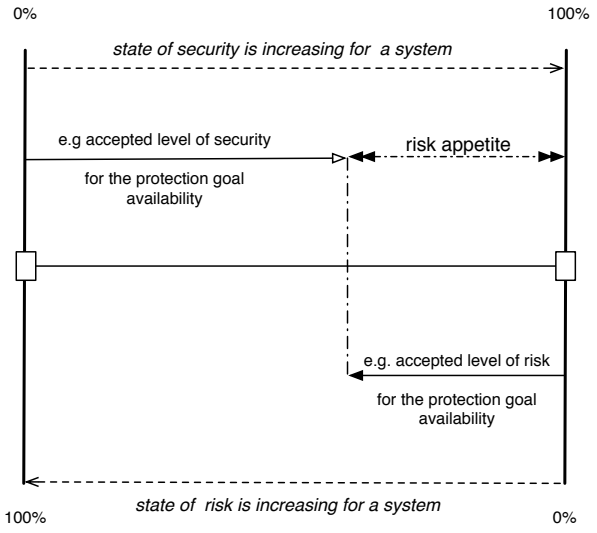

Figure 1: Security versus risk

At first glance, these two definitions (Eq. 1, Eq. 2) do not seem to attain anything. However, if the risk ($\mathcal{R}$) is regarded as a random variable in a probability space, then this is the missing link in the chain of reasoning. For a random variable let $X : \Omega \to \mathbb{R}$ be a measurable function in a probability space defined by the triple $\Omega, \mathcal{A}(\Omega), Pr$, where $\mathcal{A}$ a σ-algebra, is a certain subset in the probability space. By inserting (2) in (1) we produce (3)

$$\mathcal{S}ec = 1 - \Big(Pr_E \times L\Big). \tag{3}$$

Thus, security can be measured indirectly by measuring the risk.

A quantification of a random variable (X) is performed formally by assigning a value (x) for a range of values (W) using a certain event (E). For the random variable (X) the image of a discrete probability space then applies to the discrete result set $\Omega = \{\omega_1, \omega_2, ..., \}$ such that $X : \Omega \to \mathbb{R}$. For discrete random variables for the discrete value range that is interpreted in the context of operational risk as a monetary loss (L) (*cf. Def. 2*)

$$L_X = W_X := X(\Omega) = \{x \in \mathbb{R} \mid \exists\ \omega \in \Omega \text{ mit } X(\omega) = x\}. \tag{4}$$

In the field of operational risks, the probability (Pr) with the random variable (X) which may accept certain values (W_X) and losses (L_X) is of interest. For any event (E) with $1 \leq i \leq n$ and $x_i \in \mathbb{N}$:

$$E_i := \{\omega \in \Omega \mid X(\Omega) = x_i\} = Pr[\{\omega \in \Omega \mid X(\omega) = x_i\}]. \tag{5}$$

Since, in this context, only numerical random variables are considered, each random variable can be assigned to two real functions. We assign any real number (x) the probability that the random variable takes that value or a maximum of such a great value. Then the function f_X with

$$f_X : \mathbb{R} \to [0,1],\ x \mapsto Pr[X = x] \tag{6}$$

is called a discrete (exogenous) density (function) of X. Furthermore, a distribution function (F_X) is defined with

$$F_X : \mathbb{R} \to [0,1],\ x \mapsto Pr[X \leq x] \sum_{x \in L_x\,:\, x' \leq x} Pr[X = x']. \tag{7}$$

The value (W_X) can have both positive and negative values, depending on which is discussed in the context, the density or the distribution of values.

Now if the confidentiality (*Conf*) and integrity (*Int*) are seen as discrete sets of random variables in a probability space, it is possible to describe these two security objectives (8), (9) as the sets of a given indicator function.

Due to the binary property of the two subsets (*Int*, *Conf*), with $Int \subseteq X$ and $Conf \subseteq X$, for every x on $[0,1]$, which for $x \in X$ is 1 when $x \in Int$ or $x \in Conf$, otherwise 0. It is

$$X \to [0,1],\ x \mapsto \begin{cases} 1, & \text{if } x \in Int \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

Also (8) can be used for the random variable *Conf*, if we used *Conf* instead *Int* in (8), then we can derive (9)

$$X \to [0,1],\ x \mapsto \begin{cases} 1, & \text{if } x \in Conf \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

Thus, the binary properties of the two discrete random variables are formally described. In this paper we write $\mathbf{1}_{Int}$ to the discrete indicator function, integrity, and $\mathbf{1}_{Conf}$ to use the discrete indicator function confidentiality.

It is different with the availability (Av), which can be formally described as a *complete partial order, CPO*. With a CPO we can easily find intermediate values in the interval [0,1] in $\mathbb{R}^+$ which are the subject of a binary relation. A binary relation over the set (Av) availability of all elements is a partial order, if $a, b \in$ Av and $a \leq b$ holds. We use the following notation in this paper

$$(\text{Av} \leq) \mapsto [a \leq b] \text{ or short and sweet } (\text{Av} \leq). \tag{10}$$

Finally, a security concept ($\mathcal{S}ecCon$ (11)) is the illustration by the measures ($\mathcal{N}_{Ma}$) and with (8), (9) and (10) and the map to the method $\mathfrak{M}$ (*cf. Def. 1*)

$$\mathcal{S}ecCon\,(|\mathcal{N}_{Ma}|) := \mathfrak{M}\Big((\text{Av} \leq), \mathbf{1}_{\text{Int}}, \mathbf{1}_{\text{Conf}}\Big) \mapsto \mathbf{\Psi} \tag{11}$$

for a system $\psi \in \Psi$.

However, the security concepts are not only the power of the measures ($|\mathcal{N}_{Ma}|$) to reduce the risk of a possible injury of the three security objectives for a system, but it is necessary that the measures $\mathcal{N}_{Ma}$ have been developed using a methodology. This methodology is the function $\mathfrak{M}$ in (11). The function $\mathfrak{M}$ must be able to map the different risk types according to the underlying (open, closed, isolated) systems. Thus, the following definition is formulated for the measures.

Def. 3: The identified measures ($\mathcal{N}_{Ma}$), included in a security concept, based on the methodology ($\mathfrak{M}$).

The idea of the open (ψ_1), closed (ψ_2) and isolated systems (ψ_3) has been borrowed from thermodynamics, but can be

easily transferred to computer science and business, too [11], [12].

A broad representation of different types of risks, relating to systems all the way up to Individuums in Figure 2, has been marked by the no. (1) - (3), illustrated by T. Alpcan [13] and is the brainchild of N. Bambos.

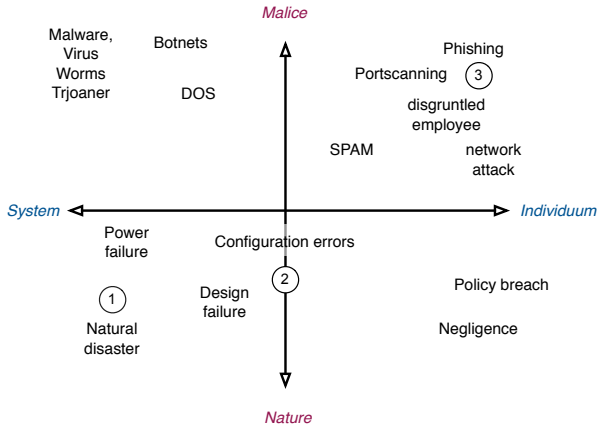

Figure 2: Different types of states and risks, according to N. Bambos [13]

Mark no. (1) denotes the *event risk*, for example, and this risk can be related to closed and / or isolated systems. No. (3), the purely *behavioral risks*, relates primarily to Individuums, as does the *hybrid risk* indicated by the no. (2). These are often considered using a scenario analysis. Hybrid risks are common in open systems.

After the different systems and risks are illustrated in Figure 2, the question becomes how to deal with the risks. It is not mandatory that every identified risk must be eliminated.

How to deal with risks is important for an organization. Risks generally could be reduced, avoided, transferred, accepted or eliminated (see Figure 3).

Economic aspects alone, and not technical aspects, are crucial in dealing with the identified risks. The different treatment methods are described below with the numbers 1 to 4. Several decisions have to be made regarding which of the risks can be avoided, reduced, transferred, or even accepted, see Figure 3.

The following are the decisions to be taken.

1) $R_1 = \sum_{i=1}^{n} R_{avoid}$, number of risks that can be avoided
2) $R_2 = \sum_{i=1}^{n} = R_{mitigate}$, number of risks that can be mitigated
3) $R_3 = \sum_{i=1}^{n} = R_{shift}$, number of risks that can be transferred
4) $R_4 = \sum_{i=1}^{n} = R_{taking}$, number of risks that can be accepted

Illustrated in Figure 3 are the upcoming decisions and these decisions are designated as the security posture. The ratio of overall risk and the various possibilities for reducing operational risks is shown.

The orientation of the possibility of a reduction of the risk depends on the cost. It is cheaper for the company to insure certain risks than to invest in adequate measures.

Companies may decide the quantification of risks according to their budget and their business objectives and their risk behavior (level of risk appetite). This turns risk management into cost management.

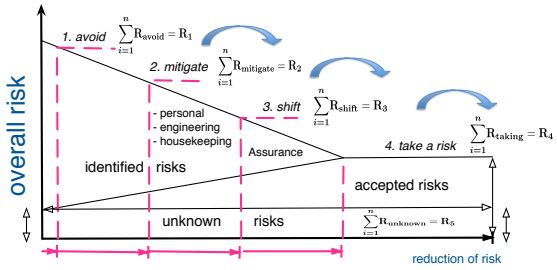

Figure 3: Aspects of risk treatment

It should be noted that in spite of a risk analysis unknown risks still exist. The goal of any risk analysis must, therefore, be to try to reduce the number of unknown risks $R_5 = \sum_{i=1}^{n} = R_{unknown}$ as much as possible. The unknown risks are not negligible, if we follow the groundbreaking book *The Black Swan* from N. Taleb [14]. He argues that the Gaussian bell curve can show probabilities, but the case of a devastating security event (Black Swan) will be an outlier to the bell curve, see Figure 4, and produce a worst case scenario.

III. Case study

Within this section, the next subsection (*A*) discusses hybrid risks from the Game Theory perspective. We argue that it is a game against nature. The second (*B*) and third (*C*) subsection discuss the Causa Stuxnet and analyze it using the trust game of the Game Theory. The solution achieved through a Nash equilibrium of the game analysis of the trust game used is presented in the fourth subsection (*D*).

A. Analyzing hybrid risks: a game against nature

The risks denoted by no. (2) in Figure 2 arise from both state risk and behavior risks. For this type of risk analysis, statistical methods and behavioral effects are both considered. This hybrid risk could be analyzed by the risk scenario technique going back to the three-point estimation method [15]. This three-point estimation method was used for the analysis of hybrid risks in the area of power plants and specifically in the field of SCADA systems. It was studied experimentally at 29 power plants, as one can read in [16]. Based on this analysis, a security concept for the SCADA system has been created.

Generally, a scenario is a possible event E_i, expressed formally in (5). It is the attribution of a certain value of a random variable ($X(\omega) = x_i$). In this context, an event E_i is understood as a risk event ($Rsz\varsigma$). Using the three-point (risk) estimate method, different loss probabilities (best case (BC), most likely case (mc), worst case (wc), (see Figure 4) of a risk event are identified. It relates the risk scenarios to the above protection objectives (Av $\leq$), $\mathbf{1}_{\mathrm{Int}}, \mathbf{1}_{\mathrm{Conf}}$. The risk of incident is related to an asset. The assumption is, an asset incorporates both a resource and a role that interact in a business process

[17]. (12) defines a risk event (RSz) with $\varsigma = \{bc, mc, wc\}$ as a possible result of variations of the risk event.

$$X(\omega) = Rsz_{\varsigma} :=$$
$$\begin{cases} if\, \varsigma = bc \,|\, (x_{bc} = x_{mc}) \wedge Pr[X(\omega) = x_{bc}] \rightarrow \text{best case} \\ if\, \varsigma = mc \,|\, (x_{bc} > x_{mc}) \wedge Pr[X(\omega) = x_{mc}] \rightarrow \text{most likley case} \\ if\, \varsigma = wc \,|\, (x_{wc} \gg x_{bc} \wedge x_{mc}) \wedge Pr[X(\omega) = x_{mc}] \rightarrow \text{worst case} \end{cases} \quad (12)$$

The possible result types (Rsz_{ς}) of a risk event were estimated by experts in workshops. An illustration of the stochastic process of (12) is presented in Fig. 4. Furthermore, a distribution (Gaussian curve) using three points of the estimates was created by a General Pareto Distribution [16]. This line shows the distribution of possible losses to absorb. In this case, the certain event $Pr = 1$ is no longer a stochastic event. In terms of operational risks, only the grey shaded area of interest is normally referred to as a downside risk with $X(\omega) = \{1, -\infty\}$. Assuming a time interval (t_1, t_3) in the probability space (Pr), the expected loss (VaR) can be determined for a confidence interval (α) using (13), which provides a lower bound

$$VaR_{\alpha} := min\{x \,|\, (Pr[X \leq x] > \alpha)\}. \quad (13)$$

The VaR is not a coherent risk measure, as demonstrated by

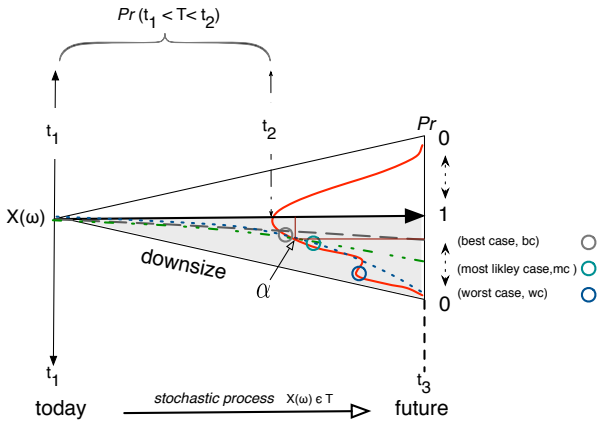

Figure 4: Risk corridor for the time interval (T)

Artzner [18], but, for this risk estimation using the VaR, the error made in this case is very small, because power plants use the standard BS25999 for the very rare risk with a catastrophic outcome [16].

After analyzing the risks created by the set $\mathcal{N}_{\mathcal{R}}$, the elements $\mathcal{N}_{\mathcal{R}} = \{r_1^{Rsz_{\varsigma}}, ..., r_{Rsz_{\varsigma}}^{Rsz_{\varsigma}}\}$ have the cardinality $|\mathcal{N}_{\mathcal{R}}|$. These can be addressed through appropriate measures. There are different measures possible. On the one hand, actions may be identified, when only one risk scenario works against one risk; on the other hand, other measures can be identified that counteract more than one risk. In general, measures are defined with the set $\mathcal{N}_{Ma}$ and the elements $\mathcal{N}_{Ma} = \{m_1^{Ma}, ..., m_{Ma}^{Ma}\}$. The cardinality is given with $|\mathcal{N}_{Ma}|$. These measures, based on the three security objectives (8), (9, (10), create the security concept according to (11).

Through risk analysis, using the risk scenario technology, which refers to assets in a process (business process), both a pure state risk and a behavioral risk are included, because in the scenarios unconscious and conscious actions (misuse) of an employee and its impact on the business process are considered.

From the perspective of Game Theory, this is still a game against nature. This is a decision problem $\mathcal{D}$ in strategic form under risk. They are making decisions for actions involving the different probabilities (Pr) in the probability space given for the environment states $z \in Z$. However, the classical decision rules (MaxiMin rule, MaxiMax rule, Laplace's rule, etc.) are not used as strategies in this paper. The decision maker who is responsible for developing a security concept (see (11)) will choose a strategy s from the set of all strategies S, to select those measures to (avoid, decrease, transfer, eliminate, accept) a risk event (see (12)). Five different strategies, $\tilde{s}_1, ..., \tilde{s}_5$, can be used

$\tilde{s}_1$ = Avoiding the outcome of the risk with a measure.
$\tilde{s}_2$ = Decreasing the outcome of the risk with a measure.
$\tilde{s}_3$ = Transferring the risk to an insurance company.
$\tilde{s}_4$ = Eliminating the outcome of a risk with a measure.
$\tilde{s}_5$ = Accept the risk.

Not all of the strategies listed above for $\tilde{s}$ are applied, because each measure requires certain costs ($\mathcal{U}$). In classical Game Theory, $u \in \mathcal{U}$ is often understood as the pay-off (function or utility function). We described $\mathcal{U}$ with the amount of the costs of all measures and u is a cost function, the decision problem $\mathcal{D}$ is a strategic decision

$$\mathcal{D} = \left(\tilde{S}, Z, \varsigma, \mathcal{U}, u\right) \quad (14)$$

under risk. (ς) represents a probability distribution on Z, the environmental conditions. The creation of the decision space (14) can be represented as follows

$$\tilde{S} \times Z \mapsto \mathcal{U}(\varsigma). \quad (15)$$

A decision matrix can be derived from the decision space, as illustrated in Table I. The decision maker (security officer) has to make a decision based on the decision matrix of Table I that included the strategies, the environmental conditions and the measures or the costs of the activities related to the risk scenario ($\varsigma = \{bc, mc, wc\}$), which should be provided in the security concept (see (11)). The decision matrix is shown above in Table I. Depending on the decision process by the security officer (see (14) and Table I) this will meet the security concept regarding the security objectives of confidentiality (9), availability (10) and integrity (8) of the identified risks with appropriate measures. With the consideration of the hybrid risks posed by the scenario technology (see (12)), consolidated findings are gained to complete the security concept. However, analysis of the hybrid risks with the scenario technology is not ideal for analyzing the Stuxnet virus.

 ISBN: 978-1-61208-298-1

Table I: CHANCE MOVES AGAINST NATURE

		nature / environment		
		z_1	z_2	z_3
security officer	$\tilde{s}_1$	u($\tilde{s}_1, bc$)	u($\tilde{s}_1, mc$)	u($\tilde{s}_1, wc$)
	$\tilde{s}_2$	u($\tilde{s}_1, bc$)	u($\tilde{s}_1, mc$)	u($\tilde{s}_1, wc$)
	$\tilde{s}_3$	u($\tilde{s}_1, bc$)	u($\tilde{s}_1, mc$)	u($\tilde{s}_1, wc$)
	$\tilde{s}_4$	u($\tilde{s}_1, bc$)	u($\tilde{s}_1, mc$)	u($\tilde{s}_1, wc$)
	$\tilde{s}_5$	u($\tilde{s}_1, bc$)	u($\tilde{s}_1, mc$)	u($\tilde{s}_1, wc$)

There is no analysis of the behavior (actions) of employees or other service providers. This has led to the conclusion that the existing security concepts in the power plants have a gap, and that the infection of an authorized service technician – *albeit unwittingly* – is possible.

In the next subsection, we analyze the infection of the Stuxnet virus to compromise the protection target ($\mathbf{1}_{Int}$) with the trust game of the Game Theory.

B. Game analysis before the Stuxnet virus arose

Pure behavioral risks (*cf.* no. (3) in Fig. 2), in contrast to pure state risks (*cf.* no. (1) in Figure 2), could not be analyzed with statistical methods.

Therefore, we consider the Causa Stuxnet and the behavior between the service technician and the staff (security officer) causing the infection using the trust game (*note:* The trust game is a modified dictator game). from Game Theory. As one of the first, [19] deals with the trust game in reference to a social environment. Typically, for the trust game, there is a different trust relationship (imbalance) between the two players.

These behavioral risks are the types of decisions (strategies) of the player (service technician / security officer) that caused the infection.

Stuxnet — *The infection of Stuxnet virus, in the area of critical infrastructure (SCADA) systems, has not been an attack. The virus was transferred from a service technician equipped with the necessary permissions unconsciously, using an infected USB stick. The virus has arrived without the knowledge of the service technician on to his USB stick.*

Subsequently we analyze this critical incident with the Game Theory to derive a solution from the chance moves of the game. This solution leads into a cooperation of the software manufacturer with the power plant operator of the SCADA systems.

In the analysis, we use a slightly modified version of the trust game, because it cannot be ruled out that tomorrow another service technician from another company with a similar virus attends to the power plant.

Pure behavioral risks, which are designed to trust, could be analyzed with the trust game [20]. We analyze the chance moves of both players. Each player reacts to the behavior of the other player. One of the basic ideas of Game Theory is to study, analyze and evaluate the reciprocal response pattern of the players. Reciprocal reaction patterns, so-called pay-offs, are determined by distribution rules and play a significant role and in turn, depend on the incentives. It depends on the distribution rules of legal, contractual, historical or political power relations. Thus, a major difference is the probability models, as these know no incentive mechanisms.

Table II: CHANCE MOVES BEFORE THE STUXNET

		σ_2	
		infect	not infect
σ_1	trust	1, 0	3,3
	don't trust	1, 0	2, 2

Game analysis of virus Stuxnet pursues a causal chain of thought. First the chain of thought which was taken before the Stuxnet virus (*cf.* Table II and Fig. 5) is followed and another chain of thought follows after the onset of Stuxnet virus (*cf.* Fig. 6 and Table IV). The concerned chance moves are performed as a *one-shot game*. Thought chains are typically illustrated in the form of branching trees, to represent the individual moves. Another name for the game tree is the *extensive form* as is noted in [5].

Formally, a strategy game Γ consists of a triple. With Σ, the set of players σ is defined, it is $\sigma \in \Sigma$. With S the set of strategies is described and we have $s \in S$. This means that a game can be characterized as follows

$$\Gamma = \{\Sigma, S, \mathcal{U}, u\}. \tag{16}$$

$\mathcal{U}$ has the same intention as in (14). In the analysis of the Stuxnet virus, are two players (σ_1, σ_2) in the space of action $A = \Sigma \times S$. The action space (*cf.* Fig. 5) for player σ_1 ist $A^{\sigma_1} = \{t, nt\}$ and $A^{\sigma_2} = \{i, ni\}$ applies to player σ_2. In this analysis, pure strategies are postulated; therefore, a single pure strategy is expressed in s. Strategies include decision rules that the player implement to some benefit (u) to obtain a pay-off. In general, the trust game can be expressed as

$$\Sigma \times S \mapsto \mathcal{U}(u). \tag{17}$$

Compared with (17), in (15) the players S now are in the place of the environmental states Z.

Typically, games in the form of a bi-matrix, called the simultaneous logical reasoning circular, are presented in a sequential chain of thought the game tree. The Bi-Matrix in the trust game between the service technician (player σ_2) and the security officer (player σ_1) has been formulated in Table II. In this situation, this game represents the situation before the virus Stuxnet arrived. Before Causa Stuxnet, there was *no* distrust due to player σ_2 (service technician) and, consequently, the chance moves (1, 3, 6) in Fig. 5 are typical chance moves. To date, no incidents justified distrust of players σ_1 (security officer) toward players σ_2. Also, it was inconceivable to date, that a special virus [8] would be written which is used in an area with property software for the small *Program* Logic Controller (PLC), *cf.* with the Step 7 software. However, for a suspicious player σ_1 (security officer), the move (1, 2, 4) of Fig. 5 is also conceivable, but impossible because thus far virus infections were not encountered and therefore without

 ISBN: 978-1-61208-298-1

consequence. It also ruled out the usual (normal) route of infection in the power plant, due to the systematic separation of networks and hermetic sealing of the internal systems to the Internet and intranet. Thus, the combination *(do not trust / not infected)* is a Nash equilibrium. In a Nash equilibrium, none of the two player could obtain a better position through a change in their attitude.

In this respect, the cost function u (not much effort, because there are no security policies to follow) is greatest for the two players when combining *(trust / not infected)* in Table II. It leads also to a Nash equilibrium, since neither player can achieve a better position by changing moves.

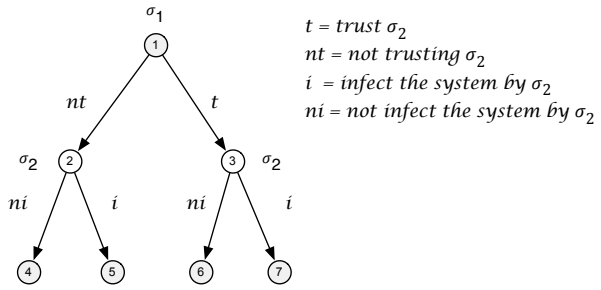

Figure 5: Change moves in a game tree before the Stuxnet virus arose

After the Stuxnet virus arose, this event changed the trust relationship drastically between player σ_1 (security officer) and player σ_2 (service technician). This change in position of trust is analyzed in the next subsection.

C. Game analysis after the Stuxnet virus arose

After the Stuxnet arose, the perspective of player σ_1 (security officer) has changed considerably. He does not know whether or not the service technician σ_2 brings an infected USB stick. The result is the typical trust game (*note:* This uncertainty could also be analyzed with a mixed strategy, a probability distribution over the pure strategy. However, in this investigation we use only pure strategies). situation because an imbalance of trust has occurred.

After the Stuxnet virus, the security officer (σ_1) could continue to trust the service technician (σ_2) or install comprehensive security policies. The behavior of σ_1 *trust* (t) is illustrated in the extensive form (see Fig. 6) in the right branch (1, 3). The player σ_2 then has the opportunity to infect the system (1, 3, 7) or not (1, 3, 6) with the result that σ_1 must check the system (c, nc) or possibly report a virus (r, n).

The left branch illustrates, on the other hand, the behavior strategy of σ_1 for *do not trust* (nt), therefore the game play (1, 2).

Security policies always increase the restrictions and the workload involved for everyone (σ_1, σ_2). Furthermore, it is evident that, when security policies are perceived as too restrictive by the players, they bypass (σ_1, σ_2) all of the policies. For the security policy for the USB stick, this leads to (bc, nbc). This realistic situation is illustrated by the extensive form in Fig. 6. If the security policies are not undermined, there is the game branch (1, 2, 5, 10). However, the branch with restrictions, imposed by the security policy, increased the workload.

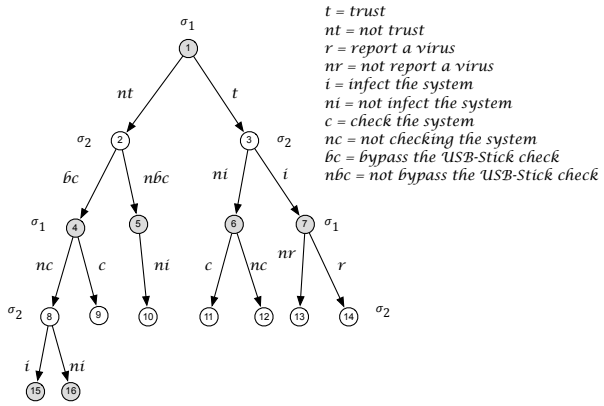

Figure 6: Change moves in a game tree after the Stuxnet virus arose

The game branch (1, 2, 4) represents the case where the service technician (σ_2) bypasses the security policy unnoticed and the security officer (σ_1), driven by their distrust, reviews the system for viruses (1, 2, 4, 9). This distrust does, however, again cause an increased effort for σ_1. Otherwise, the strategy (1, 2, 4, 8) is followed by σ_1 and a significant degree of uncertainty remains about the state of the system. It may be now, that the game play (1, 2, 4, 8, 16), or in the negative case, an infection occurs (1, 2, 4, 8, 15). As a result it can be stated that no Nash equilibrium can be achieved.

The game tree of Fig. 6 allows us to derive the bi-matrix of the Table IV with the pay-off Table III and the key parameters for the service technician (σ_2) and security officer (σ_1). In the following statements, the key parameters for the service technician (σ_2) are listed.

- G_S Benefit for successful service
- G_B Benefit to following the security policies (increasing of reputation)
- K_S Investment given by checking the security controls
- K_R Penalty for ignoring the security policies
- K_U Penalty for procedure to disinfect the system

For the security officer (σ_1), the following key parameters are provided:

- G_E Benefit given for the fact that the system was not infected by the maintenance procedure
- G_N Benefit given for the fact that the maintenance procedure was done without any problems
- G_V Benefit given for the fact that the maintenance procedure was done successfully and in a safe manner
- K_V Penalty in the case of a violation of the security policy

The payoffs are taken from a *real world assumption* and reflect observations in dealing with the service technician in a power plant.

The payoffs of the game matrix for the security officers and service technicians are illustrated in the Table III. If the payoffs in Table III are taken into account in the bi-matrix,

 ISBN: 978-1-61208-298-1

Table III: PAYOFF FOR BOTH PLAYERS

σ_1		σ_2	
G_S	6	G_E	3
G_B	6	G_N	4
K_S	3	G_V	5
K_R	8	K_V	11
K_U	2		

Table IV: MOVES IN A GAME AFTER STUXNET VIRUS

		σ_2	
		infect	not infect
σ_1	trust	$G_V - K_V$, $G_B - K_S - K_U$ (-6, 1)	$G_E + G_V$, $G_S - K_R$ (8, -2)
	don't trust	G_N, $G_S - K_S - K_V$ (4, -9)	G_E, G_S (3, 6)

the following Table IV is created. An appropriate strategy for both players is not apparent. It is also clear that for the current practice of using a virus scanner, no Nash equilibrium is appropriate and that it, at best, is only a stopgap.

D. Game of cooperation to find a solution for the Causa Stuxnet

In the previous subsection, it appears that the use of a virus scanner is only a stopgap measure in the sense of Game Theory. The game situation has been changed. In this subsection we will therefore, in the analysis of the Cause Stuxnet, initiate a modified game, which requires a collaboration of players. Then, a Nash equilibrium could be established and the utility function for the players is increased. Therefore, a pure strategy was sought that minimized the amount of costs (K_S, K_R, K_V, K_U) and correspondingly increased the value $\mathcal{U}$. The costs and benefits of the different values is still listed in Table III. These values have *not* changed after using a signature. Minimizing the cost and the strategy s is listed in (18)

$$min\,\mathcal{U}(s, K_s, K_R, K_V, K_U). \tag{18}$$

As a pure strategy, in terms of a cooperation between the two players, it means a lesser amount of work (benefits) for both players and the two companies. The effort must keep both sides balanced. This balance and the Nash equilibrium arise when the software manufacturer creates the SCADA software with a signature over a hash value and ensures that the signature was generated using the original software. Then, the signature was provided to the power plant operator. This change will change the behavior of the players in the Table IV with the same payments (benefits) in the Table III. The behavior of the two players with the appropriate response to the use of the signature is given in Table V.

The difference between Table III and Table V is apparent in the field *(don't trust / not infect)*. The use of the signature on both sides (producers and users) increases the benefit and the values (K_V, K_S, K_R, K_U) do not occur. Thus, it is possible for the field (12, 12) to obtain a Nash equilibrium. The game tree in Fig. 7 displays the game. The moves (1, 2, 3, 4) show the course.

Table V: MOVES IN A GAME AFTER STUXNET WITH AN IMPLEMENTED SIGNATURE

		σ_2	
		infect	not infect
σ_1	trust	$G_V - K_V$, $G_B - K_S - K_U$ (-6, 1)	$G_E + G_V$, $G_S - K_R$ (8, -2)
	don't trust	G_N, $G_S - K_S - K_V$ (4, -9)	$G_E + G_N$, $G_S + G_B$ (12, 12)

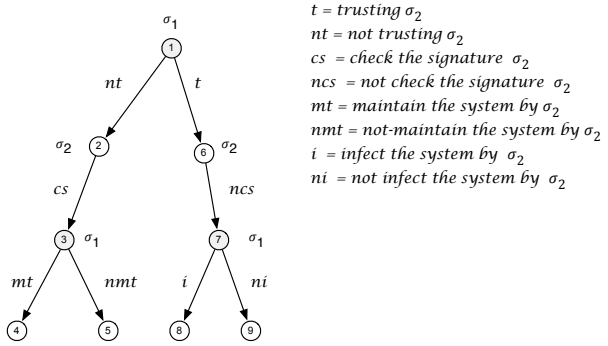

Figure 7: Moves in a strategic game in a game tree with a pre-exchanged signature

Thus, the measure (*use a signature*) met the two above-mentioned definitions 1 and 2, according to (11), and can be included in a security concept.

In essence, the strategic moves of the game in Table V and in Fig. 7 are only possible because a cooperative strategic game between the software manufacturers of SCADA systems and the power plant operators was recently initiated. A cooperative strategic game Γ consists of a tuple

$$\Gamma = \{N, v\}. \tag{19}$$

$N = \{1, 2\}$ is understood as the software manufacture (1) and the power plant (2). With

$$v \in \mathbb{V}(N) := \{f : 2^N \mapsto \mathbb{R} \,|\, f(\emptyset) = 0\} \tag{20}$$

being the characteristic function. The coalition function maps a value to each coalition. For example, if only one of the two coalition partners applied the signature, the result is given by $v(\{1\}) = v(\{2\}) = 0$. If the signature is used as described above by both, then $v(\{1\}) = v(\{2\}) = 1$. Only when both partners stick to the coalition is a benefit obtained, as one can see in the field *(don't trust / not infect)* in Table V. For the cooperative game, the Nash equilibrium is achieved. Should it not come to the coalition, the power plant operators may only use a virus scanner.

IV. Related work

The behavior of attacks on IT systems were studied in the Honeynet Project by M. Spitzer for first time [21] and has since received a lot of attention in the literature. The Honeynet Project, at the time, sought a novel approach in which the behaviors of the attacker were studied in order to develop them into conclusions for the protection of IT

 ISBN: 978-1-61208-298-1

systems. The behavior of the attacker was analyzed, but not with the methods of Game Theory. In the paper by W. Boehmer, human behavior was studied by entitling employees to perform unauthorized actions if necessary in a company. The method used is coupled to forensic analysis using data mining techniques [22]. Profiling was performed to identify the possible unlawful conduct by employees. The above examples did not use a game-theory approach. In the area of networking, T. Alpcan investigates attacks using game theory analysis. This game theoretical approach gave deep new insight into the defense of networks [13]. Based on the spy / inspector game, evidence was obtained from Alpcan. However, game theoretical methods have had hardly any or very little, but not systematic use in the field of IT security. In the case of the Stuxnet virus, infection was performed by a certified maintenance staff unconsciously and thus deviates from the usual spy / inspector game. All here above described methods of analysis would not reflect the infection realistically. We analyze the Causa Stxunet, or better the path of infection, therefore, using the trust game, to reflect the realistic situation.

V. Conclusion and further investigations

In this paper, we have studied the Stuxnet virus using Game Theory. In the multidimensional game of the Causa Stuxnet we have analyzed a part of the whole game, especially – *the infection path with the Trust / Investor game* – to compromise the security objective ($\mathbf{1}_{Int}$) of the SCADA system. From the game analysis, we derived that only a Nash equilibrium can be established if a collaboration is sought between the software manufacturer for SCADA systems and software users in the power plant. The cooperation is made possible by the implementation of a signature on the SCADA software from the software manufacturer in his laboratories. This signature can be checked very easily at the users site in the power plant, when a service technician arrives. This solution presented by the signature is a preventative solution and should be preferred to the current reactive solution of the virus scanner.

The path of infection is only one part in the multi-dimensional game, because there is an attacker in the background with the intention of damaging the power plants (compromise the security objective availability (Av $\leq$), see eq. 10). Against this background, the game analysis of the path of infection is only a part of a game in a multidimensional game. The analysis of the entire game of Causa Stuxnet and the embedding of this game into the whole game, will be part of another investigation.

References

[1] D. E. Denning, "Stuxnet: What has changed?," */Future Internet/*, vol. 4 (3), pp. 672–687, published online: 16 July 2012 / last accessed 2013-07-15/ doi:10.3390/fi4030672.

[2] N. Falliere, L. O. Murchu, and E. Chien, "Symantec security response, w32.stuxnet dossier, version 1.4." http://www.symantec.org., 02 2011.

[3] C. Salter, O. S. Saydjari, B. Schneier, and J. Wallner, "Toward a secure system engineering methodolgy," in *Proceedings of the 1998 workshop on New security paradigms*, NSPW '98, (New York, NY, USA), pp. 2–10, ACM, 1998.

[4] B. Schneier, "Attack trees, modeling security threats," http://www.schneier.com/paper-attacktrees-ddj-ft.html, 1999.

[5] F. Carmichael, *Guide to Game Theory*. Pearson Education Limited, ISBN 0 273684965, 2005.

[6] B. Kordy, S. Mauw, M. Melissen, and P. Schweitzer, "Attack-defense trees and two-player binary zero-sum extensive form games are equivalent," pp. 245–256, 2010.

[7] K. D. Mitnick and W. L. Simon, *The Art of Deception, Controlling the Human Element of Security*. Wiley, New York NY et. al., 2002.

[8] ENISA, "Stuxnet analysis, http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis," 10 / 2010.

[9] W. Boehmer, "Dynamic systems approach to analyzing event risks and behavioral risks with game theory," *PASSAT/SocialCom 2011, Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference on and 2011 IEEE Third International Conference on Social Computing (SocialCom), Boston, MA, USA, 9-11 Oct., 2011*, 2011.

[10] R. Giacometti, S. Rachev, A. Chernobai, and M. Bertocchi, "Aggregation issues in operational risk," *Journal of Operational Risk*, vol. 3, no. 3, 2008.

[11] F. Capra, *The Turning Point: Science, Society, and the Rising Culture*. Bantam, 1984.

[12] F. Capra, *The Web of Life: A New Scientific Understanding of Living Systems*. Anchor Books/Doubleday; 1st edition, 1996.

[13] T. Alpcan and T. Basar, *Network Security - A Decision and Game-Theoretic Approach*. Cambridge University Press, 1. ed., 2011.

[14] N. Taleb, *The Black Swan*. Random House, 2007.

[15] G. Dukic, D. Dukic, and M. Sesar, "Simulation of Construction Project Activities Duration by Means of Beta Pert Distribution," *in Information Technology Interfaces, 2008. ITI 2008. 30th. International Conference on*, pp. 203 – 208, 2008.

[16] W. Boehmer, *Information Security Management Systems Cybernetics*. *in* Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, (ed.) M. Gupta, J. Walp, R. Sharman, IGI Global publisher of the Information Science Reference, 2011.

[17] JTC 1/SC 27/WG 1, "ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements." Beuth-Verlag, Berlin, 10, 2005.

[18] P. Artzner, F. Delbaen, J.-M. Eber, and D. Heath, "Coherent measures of risk," *Mathematical Finance*, no. 9, pp. 203–228, 1999.

[19] J. Berg, J. Dickhaut, and K. McCabe, "Trust, reciprocity, and social history," *Games and Economic Behavior*, no. 10, pp. 122–142, 1995.

[20] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. No. 23, Society for Industrial and Applied Mathematics, Academic Press, New York, 2nd. ed., 1998.

[21] L. Spitzner, "Honeypots: Catching the insider threat," in *ACSAC '03: Proceedings of the 19th Annual Computer Security Applications Conference*, (Washington, DC, USA), p. 170, IEEE Computer Society, 2003.

[22] W. Boehmer, "Analyzing Human Behavior with Case Based Reasoning by the help of Forensic Questions." 24th IEEE International Conference on Advanced Information Networking and Applications (AINA-2010), 03 2010.

 ISBN: 978-1-61208-298-1