Security mistakes in information system deployment projects

Teodor Sommestad, teodors@ics.kth.se, Royal Institute of Technology, Industrial information & control system, Stockholm, Sweden, Osquldas väg 12, 7 tr, 100 44 Stockholm, Sweden

Mathias Ekstedt, mathiase@ics.kth.se, Royal Institute of Technology, Industrial information & control system, Stockholm, Sweden, Osquldas väg 12, 7 tr, 100 44 Stockholm, Sweden

Hannes Holm, hannesh@ics.kth.se, Royal Institute of Technology, Industrial information & control system, Stockholm, Sweden, Osquldas väg 12, 7 tr, 100 44 Stockholm, Sweden

Mohammed Afzal, afzalfast@hotmail.com, Royal Institute of Technology, Industrial information & control system, Stockholm, Sweden, Osquldas väg 12, 7 tr, 100 44 Stockholm, Sweden

1 Introduction

To secure information systems from malicious attacks have become an increasingly important task in most businesses today. A common way of approaching this problem is to think of securing systems as removing vulnerabilities in them. What defines a vulnerability is however multifaceted. Vulnerabilities are often seen as mistakes made during the development of the system and that have potentially both related exploits and patches. This type of vulnerabilities can for instance be found in databases such as the National Vulnerability Database (NVD) (NIST 2010). From a more conceptual perspective, a vulnerability could also have its root cause in mistakes performed later in the information system lifecycle. Systems may not be configured appropriately in relation to their usage and systems which lack all necessary security mechanisms may not be appropriately supported and protected by countermeasure mechanisms. Classical examples of such vulnerabilities are poorly configured firewall rules and usage of weak passwords. Of course, since the security area is (in-)famous for suffering from the weakest link syndrome, the consequences of any vulnerability could potentially be equally devastating.

This article focuses on mistakes made in between the development and the operational usage of the system, i.e. the deployment phase. Specifically, the context of the article is that of industrial control and SCADA (Supervisory, Control and Data Acquisition) systems for critical infrastructures. Industrial control and SCADA systems are used throughout a large number of industrial domains: the power sector, the water and waste water sector, in chemical plants, at oil and gas plants and distribution, and more. A common characteristic of the usage of systems in those businesses is that the control and operation of the infrastructure process is done through multiple instances of various industrial control systems originating from various vendors, combined into larger architectures of system-of-systems. Each

individual system is also a product that has been developed by the vendor over a long time for a large variety of customers. Thus, when individual systems are sold and deployed there is extensive work with configuring the product to the specific operation situation and integrating it with surrounding systems. Typically, when deploying these systems a large number of people from the vendor(s) are involved as well as external consultants. After taking the system into operation the responsibility of the systems are handed over to the user organization, but they seldom have the detailed knowledge about each and every configuration in the system. Thus, the user organization is highly dependent on that the deployment was done correctly in order to have a secure system.

If the deployment is correct in terms of security is dependent on human and organizational factors in the deployment project. This organizational and human side of information security is however significantly less researched than information security's technical side (Beznosov and Beznosova, 2007).

The purpose of this article is to investigate what kind of mistakes that can be made during the deployment phase of industrial control and SCADA systems and relate them to what kind of technical vulnerabilities these mistakes end up in. By doing this the ambition is that this knowledge would help the decision makers and analysts at critical infrastructure operators as well as system vendors to be more efficient in achieving a high level of cyber security. The investigation makes use of a Bayesian network in order to quantify the relationship between deployment mistakes (and factors) and their consequences in terms of vulnerabilities. The knowledge presented is based on interviews with experts with long experience on industrial control and SCADA system deployment.

2 Related work

Studies on human and organizational aspects are greatly outnumbered by studies on technological advances (Beznosov and Beznosova, 2007). With respect to studies of human and organizational aspects some research efforts has been spent on identifying which human and organizational factors that cause vulnerabilities in information systems. Other work has focused on classifying and investigating the actual vulnerabilities introduced due to human and/or organizational factors. However, comparably little effort has been spent on researching the relationship between human and organizational factors and actual flaws in information systems. This section aim at describing related work from these three perspectives.

2.1 Human and organizational factors causing vulnerabilities

A number of studies have been carried out in order to assess the determinants of low security due to the human factor, e.g. (Dourish, dl Flor & Joseph 2003)(Carstens et al. 2004)(Adams, Sasse & Lunt 1997)(Werlinger *et al.,* 2009)(Veiga & Eloff 2009)(Kraemer and Carayon, 2005) (Kraemer *et al.,* 2009)(Brostoff & Sasse 2001)(Knapp, Marshall & Rainer 2006)(Pattinson and Anderson, 2007)(Tsohou *et al.,* 2006). The research most closely related to the topic is described below.

The study described in (Werlinger *et al.*, 2009) involves a data set of 36 semi-structured interviews and suggest that three types of factors affect information security: human factors, organizational factors and technological factors. (Veiga and

Eloff, 2009) uses 1085 survey participants to evaluate reasons behind vulnerabilities caused by the human factor. These seven factors are very similar to those found by (Werlinger, Hawkey & Beznosov 2009).

(Kraemer, Carayon & Clem 2009) involves two focus groups of red teams (i.e. "hackers") and evaluates different "pathways", i.e. connections between causes of low information security. Some major themes found that affect vulnerabilities are training, policy, resource management and management.

(Brostoff & Sasse 2001) argues that safety critical systems design has similar goals and issues as IT security design and thus should be able to be modeled using the same principles. The model developed by the authors is based on the Generic Error Modeling System (Reason, 1990) and consists of five classes, each belonging to either latent and/or active failures. Latent failures include fallible decisions (e.g. security given a low priority), line management deficiencies (e.g. poor training of staff), psychological precursors of insecure acts (e.g. previous insecure acts unpunished). Active failures consist of insecure acts (e.g. weak login password). Active and latent failures include inadequate defenses (e.g. unusable encryption software). The four classes involving latent failures all involve different determinants of low security.

2.2 Vulnerabilities due to the human factor

There are various vulnerabilities which can be exploited by attackers. Taxonomies describing these include e.g. (Aslam, Krsul & Spafford 1996) (Alves-Foss & Barbosa 1995)(Bishop & Bailey 1996)(Yoshioka, Washizaki & Maruyama 2008)(Ye, Newman & Farley 2006)(Hansman and Hunt, 2004). Three of these studies are outlined below.

(Hansman and Hunt 2004) proposes a taxonomy which describes three types of vulnerabilities: implementation-, design- and configuration vulnerabilities. This classification is frequently used in publications, e.g. (Kraemer, Carayon & Clem 2009). (Alves-Foss & Barbosa 1995) presents a taxonomy which consist of system characteristics (e.g. unpatched operating system, physical security vulnerabilities), potentially neglectful acts (e.g. number of individuals with super user privileges, dormant accounts) and potentially malevolent acts (e.g. objects with same name as system commands or programs). (Aslam *et al.*, 1996) provides a classification of IT security faults in Unix operating systems. Among other things the author suggests synchronization errors, condition validation errors, configuration errors and environment faults as vulnerabilities due to human error.

These taxonomies are to some extent very similar in the sense that they all hint towards the same types of vulnerabilities. However, most research does not assess which vulnerabilities that are caused by what human errors. While there are some research in this area, e.g. (Carstens *et al.,* 2004) (Adams, Sasse & Lunt 1997) (Stanton *et al.* 2005) (Sasse, Brostoff & Weirich 2001)(Besnard & Arief 2004), most of these researchers are focused only on looking at a certain parameter such as passwords, access restrictions and/or software updates.

2.3 The relationship between causes and vulnerabilities

As described in section 2.1 and 2.2, both the variables associated to organizational and human causes to vulnerabilities as well as the vulnerabilities as such have undergone research. There has however not been much work carried out to assess the relationship between these two areas. In particular, the relationships between specific variables have not been researched quantitatively.

A few studies include empirical data, e.g. (Kraemer, Carayon & Clem 2009)(Stanton *et al.*, 2005)(Veiga & Eloff 2009). However, these merely hold qualitative results and do not assess the significance or strength of the causal relations between tangible vulnerabilities and their causes. For instance, (Veiga & Eloff 2009) investigates the variables that influence a security culture, but not the concrete vulnerabilities that a security culture with certain properties causes. The work of (Brostoff and Sasse, 2001) also discusses the relationship between human and organizational factors and flaws. However, they do not quantify this relationship.

This study aims to somewhat fill that gap through utilization of well-recognized theory in combination with empirical data from a sizeable international organization. Furthermore, this data is analyzed using statistical methods in order to assess the strength of the causal relations between causes of low security and resulting tangible vulnerabilities.

3 Formalism and method

This paper's main contribution is the Bayesian network presented in section 4. This section describes the Bayesian network formalism and how the Bayesian network in section four was developed.

3.1 Bayesian networks

A Bayesian network (BN) consists of two components: a qualitative structure and quantitative parameters. These two components are a representation of a joint probability distribution (Friedman and Koller, 2000). This section will describe the mathematical formalism of BN and how a BN is specified.

3.1.1 Mathematical formalism

The qualitative structure is represented in a directed acyclic graph $G=(V, E)$, with vertices V and edges E. The vertices V is a set of random variables $X_1,\ldots, X_n$ which may take on one a value from a finite domain of mutually exclusive states, e.g. {*True, False*}. An edge E in the directed acyclic graph denotes a causal dependency between two vertices, i.e. where the state of one variable influences the state of another variable. The variables that directly influence a variable's state are parents to the variable. In other words, the qualitative structure of the BN defines that there exist a causal dependency between variables, but not how strong it is. *Figure 1* shows a BN. In this figure the arcs and rounded rectangles represent its qualitative structure.

To define the strength of this dependency the quantitative parameters of the directed acyclic graph $G=(V, E)$ should be specified. These are specified as conditional probability distributions that express a probability distribution over the variables states, given the states of its parents in G. The tables in *Figure 1* show such conditional probabilities for variables.

The quantitative parameters make it possible to infer the probability distribution over the variables in the graph *G*. The joint probability distribution over the variables $X_1 \ldots X_n$ in *G* can now be written in product form:

$$P(X_1,..., X_n) = \prod_{i=1}^{n} P(X_i \mid Parents(X_i))$$

In other words, the probability of all variable states can be inferred in the BN. This inference can also take evidence on the state of variables into account, i.e. where the states of some variables are known and some are not.

3.1.2 Construction of Bayesian networks

To specify a BN, its qualitative structure and quantitative parameters need to be defined. This is usually done using either literature, statistical data, experts' domain knowledge, or through a combination of these sources (Druzdzel and van der Gaag, 1995)(Druzdzel & van Der Gaag 2000).

Literature can provide input to qualitative relations between variables in the domain and sometimes also specify probabilities that can be used to develop the BN. In domains rich of statistical data the construction of BN can be automated using computational methods, either fully or partially. If the dataset is large enough, both qualitative structure and quantitative parameters can be learned from statistical data. The knowledge possessed by domain experts is however often used as an input also when BN are constructed from statistical data (Druzdzel and van Der Gaag, 2000).

In the domain studied in this paper the availability of statistical data is sparse. In fact, no reliable statistical data on the relationship between properties of information technology projects the security related mistakes made in the projects. Domain experts have therefore played an important role for both defining to qualitative structure and specifying conditional probabilities. Section 3.2 will describe the domain experts that supported the construction of the BN; sections 3.3 and 3.4 describe how the qualitative and quantitative parts were constructed.

3.2 Domain experts

The BN presented in this paper is elicited from eight domain experts. They are all active within the same organization and where selected by management to represent a heterogeneous group of persons with substantial experience from control and SCADA system delivery projects.

Table 1 describes the current role of these experts, the amount of time they have worked with delivery projects, and their respective areas of expertise. The expertise category assessment was made by respondents themselves.

Table 1. The experience and competence of domain experts.

Domain expert	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*
Experience of deploying IT systems (years)	*33*	*30*	*25*	*20*	*10*	*30*	*40*	*25*
Area of expertise:								
Technical project management		●				●	●	●
Requirements engineering		●						●
System design and architecture			●	●				●

System development	●	●				●		●
System testing		●						●
System integration, installation and configuration		●	●		●		●	●
Communication networks	●		●					

At the time of this study respondent A and respondent B and had roles in system development. Respondent A's is a line manager and respondent B is a manager over systems engineering. Respondent C is a system engineer and respondent D is a system architect and the security expert within the organization. Respondent E and G work with plant engineering, respondent G as a manager and respondent E as an engineer. Respondent E is a service manager with a background in R&D, system engineering and system development. Respondent H is a project manager with a broad expertise.

3.3 Assessing the qualitative structure of the Bayesian network

The qualitative structure consists of two parts: a set of mistakes that can be made during delivery projects and a set of factors that influence the probability that these mistakes are made. How these two groups of parameters have been defined is described below.

3.3.1 Identifying mistakes

The definition of the qualitative structure was initiated with a literature study. The objective of this literature study was to identify common and/or severe mistakes made when information technology systems where installed. Both academic publications (e.g. (Veiga and Eloff, 2009)), text books (e.g. (Anderson 2008)), and technical reports (e.g. (Fink, Spencer & Wells 2006)) was surveyed in this study.

These mistakes discussed in literature were grouped in of classes of mistakes such as "Access control policies are not implemented properly". The domain experts were consulted to validate the relevance of the mistakes included in this list in interviews. The exact definition of the mistake categories and what should be included in them was left for the respondents to do. The categories were presented to the experts in the same way as they are presented here.

3.3.2 Identifying causes to mistakes

When mistake classes had been discussed with the domain experts, factors that influence the probability that such mistakes are made, were discussed. Each respondent was asked to list the most significant causes for each mistake using their own words. For each mistake the domain experts identified between two and eight causes.

There was a significant overlap between the causes that the different experts listed. Different experts provided the same causes and identified some cause influencing several mistakes. An aggregated list was created based on the domain experts' lists. This list, as well as the mapping between mistakes and their causes, was then presented for the domain experts in interviews to validate the aggregated list's content.

The number of causes qualitatively related to a mistake in this step determines the amount of quantitative data required for the BN in the next step. In order to make the next step practically viable, a sub goal of this aggregation process was to reduce the amount of the needed data. For this purpose, the experts' opinions on the most influential causes in the list were collected in face-to-face interviews. The list of causes was reduced during these interviews. Finally, the qualitative structure was presented to the domain experts in a number of iterations to validate it and assure a consensus among experts. The qualitative structure of the resulting BN is found in Figure 1, in section 4.

3.4 Assessing the quantitative parameters of the Bayesian network

The conditional probabilities associated with the BN have been elicited from the domain experts described in Table 1. Using a structured process for expert elicitation is important in order to minimize the bias of the domain expert. A rough outline for the stages in such an elicitation process is given in (Renooij, 2002):

- Selection and motivation
- Training
- Structuring
- Elicitation and documentation
- Verification

How these five stages were addressed in the study is described below.

3.4.1 Selection and motivation

When eliciting conditional probabilities for BN it is preferable to use more than one domain expert (Clemen & Winkler 1999)(von Winterfeldt and Edwards, 1986). It is also preferable to elicit quantitative data from the domain experts from who the qualitative structure was elicited (Renooij 2002). This will limit errors due to the definitional uncertainty associated with the variables.

As described, the eight domain experts were selected to represent a heterogeneous group of experts within the organization. They were in this case motivated by the fact that this study aimed at assessing and improving potential problems in their organization.

3.4.2 Training

If respondents are not previously familiar with the qualitative structure they need to be trained so that they understand the meaning of the parameters in the network. However, as quantitative data was elicited from the same group of persons that developed the qualitative structure they already had an understanding of the variables and relationships in the BN. To ensure an understanding of the quantitative parameters the concept of conditional probabilities was explicitly explained to the respondents. Finally, it was assured that the expert felt comfortable in the method used, in accordance with the recommendation in (Renooij, 2002).

3.4.3 Structuring

In addition to ensuring that the definitions of variables are understood by the experts, a suitable format to present the questions needs to be decided and preparations to suppress overconfidence among respondents (Renooij 2002).

Documented variable definitions were made available during elicitation sessions in case respondents needed to refresh their memory. The respondents were asked to provide a probability for each of the conditions specified in the conditional probability table. With respect to question format, experts in general feel uncomfortable with supplying probabilities directly, and prefer other more graphical answering formats such as checkboxes or graphs (Cooke. 1991). In this case the format on which quantitative data was collected (interviews) made it possible to ease potential discomfort. The experts were able to use other formats to express themselves and together with the interviewer find a number based on that. For example, the experts had the possibility to put their numbers in relation to other estimates and for instance state that probability X is about twice as big as probability Y. To suppress overconfidence the questions were complemented with verbal feedback on the complement of this probability, i.e. that mistakes were not made.

3.4.4 Elicitation and documentation

It is in (Renooij, 2002) described that experts may feel discomfort in expressing themselves in quantitative numbers on which they can be evaluated. To ease the experts' potential stress about providing such numbers they were asked to provide numbers that only are accurate in the sense that they represent their own experience and judgment, as recommended in (Renooij, 2002).

Another recommendation from (Renooij 2002) is to keep coaching to a minimum during the actual elicitation. This was done and during a session the questions where presented to the expert as described in 3.4.3, and only direct questions were asked. If a question needed to be clarified or further explained this was done using the documentation brought to interview sessions.

3.4.5 Verification

Verifying if the probabilities provided by the domain experts conform to observed frequencies was, as it often is (Renooij, 2002), difficult to do in this study. However, several efforts were made to make the result as reliable as possible. Also, the use of multiple domain experts did allow individual estimates to be compared.

Several types of bias can influence the accuracy of expert judgment (Cooke. 1991). In the present case, the risk of domain experts anchoring their estimates to each other was limited since the elicitation sessions were individual and others' estimates were not shown until after the elicitation was completed. Overconfidence has been addressed by discussing the complement to elicited probabilities, as recommended in (Renooij 2002). In the present scenario there is a risk that the domain experts would like to influence the result in order to achieve some particular motive. Two factors limit the risk of such motivational biases in this study. Firstly, the group of domain experts elicited represents a heterogeneous group of persons, were some are managers and some are engineers, some are in the project management functions and some are the system development function (c.f. Table 1). Secondly, the domain

experts knew that they would be held accountable for their numbers in front of their peers. All individual estimates where shown to the group once they were collected.

The arithmetic medium of the experts' assessments was used to construct a BN. This network was presented to the eight experts. They were shown the resulting probabilities for the scenario where no variables' states are known, and also shown some examples where evidence had been entered and the probabilities were updated. All experts found the resulting network overall accurate. Also, an additional domain expert within another branch of the same organization was consulted. This person also found the aggregated numbers reasonable.

A condition further indicating accurate data is the low variance among the numbers provided by the experts. The standard deviation of the domain experts' predictions is shown in the tables of section **4** and discussed in 5.3.

4 Result

The structure of the BN produced with the domain experts' help is depicted in *Figure 1*.

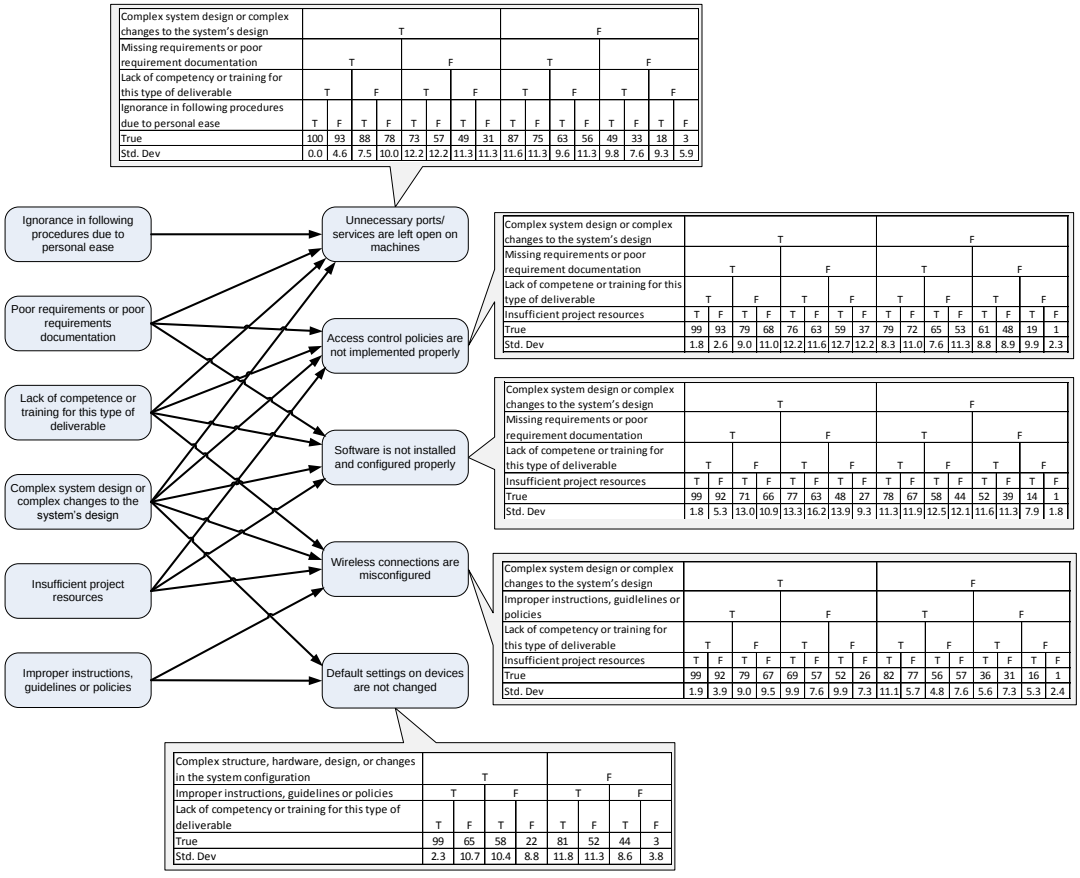

Figure 1. Bayesian network over mistakes in industrial control and SCADA system delivery projects.

It should be noted that this BN does not aspire to be complete in the sense that all relevant dependencies are outlined. As described in section 3.3 the dependencies included are those that have been identified as the most influential parameters by the domain experts while considering the cost of specifying quantitative parameters over the dependencies.

5 Applications and accuracy

The resulting BN can be applied for decision making in a number of ways. This section will describe how the mistakes' probabilities can be predicted and how the influence strength of variables can be assessed. The methods used here present some possible applications of BN in this research field. Last in this section, the accuracy of predictions offered by the network is discussed. The software tool Genie (Druzdzel 1999) has been used for calculations.

5.1 Predicting mistakes' probabilities

The tables detailed in Figure 1 describe the probability that a mistake is made under different conditions. These can be used to assess the probability that a mistake is made in a project. For instance, the probability that default settings are not changed can be calculated based on an assessment of: 1) the complexity of the project and changes made to it, 2) the instructions and policies used and 3) the competence of project participants. Given that prior (default) probabilities for these variables are available these calculations can also be made for the "typical" project or for projects which conditions are only partly known.

Table 2 shows prior probabilities for the conditions included in the network. These have been elicited from the same domain experts as the conditional probabilities. They intend to reflect the probability that a random project within the organization is executed under these conditions.

Table 2. Prior probabilities for conditions in the organization's projects. C1 to C6 denote the causes identified as the most influential.

Id	*Condition*	*Probability*	*Standard deviation*
C1	*Ignorance in following proper procedures due to personal ease*	*38.3*	*28.3*
C2	*Poor requirements or poor requirements documentation*	*44.2*	*14.2*
C3	*Lack of competence ore training for this type of deliverable*	*39.2*	*22.5*
C4	*Complex system design or complex changes to the system's design*	*63.3*	*21.1*
C5	*Insufficient project resources*	*37.5*	*13.3*
C6	*Improper instructions, guidelines or policies*	*54.8*	*28.2*

With these baseline probabilities the probability that a mistake is made can be assessed for a random project. These are shown in Table 3. With prior probabilities for conditions elicited predictions can also be made for different scenarios where some conditions are known and other are not. Table 3 illustrates this through scenario A and B. In scenario A, condition C1 is true and C2 is false; in scenario B condition C1, C2, C3, and C4 are false.

Table 3. Prior probabilities for conditions in the organization's projects. M1 to M5 denote the mistakes identified as the most influential. Random project denote the possibility of the corresponding mistake to occur for a "general" project. Scenario A and B denote the probabilities of corresponding mistakes to occur given certain cause conditions.

Id	*Mistake*	*Random project*	*Scenario A*	*Scenario B*
M1	*Unnecessary ports are left open on machines*	*56*	*48*	*3*
M2	*Access control policies are not implemented properly*	*57*	*43*	*8*
M3	*Software is not installed and configured properly*	*52*	*37*	*5*
M4	*Wireless connections are misconfigured*	*56*	*63*	*33*
M5	*Default settings on devices are not changed*	*52*	*56*	*28*

Another possible application is to assess how observations of mistakes that are absent or present influence the belief on the absence or presence of other mistakes. Bayesian networks makes it possible to calculate the posterior probability for any of the network's variables given observations of other variables in the network. This can be used to assess the likely conditions of a project based on observations of mistakes made in it. With updated beliefs on the conditions of a project, updated beliefs for other mistakes can be inferred. For instance, if it has been observed that unnecessary ports/services are left open on machines (M1) this will indicate the state in conditions C1, C2, C3 and C4. As these conditions also influence the probability that other mistakes are made this piece of information will update the probability that these mistakes are made. In the case where M1 is known to be true the probability that M2, M3, M4, and M5 are true is also increased.

5.2 Assessing the influence strength of conditions

The BN in *Figure 1* details how the state of 11 variables relates to each other. For a decision maker this can be used to assess the impact of six causes on five types of mistake. This impact can be examined by looking at the conditional probabilities depicted in *Figure 1*. These detail how inference would behave under different conditions. However, the theory expressed in the conditional probabilities of the BN can be difficult to understand, even for the most experienced users.

The static normalized "Strength of influence" is one of many methods that have been developed to visualize and congest the inference of a BN into elements that are easier to understand. This quantity shows how a change in the state of a variable influences the state of another variable in the model. *Table 4* shows the influence a cause has on the mistake probability in the general case is indicated in *Table 4*. The Euclidian distance is here used to measure the extent a cause impacts the probability that a mistake is made.

Table 4. Average static strength of influence.

	M1	*M2*	*M3*	*M4*	*M5*
C1	*0.13*	*	*	*	*
C2	*0.41*	*0.31*	*0.32*	*	*
C3	*0.22*	*0.26*	*0.30*	*0.24*	*0.35*
C4	*0.23*	*0.22*	*0.24*	*0.23*	*0.16*
C5	*	*0.13*	*0.12*	*0.10*	*0.43*
C6	*	*	*	*0.40*	*

Sum	*0.99*	*0.92*	*0.97*	*0.98*	*0.94*

** Cells marked an asterisk are undefined.*

Table 4 thus shows the influence a cause has on the mistake-probability in the general case. The influence of "Poor requirements or poor requirements documentation"(C2) on the state of the state in the variable "Unnecessary ports are left open on machines" (M1) is for instance 0.41. However, the influence of "Ignorance in following proper procedures due to personal ease" (C1) on the same mistake is only 0.13. The sum of the causes' influence-strength reflects how well they explain variation in the probability distributions. As can be seen in the conditional probabilities of *Figure 1* and in *Table 4* these mistakes are well explained by the causes included here.

5.3 Model accuracy and reliability

The accuracy of the predictions made by the presented BN is a key indicator of its utility. This BN is developed with the help of domain experts. Because of this the uncertainty associated with predictions can be assessed in terms of these respondents' domain expertise and the process used to elicit the network. Flaws in these two would lead to a disagreement among the respondents. The elicitation method, the respondents and their agreement is discussed below.

Table 1 describes the experience of domain experts. As can be seen from this table they have experience from a diverse set of functions in SCADA system deployment projects. In terms of time working with deploying information technology their experience ranges from 10 years to 40 years. Based on this it is reasonable to believe that the set of persons used to create the BN have sufficient expertise. However, as they are all employed by a single organization it can be questioned if their statements on conditional probabilities can be generalized other organizations.

With respect to the elicitation process the best-practice process described in (Renooij, 2002) has been applied with some exceptions. More precisely, data was not collected with the help of figures or other annotations and the data it has not yet been verified with respect to observed frequencies. On the other hand the interview format offered the domain experts a certain degree of freedom when answering questions and the use of multiple respondents offer some degree of verification.

The BN relies heavily on the opinion of a number of experienced individuals. According to (Einhorn 1974) a necessary, but not sufficient, condition for these individuals to possess domain expertise is that they agree and can reach a consensus, i.e. that they share the same opinion. The agreement between respondents' answers can thus offer a certain degree of verification of the models correctness. Or more precisely, that it is based on data from domain experts. (Weiss & Shanteau 2003) argues that this criterion requires that the experts share a common view on the definition of variables, which they not necessarily do. In the present case the respondents could form a consensus on the BN qualitative structure and the variance of the respondents' assessment of quantitative parameters is also low (cf. the tables in *Figure 1*). This shows that they share the same definitions of the concepts studied. More importantly, it offers support for the model's correctness and indicates that domain experts have a good idea of how organizational/human

variables influence the presence of mistakes. However, further work is needed to assert that the domain experts are calibrated (i.e. correct), for example by comparing the BN's probabilities to observed frequencies.

6 Conclusions

Information system vulnerabilities are often introduced due to human and organizational factors. Previous research in this field has either focused on the human/organizational variables that cause flaws or the flaws per se. However, the relationship between these types of variables has not been researched in quantitative studies. This study shows that domain experts in the field of information system deployment have a general opinion on how different variables relate and how important they are. The domain experts used in this study were able to agree on both with respect to the definition of variables and their conceptual relationship to each other. Also, when assigning quantitative parameters to these relationships an agreement among the respondents can be found.

With this data as a basis this study confirms the notion that human, organizational, cultural and policy factors influence the information security in organizations. In particular, this study confirms that these factors have a substantial influence on the presences of flaws in an organization's information systems. The context of this study was deployments of industrial control and SCADA systems. As these systems often operate critical infrastructures it is notable that flaws due to mistakes is common this context.

7 References

Adams, A., Sasse, M. and Lunt, P. (1997), "Making passwords secure and usable", In *Proceedings of HCI on People and Computers XII*. Springer-Verlag, London, UK.

Alves-Foss, J. and Barbosa, S. (1995), "Assessing computer security vulnerability." ACM *SIGOPS Operating Systems Review*, Vol. 29, No. 3, pp. 3-13.

Anderson, R. (2008), *Security Engineering: A guide to building dependable distributed systems*, New York, NY, USA: Wiley Publishing.

Aslam, T., Krsul, I. and Spafford, E. (1996), "Use of a taxonomy of security faults", In *Proceedings of the 19th National Information Systems Security Conference*, Baltimore, MD, pp. 551–560.

Besnard, D. and Arief, B. (2004), "Computer security impaired by legitimate users.", *Computers & Security*, Vol. 23, No. 3, pp. 253–264.

Beznosov, K. and Beznosova, O. (2007), "On the imbalance of the security problem space and its expected consequences", *Information Management & Computer Security*, Vol. 15, No. 5, pp. 420-431.

Bishop, M. and Bailey, D. (1996), "A critical analysis of vulnerability taxonomies", Technical Report CSE-96-11, Dept. of Computer Science, University of California at Davis, Davis, Sep. 1996

Brostoff, S. and Sasse, M. (2001), "Safe and sound: a safety-critical approach to security", In *Proceedings of the 2001 workshop on New security paradigms*, ACM, Cloudcroft, New Mexico, pp. 41 - 50 .

Carstens, D., McCauley-Bell, P.R., Malone, L.C. and. DeMara, R.F. (2004) "Evaluation of the human impact of password authentication practices on information security", *Informing Science: International Journal of an Emerging Transdiscipline*, Vol. 7(2004), pp. 67–85.

Clemen, R.T. and Winkler, R.L. (1999), "Combining probability distributions from experts in risk analysis", *Risk Analysis*, Vol. 19(187) pp. 187-204.

Cooke., R.M. (1991), *Experts in Uncertainty - Opinion and Subjective Probability in Science*, K. Shrader-Frechette, New York, US: Oxford University Press, inc.

Dourish, P., de la Flor, J.D. and Joseph, M. (2003), "Security as a practical problem: Some preliminary observations of everyday mental models", In *Proceedings of CHI 2003 Workshop on HCI and Security Systems,* Fort Lauderdale, Florida.

Druzdzel, M. and van der Gaag, L. (1995), "Elicitation of probabilities for belief networks: Combining qualitative and quantitative information", In *Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence*, San Francisco, CA, Morgan Kaufmann Publishers, Inc., pp. 41-148.

Druzdzel, M. and van der Gaag, L. (2000), "Building probabilistic networks: "Where do the numbers come from?"", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 12, No. 4, pp. 481-486.

Druzdzel, M.J. (1999), "GeNIe: A development environment for graphical decision-analytic models", In *Proceedings of the 1999 Annual Symposium of the American Medical Informatics Association (AMIA-1999)*, Washington, D.C*,* p. 1206.

Einhorn, H. (1974), "Expert judgment: Some necessary conditions and an example", *Journal of Applied Psychology*, October, pp. 562-71.

Fink, R., Spencer, D. and Wells, R. (2006), "Lessons learned from cyber security assessments of SCADA and energy management systems", Technical report: INL/CON-06-11665, US Department of Energy, September.

Friedman, N. and Koller, D. (2000), "Being Bayesian About Network Structure. A Bayesian Approach to Structure Discovery in Bayesian Networks", *Machine Learning*, Vol. 50, No. 1-2, pp. 1-30.

Hansman, S. and Hunt, R. (2004), "A taxonomy of network and computer attacks", *Computers & Security*, Vol. 24, No. 1, pp. 31-43.

Knapp, K., Marshall, T. and Rainer, R. (2006), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14, No, 1, pp. 24-36.

Kraemer, S. and Carayon, P. (2005), "Computer and information security culture: Findings from two studies", *Human Factors and Ergonomics Society Annual Meeting Proceedings, Macroergonomics,* Vol. 49, pp. 1483-1487.

Kraemer, S., Carayon, P. and Clem, J. (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", *Computers & Security*, Vol. 28, No. 7, pp. 509-520.

NIST, 2010. National Vulnerability Database Home Page. Available at: http://nvd.nist.gov/.

Pattinson, M. and Anderson, G. (2007), "How well are information risks being communicated to your computer end-users?", *Information Management & Computer Security*, Vol. 15, No. 5, pp. 362-371.

Reason, J. (1990), *Human Error*, Cambridge, UK: Cambridge University Press.

Renooij, S. (2002), "Probability elicitation for belief networks: issues to consider", *The Knowledge Engineering Review,* Vol. 16 No. 3, pp. 255-269.

Sasse, M., Brostoff, S. and Weirich, D. (2001), "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security", *BT technology journal*, Vol. 19, No. 3, pp. 122–131..

Stanton, J.M., Stam. K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24, No. 2, pp. 124-133.

Tsohou, A., Karyda, M. and Kokolakis, S. (2006), "Formulating information systems risk management strategies through cultural theory", *Information Management & Computer Security*, Vol. 14, No. 3, pp. 198-217.

Veiga, A.D. and Eloff, J. (2009), "A framework and assessment instrument for information security culture", *Computers & Security*, Vol. 29, No. 2, pp. 196-207.

Weiss, D.J. and Shanteau, J. (2003), "Empirical Assessment of Expertise", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 45, No. 1 pp. 104-116.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009), "An integrated view of human, organizational, and technological challenges of IT security management", *Information Management & Computer Security*, Vol. 17, No. 1, pp. 4-19.

Ye, N., Newman, C. and Farley, T. (2006), "A System-Fault-Risk Framework for cyber attack classification", *Information, Knowledge, Systems,* Vol. 5, pp. 135-151.

Yoshioka, N., Washizaki, H. and Maruyama, K. (2008), "A survey on security patterns", *Progress in Informatics*, Vol. 5, No. 5, pp. 35-47.

von Winterfeldt, D. and Edwards, W. (1986), *Decision Analysis and Behavioral Research*, Cambridge, UK,: Cambridge University Press.