ASK AND YOU SHALL KNOW: USING INTERVIEWS AND THE SBC MODEL FOR SOCIAL-ENGINEERING PENETRATION TESTING

Marcus Nohlberg
School of Humanities and Informatics,
University of Skövde,
Skövde, Sweden
and
Stewart Kowalski
Department of Computer and Systems Sciences,
Stockholm University/Royal Institute of Technology,
Stockholm, Sweden
and
Kerstin Karlsson
School of Humanities and Informatics,
University of Skövde,
Skövde, Sweden

Abstract

This paper presents the result of a case study where the SBC model was used as a foundation to perform semi-structured interviews to test the security in a medical establishment. The answers were analyzed and presented in an uncomplicated graph. The purpose was to study the feasibility of letting the users participate, instead of exploiting their weaknesses. It was found that the approach of interviewing the subjects rendered interesting, and relevant, results, making it an approach that should be studied further due to its apparent gains: less ethically troublesome penetration testing, increased awareness, improved coverage and novel information as added bonuses.

Keywords: Social Engineering, SBC model, Penetration Tests

1. Introduction

The paper begins with an introduction to social engineering, penetration testing and the SBC model. It then presents our method and the results, ending with a discussion of usefulness of the approach. Social engineering is the manipulation of humans in order to get them to, more or less willingly, gives out information or access to an asset (Mitnick [1]). It can be in a simple form, such as simply asking for the information, or in more complex form with the use of complicated ruses. It might also be to use technical means to improve the efficiency of the attack or the scope of the attack. Phishing is an example of this, where manipulative techniques from social engineering are used in combination with techniques used in spam to form an efficient attack vector affecting thousands, if not millions, of potential marks at once (Jakobsson, [2]).

For a long time, one of the most important tools in information security has been the penetration test. This tool gives us new insights into the weaknesses, and strengths, of a information security system. The focus has historically been on testing the network, firewall, and other technical aspects. The dilemmas with penetration testing and social engineering are discussed by Barrett [3], where the conclusion was that it is preferable better to use an audit style which has results and objectives that are clear and can be accepted by both subjects and company. The testing should also not lead to discipline or dismissal for the individuals.

Another review of the social engineering audit approach was done by Hasle et al. [4] who did social engineering penetration tests that tried to test a larger population. They performed two tests; the first was a survey where the users were asked to submit their login information in order to authenticate if they were to win a price, the second test was an e-mail sent out which triggered a login box. The study by Hasle et al. [4], is interesting but it can be argued that it is testing resistance to Phishing attacks, rather than what we consider pure social engineering. For instance, in none of their tests human interaction was used. Another approach is the one used in Nohlberg [5] where the subjects were asked to answer a set of questions under a false pretext (in this case “micro efficiency”) in order to get them to answer somewhat truthfully about their actions in certain security related situations. A more traditional approach to

social engineering auditing is argued by Jones [6], where the auditor is advised to actually perform social engineering attacks on the users. A similar approach is used by Orgill et al. [7], where they actually have a person trying to manipulate his way to information from the employees of the tested organization. They do this test in two stages. The first is to let the person wander around submitting employees to a written questionnaire with questions on security, logins etc., and the second stage is to try to gain physical access to the perimeters. Both approaches are disturbingly efficient. 81 % of the subjects asked gave away their login name. 59 % also gave away their passwords. Very few employees asked for identification or questioned the auditor. The auditor also managed to get unrestricted, physical access to the building.

Dalrymple [8] describes the highly successful internal audit on social engineering done by the IRS, where they called a select number of users under some pretext, requesting their passwords, which 35 % of the employees gave out. The classic approach, as used by Orgill et al. [7] definitely has it uses, but the weakness are that it is costly (since it takes a lot of time to perform) and that it might be perceived as more ethically questionable among the employees. One can also question the educational aspect. Will tricking a subset of all users make those who were not audited identify with the colleagues that actually were conned and learn from that, or would they stick to the "lie detection" bias (Marett et al.[9]), believing that they themselves would not fall for "tricks like that"?

For the audit professionals, Information Systems Audit and Control Association, ISACA [10] gives a list of areas that should be tested when doing a social engineering audit. Their suggested four areas to test are:

- Test of Controls – the general overview of the organization, can give a basic knowledge usable in further tests.
- Telephone Access – to use a set of well know attacks to test the resistance of the organization to attacks over the telephone.
- Garbage Viewing – to see if there is any sensitive information being thrown away (dumpster diving).
- Desktop Review – Check the user's workplace. Merge the data from the social engineering audits with other audits.

The guidelines given by ISACA [10] presents a basis for testing that could be perceived as ethical, at least by the organization, but the attacks suggested and the general set-up seems, in our opinion, to provide little useful data, and the approach leaves out any user input and feedback from the subjects, thus limiting the knowledge gained to that from a small set of attacks, and the learning experience of the subjects are absent. It also only tests how the users would act in a specific setting and does not give any general information about values, knowledge, attitudes etc.

One of the novel approaches that inspired us was Stanton et al. [11] where they did a survey asking employees about their view on security, and then contrasting the results with an actual audit done by experts. The results from Stanton et al. [11] indicated that one of the key success factors lay in the clear communication that the management takes security seriously and that the employees believe that they are accountable for their actions. While this approach covers more areas of information security than the social, and was done in a survey, the idea was inspiring.

The SBC-model

In order to create questions on the social element of security we needed a model describing security that covered both social and technical issues in order to have a starting point. The frequently used SIS-model (SIS, [12]) seems more to be a model of the hierarchical set-up of an information security organization than a good description of the term information security in our opinion. It is especially lacking in the sections covering social elements of security, as they are not included. In fact, the efficiency of social engineering attacks against an organization that has modeled its security tightly after the SIS-model would probably be great, due to the attack falling "between the cracks". A model of security which attempts to combine both the social and technical aspects of security is the SBC (Security by Consensus) model proposed by Kowalski [13]. The model was developed using the socio-technical systems school as used by Trist [14] of the functionalist approach and Tägil's model of technology and social change [15]. The model starts with two basic components of a social subsystem and a technical subsystem. These subsystems are further divided into culture and structure, methods and machines. The components structure, methods and machines refers to both abstract structures such as authority systems and concrete structures such as roads and mass communication systems. The technical subsystem is divided into two artifacts of machines, and methods used to produce work with the machines. The culture component of the model is taken from Tägil [15] and refers to both collective and distributed plural values in actions.

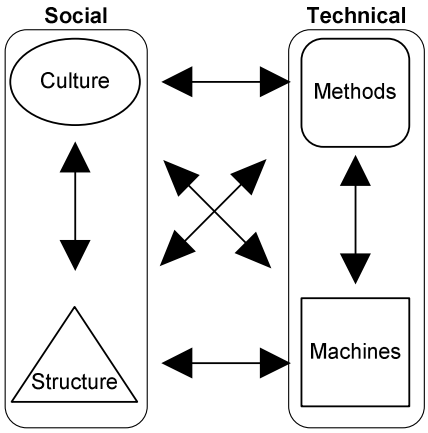

Figure 1. Socio-technical System (Kowalski [13] p.10).

The arrows in Figure 1 indicate mutual patterns of interchanges between the components. That is to say, a change in the machines used in the system can not only effect the methods used in the system but also the structure and culture. The underlying principle driving these interchanges is homeostasis or balance. The system is always trying to maintain a certain degree of control by apply a hierarchical of social technical controls that is to refer to as the Security By Consensus or SBC which consist of a hierarchical structure of social and technical controls. With ethics and law at the top of the hierarchy and IT technology at the bottom.

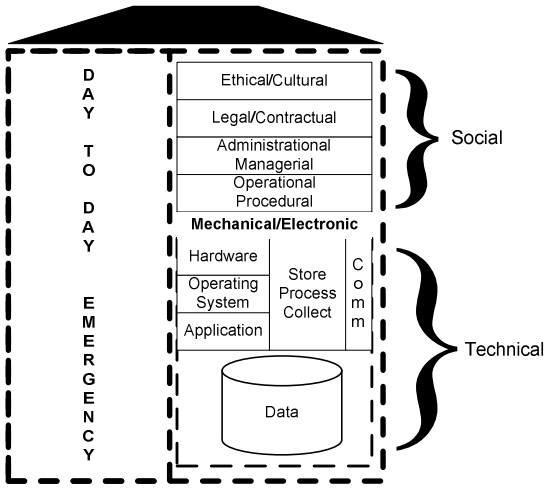

Figure 2. SBC Model, (Kowalski [13], p. 19).

The SBC model can be used to analyze security at every level, from individual to national; this flexibility combined with the inclusion of the social elements meant that the SBC-model was the best fit for this study. The SBC model has been developed in a well-defined SBC checklist that can be used in order to analyze a computer crime, or to report a crime, or just to understand an event better. This checklist was expanded on and improved by Tarimo [16], who created a checklist for general information security work, with the SBC model as a basis. That checklist is, however, mostly for use by people actually working with the information security, and not a tool to use in order to test subjects in the context that we are doing in this study.

Another problem is that most users do not understand how security works, and therefore construct their own, often incorrect, models (Adams & Sasse, [17]). The "old" way of managing information security has led to two specific problems (Adams & Sasse, [17] p. 45):

(a) users' lack of security awareness, and
(b) security departments' lack of knowledge about users, producing security mechanisms and systems that are not usable. These two factors lower users' motivation to produce secure work practices. This in turn reinforces security departments' belief that users are "inherently insecure" and leads to the introduction of stricter mechanisms, which require more effort from users.

The use of the SBC model to visualize the whole area of information security is to facilitate the creation of a mental model amongst the subjects, and indeed the readers of the results of the study. According to Sasse [17], users tend to create mental models of the functions and behavior of the system that are relevant to the user. The SBC model uses common sense terminology and therefore makes it easy for the user to be directed in the creation of a mental model of security that is as intended by the researcher. With a correct mental image of security, awareness can be improved and less strict mechanisms might be needed. The areas we focus on in this study are those in the social group (taken from Kowalski, [13]):

Ethical/Cultural: Educational measures to deal with ethical or cultural problems.
Legal/Contractual: Legal contingency structure, knowledge of contractual and legal requirements.
Administrative/Managerial:Measures activities focused on control, the formulation of policy, and regulations. Risk and vulnerability analysis.
Operational/Procedural: Concrete activities for security.

In this study, our aim was to see if a soft approach to penetration testing could be used to complement or even replace traditional penetration testing when it comes to the human element of security. The research question was: Can interviews of employees on their awareness of the social areas of information security as proposed by the SBC model give useful information like traditional penetration tests do?

2. Method

In the beginning of this study we struggled with the choice of method. In a longer study, observation, a case study, or even action research could have been

interesting, but we could only get a limited access to the nurses, making a qualitative method suitable. The strength of qualitative method is that you get an insight into people's world and views. While a stricter approach, such as grounded theory, was tempting, we realized that this was a preliminary study, with the goal of developing a pragmatic set of questions and guidelines that could be used by professionals, and not just researchers and adapted the method to those demands.

As we wanted to get input from the users, while still allowing for them to think freely to some extent, we chose to use a semi-structured interview as described by May [18]. With a semi-structured interview the questions are prepared in advance, but the researcher can ask complimentary questions and have a dialogue with the subject. In order to facilitate elaboration, certain possible follow up questions were prepared beforehand. As we suspected that the subjects would be unwilling to consider themselves behaving insecurely, we also asked about what their colleagues would do. This also has the benefit of covering more subjects.

The questions were developed with the SBC model as a foundation. A preliminary test was done on the interview questions, after which slight changes were made on the order in which the questions were asked and how the questions were formulated. By listening to the recording, the researcher became more aware about how the wording and how the formulation of the questions could influence the subject. While the process of developing questions by using the SBC model as a background can be used for most studied organizations, the questions themselves should be adapted to the organization and the people studied. As the subjects studied mostly work with electronic journals, the questions were developed with that in mind. The goal was to ask them questions that they understood, about areas that were relevant to them. It was no use asking them complex questions that they could not answer; it would only lead to weakened rapport. The validity of the study is ensured through the description of the process, that several persons were interviewed and by the opportunity for feedback on the transcriptions for the subjects as well as the fact that the results are quite reasonable.

The interviews

The interviews all started with an explanation of the study, ethical aspects etc. During the interviews other questions than the pre-developed were asked, which was expected in advance. The researcher asking the questions is not only trained in security but is also a trained nurse, which made the interviews easier. The interviews lasted between 35 and 55 minutes. They were taped and later transcribed and then sent to the subjects in order to see that there were no major misunderstandings or misquotes after which the interviews were analyzed using qualitative methods. This was sent using e-mail due to practical reasons but it is notable that poor e-mail security might danger the anonymity of the subjects. Different themes and categories in the answers were apparent, and in some cases the subjects answered in such a way that the answers could easily be compared; in those cases a comparative analysis was made.

Ethical aspects

This study was done in connection with a larger research project, Melior, where the aim is to study different aspects of electronic patient journals in the Swedish healthcare. The involved organizations approved that their employees would take part in this study. The department heads were contacted and got a description of the study, approved, and then facilitated contact with a suitable nurse that could participate in the study.

The nurses were contacted, got a description of the project and what the interview would consist of as well as the method, and were asked if they would like to participate.

At the start of the interview, the subjects were informed again about the aim and method of the study, both orally and in a written document. They were also informed that the interviews would be taped and the tapes stored, but that they would remain anonymous in the study and on the tapes, how the material would be published and also that they could abort the study at any time, without needing to give a reason. Both the subject and the researcher then signed the document. The subjects were also offered a chance to see the transcriptions from their own interviews to ensure that there were no misunderstandings or misquotes.

3. Results

This section contains three sets of results. The first part is the procedure, the method, for doing this kind of penetration test, the second is the questions we developed, and the third set of results are those we got from using the questions in the health care organization, which are included as an example of the kind of real world data that can be gathered from using this approach.

The procedure for the penetration testing

The procedure is described as a numbered list, as there is some importance in doing the steps in the right order. The steps are taken from our own process, but improved based on our experience from this study.

1. Get the permissions you need from those involved.
2. Randomly select subjects if possible, or find who out you can use from the organization.
3. Study the organizations domain; learn about typical flaws, if any.

4. Using the SBC model as a basis, develop questions and follow-up questions covering the relevant areas.
5. Interview the subjects using semi-structured interviews and remember ethical demands.
6. Analyze the interviews based on answer frequency, content, and context.
7. Using the SBC model, try to visualize strong and weak areas of the information security based on this test. Be sure to include relevant thoughts and fears from the interviews in written materials too.

The process is deceivingly simple, but it worked well in this study.

The questions

There were ten questions asked, with between two and ten prepared follow-up questions to each. The questions were asked in Swedish, but are translated to English for this paper, and they were not always asked exactly as phrased below. There might be slight differences in meaning between the languages lost in translation.

While our aim was to study the Social section, it was apparent that some areas in the Technical section were also of interest. In 0the areas we focused on are in white, while the other areas are grayed out. In the questions below, the intended focus areas from SBC are in brackets.

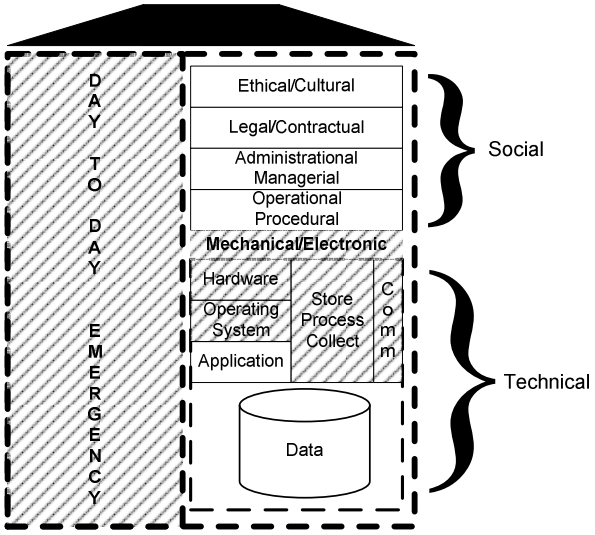

Figure 3. The areas of the SBC model that were studied.

1. Introduction

First I would like you to tell a bit about yourself, your professional background, and your computer experience.

- Do you have any other education?
- How long have you been working with Melior [The electronic journal system]?

2. Electronic journals and availability (Technical/Cultural/Application).

Could you tell a bit about how you feel about using electronic journals?

Follow-up questions:

- How is the availability to data when using the journal?
- Are the systems ever down?
- Do you find log-ins time consuming?
- From which mode do you log in?

3. Passwords (Cultural, Operational).

Could you tell a bit about what is important to you when choosing a password.

Follow-up questions:

- What do you do if you forget passwords?
- If you write down passwords, where do you store them?
- Do you reuse the same passwords inside or outside the hospital?

4. Log-ins, log-outs and log-files (Cultural/Legal/Contractual).

Could you tell a bit more about log-ins and especially log-outs?

Follow-up questions:

- Do people always log-out? If not, how common is it?
- Why do you believe that someone do not log out?
- What kind of consequences do you think it might have to not log out?
- Do colleagues know or use each other's logins in the different systems? What do you feel about that?
- Do you use shared log-ins anywhere?
- If so, where are the passwords stored?
- What do you feel about that everything you do is stored in log-files?
- When using Internet at the hospital, do you consider that those pages you visit are also logged, and how do you feel about it?
- Is there anything you would like to add about passwords and log-ins?

5. Short scenarios (Operational, Cultural).

You will now get a couple of short scenarios to answer, and you are welcome to think out loud about them, and ask if there is anything more you would like to know.

Follow-up questions:

- A systems administrator phones you, asking for your username and password. How would your colleagues react, and how would you react?
- A guy from the IT department comes to fix some error on the computers. He is wearing a sweater with the logo of the hospital and the IT department. How do you think that you and your co-workers would react? If he sat down by a computer connected to the network and started to work?
- Today there are a lot of web sites for special interests, where many people have a lot of friends. If they access such a site when they are at the hospital, and a friend send a link

with a cool motorbike or cute dog using that site, would people think differently about clicking on that link if they were at home or at work? How would your colleagues think, and how would you think?

6. What do you believe is the probability for something like that to happen in your workplace? (Operational, Cultural)

Follow-up questions:

- Have you ever heard about, or experienced a similar incident?
- Strange phone calls?
- Someone coming to your work, asking "the wrong questions"?
- Strange e-mails?

7. Tell me about the threats that you believe exists against the patient's data, and against the computer system as a whole, now that more and more information is available from the same source. (Ethics, Operational, Legal)

Follow-up questions:

- Why do we protect patient data, and what would happen if we did not?
- What would happen if access to Melior and the patient data would get into the wrong hands?
- Who would be interested?
- What would the information be used for?
- How do you think someone would go about getting access to the information systems, that is, rights to change the data?
- Who would want to do that?
- What would it be used for?
- What could happen?

8. Tell me more about how, where, and by whom you have been trained, or educated, about information security? (Legal, Contractual)
   - The security policy?
   - Can you read about this somewhere?
   - Is it a continuous education?
9. Is there anything you would like to add on this subject, perhaps something has come to your mind during the interview?
10. Last question: Could you give an estimate on how many times a day you write your password? (Operational)

Results from using the method

Seven interviews were done. The nurses came from six different departments. Six were females, one male. The ages were between 25 to 50 years. They had been nurses for 4 to 26 years. The distribution of the subjects seems to match the age/gender distribution in the nurse community. Four nurses worked with computer related tasks in their departments, but none had any specific computer education. They were self-taught.

Interviewing the subjects gave us ample examples of potential insecurities. A brief summary of the kind of data we got is described below, in order to illustrate some of the flaws found by this study. They are presented below in a manner modeled after the SBC model.

Ethic/Cultural: The awareness of ethical demands was high, and the subjects expressed a serious concern for secrecy concerning patient data. There is a tradition of keeping patient data safe. There is also, however, a tradition of unsafe behavior, for instance poor password management, an inability to lock unsupervised computers etc. The stated awareness is good, but the actions are not. The focus on functionality meant that passwords were selected so that they were easy to remember and quick to type.

Legal/Contractual: The law clearly states that it is illegal to study patient information that one is not entitled to read. This made the nurses aware of the importance of keeping passwords safe, and they had an intention of locking computers in order to not be legally responsible for the actions of others using their account. While there was information on security, the documents were not known by most of the subjects, and their actual influence on the day-to-day security work is probably very slight.

Administrative/Managerial: The subjects rarely acted with the written policies as support; they only had a vague idea of what the policy consisted of and where it could be found. The subjects' understanding of the policies was more that they regulated the relationship between employer and employee when it comes to not conducting personal business during working hours. As personal use of Internet was forbidden, it was also not regulated, e.g. no rules regulating receiving files from friends. The users did not know about any regulations on how often to change passwords, how to create a good password etc.

Operational/Procedural: The subjects had a specific vision of the threats to their information. The threats were from staff, patients, and relatives. Other attackers seemed highly unlikely. The consequences of an attack were primarily loss of personal information, but the concern for the integrity of data was quite low, as well as the availability of data. While there was an appreciation of the influences ones own actions might have on the security, the awareness of what one could actually do to improve security was very low. Technical attacks were generally not understood at all, and there was little awareness of attacks aimed against the social side.

Technical: The login procedure to the network was slow and tedious, and the systems lacked any automatic screen locks, as discussed above.

General Trends: The awareness of the importance of password quality is apparent. The actual quality of passwords, however, is not good. The argument

among the subjects is that this is because of complicated routines. The knowledge of legal and ethical demands does seem to at least improve awareness of password importance, but not enough to change behavior.
It is notable that the users are an apparent risk. They do not see any links between their own behavior and potential external attacks. They know little about the security documents that are available, and the documents they have read give them only limited information. This is because the documents have not been created to give guidelines for the usage of the information systems. They tend to focus on protecting the patient journals rather than to protect the systems themselves.

This study shows that two suggested social engineering attacks would be quite successful: Asking for login information over the phone and pretending to be an IT technician to gain access. The relative inexperience of the subjects on using the Internet meant that there were no conclusive answers on whether or not they would click on links. The major reason for their stiff resistance to this was probably that the scenario was to far away from their situation for them to grasp it.

Using the data acquired in the interviews, we made a judgment on the readiness of the areas surveyed based on frequency of answers, and the impact of the vulnerabilities. It can be seen in Figure 4 below.

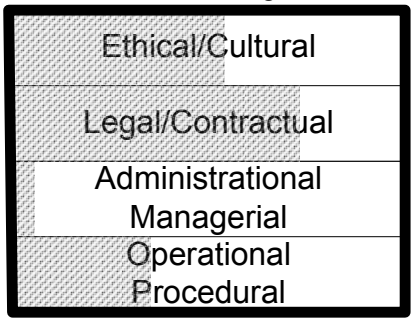

Figure 4. State of the social area.

The dark areas in Figure 4 above represent coverage, i.e. the darker an area, the more protected it is. ‘

4. Conclusion

Our aim of this study was to see if it was possible to get useful and relevant information by asking the users, instead of performing a penetration test on them. We argue that our result indicates that there is a surprising amount of information available from simply asking the users, instead of trying to trick them. The major advantages of this approach is that there are no major ethical concerns and that the users are asked to reason and think about security, hopefully creating a learning process simply by involving them in a non-judgmental manner. The very audit gives at least a selection of users increased awareness of possible attacks and the status of the information security situation. Hopefully they will be asked by or ask their colleagues about security after the audit. It also manages to capture certain risks that are quite hard to ask about in a more strictly formalized environment. The users were not afraid to report believing that both they themselves and their colleagues could potentially fall for certain attacks. This is interesting to contrast to some of the arguments put forth by Nohlberg [5] about the need to deceive subjects in order to get an accurate view of security. This might depend on the subjects, where subjects who claim to have a greater understanding of technology and security might have more "pride", while people who do not have the same “pride” might be more honest, or even too honest. Their lack of knowledge might make them believe that they and their coworkers are far more gullible than they actually are, and that the attacks are super-efficient. This is why the auditor needs to have a grasp of information security, to be able to gently and without bias bring potentially too far-fetched and biased ideas and thoughts in line with reality. We did not experience any problems with this.
The weaknesses of the approach is that it is quite resource intensive. With slightly more formalized interview guidelines and simplified reporting a lot of time could be saved. Another problem is that in most cases only a small selection of employees can be surveyed, but that is a problem shared with all but the automated penetration tests.
One of the future improvements is to develop a metric on how to judge the vulnerabilities in every category. It would be quite interesting to compare the results from this very “soft” approach to penetration testing to those from other methods. By doing this it would be possible to more fairly judge the merits of each method, but it is important in such a study to assess more than the results. Increased awareness among the subjects and their colleagues, attitude change, ethical concerns, and time spent are also important factors that could be studied in a future study. We believe that there is a problem in using just one method, because they all probably have their own merits and specific contexts in which they are useful.

In general, this approach could be useful for most organizations. The SBC model allows the results to be presented in such a way that they are easy to understand by non-specialists, and the survey of the organization can also be complemented by technical assessment to give a complete overview of the status. The approach suggested in this paper can either be used as a pre-study before a traditional penetration test if the organization sees the need for the traditional approach, or as a stand alone tool to gain an understanding of the status of the social section of information security.

The scary fact is that a skilled social engineer is successful in far too many cases today. Our primary task as security specialists now is not to simply see that there are vulnerabilities, but instead to understand more about the situation our users are in, and improve that. Only by understanding their situation can we limit the success of social engineering in the future. We will not build better security by pointing fingers at our employees, but by holding hands with them fill gaps in the security value chain we currently are running

5. References

[1] Mitnick, K.*The Art of deception.* Indianapolis: Wiley Publishing, Inc, 2002.

[2] Jakobsson, M. *Modeling and Preventing Phishing Attacks.* Phishing Panel of Financial Cryptography 2005.

[3] Barret, N , Penetration testing and social engineering: hacking the weakest link. *Information Security Technical Report.* 8, 4, 56 – 64.

[4] Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes, E. (2005) *Measuring Resistance to Social Engineering.* In Proceedings of the First International Conference on Information Security Practice and Experience, 2005, Singapore, April 11-14, volume 3439.

[5] Nohlberg, M, *Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned.* In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.

[6] Jones, C,*The Social Engineering: Understanding and Auditing* [Online]. SANS Institute. Available from: http://www.sans.org/rr/whitepapers/engineering/1332.php [Accessed May 1 2008]. .

[7] Orgill, G., Romney, G., Bailey, M., Orgill, P. (2004) The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems, Proceedings of SIGITE'04, Salt Lake City, UT 2004.

[8] Dalrymple, M. *Auditors Find IRS Workers Prone to Hackers*. [Online]. AP. Available from: http://sfgate.com/cgi-http://www.securityfocus.com/news/10708 [Accessed 30 Mar 2008].

[9] Marett, K., Biros, D., Knode, M. (2004) A Longitudinal Study of Lie Detection Training, Lecture Notes in Computer Science, Volume 3073, Jan 2004, 187 – 200. Springer, 2004.

[10] ISACA, IS Auditing Procedure Security Assessment-Penetration Testing and Vulnerability Analysis. [Online]. ISACA. Available from: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=18750 [Accessed May 1 2008].

[11] Stanton, J., Yamodo-Fagnot, I., Stam, K. *The Madness of Crowds: Employees Beliefs about Information Security in Relation to Security Outcomes*. In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.

[12] SIS 2003. SIS Handbok 550. *Terminologi för informationssäkerhet.* SIS Förlag AB. Stockholm (in Swedish).

[13] Kowalski, S. (1994) *IT Insecurity: A Multi-disciplinary Inquiry.* Diss. University of Stockholm. Report series No. 94-040, Stockholm, 1994.

[14] Trist E.L., Higgin G.W., Murray H., Pollock A.B., Organisational Choice, Tavistock Publications, London, 1963.

[15] Tägil S., Technology and Social Change - an Interdisciplinary Research Project at the University of Linköping, Sweden, in the proceedings of the Symposium on Technology and its Impact on Society, Tekniska Museet, Stockholm, Sweden, 1977.

[16] Tarimo, C. *ICT Security Readiness Checklist for Developing Countries : A Social-Technical Approach.* Diss. University of Stockholm. Report series No.06-017, 2006

[17] Sasse, M. A Eliciting and describing users' models of computer systems. PhD Thesis. Birmingham, UK: University of Birmingham, Faculty of Science, 1997.

[18] May, T. (2001) *Social Research: Issues, Methods and Process.* Buckingham: Open University Press, 2001.