APPLIED HOLISTIC APPROACH FOR SECURITY AWARENESS AND TRAINING

Kjell Näckros and Louise Yngström

Department of Computer and Systems Sciences
Stockholm University and Royal Institute of Technology, Sweden
kjellna@dsv.su.se, http://www.dsv.su.se/~kjellna
louise@dsv.su.se

ABSTRACT

In order to decrease Information and Communication Technology (ICT) security threats caused by human errors an increased concentration on education and learning is necessary. Because of the large amount of new users, with different kind of learning capabilities, the traditional teaching methods are not sufficient. Alternative forms of education are needed.

This article discusses why ICT security functionalities are important to understand and how nonlinear interactive computer games can support the holistic understanding of ICT from a security perspective[1].

Through visualizing common security functionalities a practical attempt to make learners understand the basic concepts of Public Key Infrastructure (PKI) is described, why it is needed and how these concepts can be applied in the daily use of ICT. The findings from several conducted experiments investigating the effect learning through a single-user computer game has on the acquired knowledge will also be presented and discussed. The findings show that a computer game can be an efficient instrument when learning to understand ICT security.

KEY WORDS

IT security, Awareness, Training, Teaching, Learning, Game-Based Learning (GBL), Game-Based Instruction (GBI), Computer Game, Nonlinear Instruction, Visualizing Security, Transparency

[1] This is an ongoing research and a continuation of Nordsec2000 [Näckros, K. (2000). *Using Computer Games in IT Security Education - preliminary results of a study*. pp.251-258] and discussed at Wise2 [Näckros, K. (2001). *Game-Based Learning within IT Security Education*. Wise2: IFIP TC11 WG11.8 pp.243-260].

APPLIED HOLISTIC APPROACH FOR SECURITY AWARENESS AND TRAINING

1 INTRODUCTION

All existing strategic organisational models stress the importance of educating the employers in order to get a sound and functional security culture, but none explains how this should be accomplished. In this article we are describing a practical attempt to make learners to understand why basic ICT security functionality are needed, familiarising the learner in the terminology and concepts within the domain, and how these concepts can be applied in the daily use of ICT.

1.1 ICT security is important to understand

The future of the digital society depends heavily upon peoples trust on ICTs. Ambiguities concerning computer user's privacy in conjunction with data integrity and confidentiality are major obstacles towards a sound and functional electronic society.

1.2 Two Views on ICT Security

There appears to be two fundamentally different views to look upon ICT security; centralised versus decentralised. In the former, the security functionalities are central with no interference of the users. The latter involves the users; the security functionalities should be situated where the possible damage is supposed to occur, the clients or the databases.

Another way of looking at this divergence is by using the term transparency. On one hand, we have the school of hiding the security functionalities from the user as much as possible. The applications will take care of the security for the user; the security functionalities are transparent to the users e.g. some web browsers presupposes that the users trust certain companies, or sign every correspondence s/he does without asking. In the other, the user has to handle the security functionality of his/her own e.g. actively verify a sender of a received email or sign with an active action.

1.3 Controlling your own system

Many of today's digital environments totally disregard privacy or other fundamental security aspects in favour for new technology advancements. They are in fact, making it almost impossible to control or safeguard your own information and communication. System designers ought to pay more attention to preserve the ability for the user to control their own security functionalities in order to support the creation of reliable trust between consumers/users/producers. Assuring user's privacy in digital environments could instead become vital competitive means for service and product providers. It is important to mention that security is about control. The more sense of control the more sense of security (without control, security becomes impossible). This implies that the users themselves must have the possibility to take certain responsibility of their own e.g. signing a document or choosing where to store sensitive information. It is perhaps not desirable to automate every task that is possible to automate. A sound security culture has to emerge concerning handling digital information. Nevertheless, systems designers can support the user when sensitive decisions have to be made.

1.4 Different Terminology

In an organisation, the interpretation of 'control' and 'secure' seems to differ depending on which organisational level[2] the user belongs to; at the organisational and group level 'control' may be interpreted as monitoring the employees within the system[3] while the employees', at the individual level, interpretation is more of the kind 'understanding'. The fact is that the more knowledge the individual has about the system environment, the more intentional harm may s/he accomplish and therefore becomes a higher threat. A sound and stable information security culture develops, however, from the individuals using it, although they need incentives and support from the management. It is also important to remember that manager's behaviour will function as the reference for employee behaviour (Martins and Eloff 2002).

1.5 Goal

One of the objectives with the research I am conducting is to increase the individuals' understanding of fundamental ICT security through visualising complex security issues and consequently, reduce unintentional misuse of the systems by employees and arguably more dedicated employees[4].

This author regards privacy as one of the fundamental ICT security issues; consequently, henceforth when mentioning IT security functionalities the protection of an individual's privacy is also included herein.

To empower the average computer user (in the role as citizen, producer, consumer as well as manager) to gain control of their ICT they need to have the necessary ICT security knowledge. By increasing the fundamental ICT security understanding (i.e. not only press that particular button in that particular application) so that users recognise and know how to behave when the unexpected system behaviour occurs, which it eventually always does, we will increase the overall robustness of the system[5].

1.6 Why a new method within security education

Current instructional methods in IT security have a tendency to fit certain individuals better than others. This in turn increases the feeling of insecurity for those who do not understand and therefore increase the IT vulnerabilities in the systems they are using. Hence, it is important to find alternative/ complementary methods that will stimulate learning/understanding of IT security issues also for these individuals, in order to strengthen the viability of the system as a whole. It is of course impossible to meet every individual's personal needs, although, it is substantiated that people learn and understand in several different ways of which some tend to be more efficient. One reason for this may be that most didactic methods e.g. books, multimedia, and front-end teaching, are structured and performed in a *linear fashion* i.e. teaching small pieces of information in a

---

[2] Organisational behaviour focus on three different levels; organisation, group and individual Robbins, S. P. (2000). Essentials of organizational behavior. Upper Saddle River, N.J., Prentice Hall.

[3] In spite of the fact that "…good practices are not added to an organisation through regulation, incentives and monitoring." LeGrand, C. and W. Ozier (2000). Information Security Management Elements, Audit and Control. **2002**.

[4] The percept trust between management and employees will aid in instilling an information security culture Martins, A. and J. Eloff (2002). Information Security Culture. IFIP TC11, 17th International Conference on Information Security (SEC2002), Ain Shams University, Cairo, Egypt, Kluwer Academic Publishers Group, Netherlands..

[5] In this case, all the different subsystems with humans, databases and information and communication supported technologies that are within the boundaries of the system in focus.

predetermined sequence in hope that the learner eventually will understand the overall picture. Unfortunately, the linear teaching strategy does not meet a large number of individuals' learning capabilities (also called *cognitive styles*). This leads to unnecessary efforts for the unmatched group of people in the learning process (Pask 1976; Turkle 1990; Yngström 1996) with a possible dissatisfaction and a low degree of understanding as a consequence.

ICT security differs from other learning domains in that respect that every person, regardless of profession, needs to use and rely on it. This researcher believes that ICT security is too important not to consider meeting the learners' individual cognitive learning styles. There is still a lack of alternative non-linear teaching methods that will stimulate holistic learning within IT security.

During 1999-2001, a Game-Based Instruction (GBI) within IT security was developed, and evaluated. The reason was to investigate if this could be a suitable method to stimulate learning of IT security for the individuals that may have difficulties with the conventional instruction. This research was first presented at Nordsec2000 (Näckros 2000) and the findings are to be found in full in the thesis '*Game-Based Instruction within IT Security Education*'(Näckros 2001).

This research is multi-disciplinary, containing theories within ICT security, learning, knowledge, instruction and game design. Figure *1* is an informal mindmap, on different conceptual levels, illustrating how the different keywords and concepts in the research relate to each other. The intention is to keep the figure as simple and holistic as possible and therefore the type of relations are not discussed. Marked area indicates scope of research in focus. Lines indicate relations.

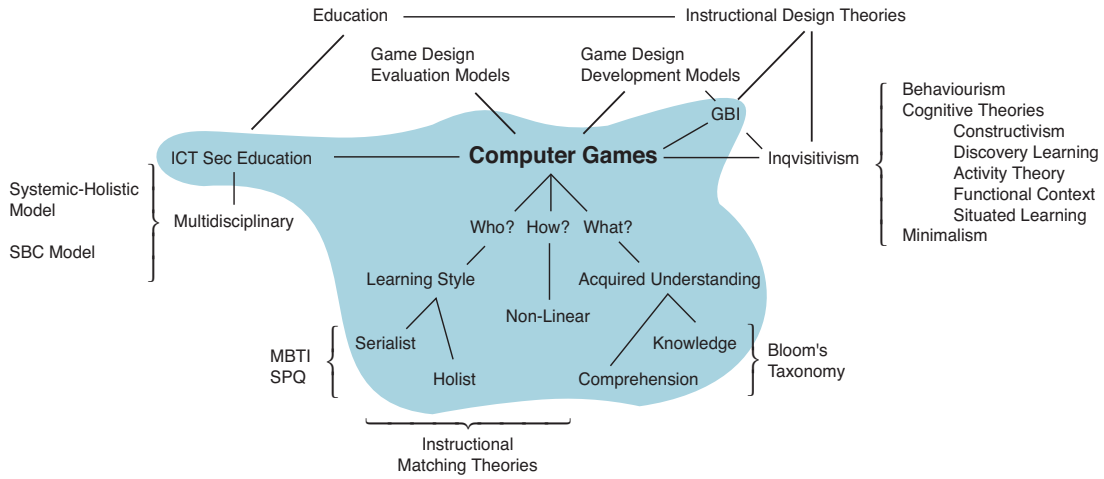

Figure 1, Graphical overview of the research

2 CONTRIBUTIONS

Although, this is still an ongoing research, thus far I have shown there is a necessary need for non-linear teaching methods in order to educate more individuals to understand ICT security and that computer games can be such a method.

I have also shown that this counts especially for people with little or no initial knowledge in the area.

During the investigation, a framework for Game-Based Instruction (GBI) and Design grounded in existing learning theories was proposed and discussed[6].

---

[6] The framework is presented in Näckros, K. (2001). Game-Based Instruction within IT Security Education. Department of Computer & Systems Sciences(DSV), Report Series: No-01-018-DSV-SU. Kista, Sweden, Stockholm University (SU)/ Royal Institute of Technology(KTH).

Based on this framework an applicable teaching method – a computer game to increase awareness/understanding of ICT security related issues – has been developed and its impact on IT security *understanding* [7] evaluated.

Furthermore, I have demonstrated that the type of knowledge acquired depends on the teaching method used i.e. the subjects who learnt through the computer game acquired more '*comprehension'* and the subjects who learnt through reading acquired more '*knowledge'*.

3 RELATED WORK

At the time this research was initiated (1998) most of the following games within IT security were not developed i.e. Cyberprotect and Warning for Virus. During 2000, Telia[8] and ÖCB[9] together with 'Dataföreningen i Sverige'[10] developed a computer game to increase the players' awareness of basic IT security. The author of this paper was also involved through active participation in the reference group.

Cyberprotect[11] is an interesting product because it is a professionally developed product, that utilizes action in such a way that the user maintains the overview of how the different objects in the system interact together.

It is the author's belief that these are both good examples of introducing computer games as instruction in the society. Unfortunately, this researcher has so far not seen any attempts to evaluate these as instructions.

4 METHOD

By comparing an educational computer game within ICT security with a conventional linear instruction through conducting experiments[12], data were collected and subjected to quantitative as well as qualitative analyses. Each participant's *learning preference*[13] was evaluated.

The analyses were also made to catch possible side effects during the learning experience such as satisfaction, gender and age differences, and efficiency in terms of time-consumption versus

---

[7] Since we want to investigate the amount of acquired understanding, we used Bloom's taxonomy of educational objectives Bloom, B. S., M. Engelhart, et al. (1956). Taxonomy of educational objectives : the classification of educational goals, Handbook 1, Cognitive Domain. New York, Longmans. He distinguishes between `knowledge' and `comprehension' where `comprehension' has a higher degree of understanding than `knowledge'.

[8] Telia - a major phone company in Sweden.

[9] ÖCB - Överskyddstyrelsen för Civil Beredskap (the Swedish Agency for Civil Emergency planning).

[10] Dataföreningen i Sverige (the Swedish Information Processing Society) http://www.dfs.se/sba/vvhs/

[11] Produced by SAIC - US Defence Information Systems Agency and Carney Interactive

[12] The data collection included two experiments with pretest – post-test and control group design.

[13] In this research, we distinguished between a persons learning preference – Gordon Pask called this conceptual competence Pask, G. and B. C. E. Scott (1972). "Learning strategies and individual competence." International Journal of Man-Machine Studies **4**: pp. 217-253. – *serialists* learn from details to wholes and *holists* from wholes to details.

acquired knowledge. The subjects were 78 students at the department of computer and systems sciences at Stockholm University and Royal Institute of Technology.

Additional experiments were also conducted by our industry partners SEIS and Nexus AB on 24 selected professionals. Only qualitative analyses were made.

5 RESULTS

Table 1 presents the improvements the subjects received in the post-test compared to the pretest. The columns are divided according the kind of questions the subjects received; questions related to 'knowledge' and questions related to 'comprehension'. The last column presents the average time the subjects within 'the group' used for learning. The rows show the groups', common characteristics for each subject e.g. the subject's learning preference and the kind of instruction the subject received during the experiment.

The subjects who been taught by reading a text acquired a higher degree of 'knowledge' and a lower degree of 'comprehension' compared to the subjects who 'played' the computer game.

The subjects with holistic learning preferences who received the computer game as instruction acquired a significant improved 'comprehension' compared to those who been reading a text. Surprisingly, this counted also for the subjects with non-holistic learning preference, though not with a significance.

Table 1, Improvements; relative difference as percentage units

$\Delta t_1 - t_0$ (% units), Standard deviation; used time (min:sec)

	Knowledge	*SD*	Comprehension	*SD*	Time
All	31,88	*0,2066*	22,70	*0,2266*	42:54
Game	30,65	*0,2261*	32,26	*0,2320*	59:52
Text	33,07	*0,1887*	13,44	*0,1807*	23:42
Holist	30,00	*0,1909*	27,14	*0,2257*	50:13
Serialist	35,19	*0,2245*	17,78	*0,2207*	33:51
Holist game	29,17	*0,1836*	37,78	*0,2264*	60:31
Holist text	30,88	*0,2036*	15,88	*0,1661*	37:40
Serialist game	32,69	*0,2815*	24,62	*0,2259*	43:33
Serialist text	35,56	*0,1739*	10,67	*0,1981*	24:51

The distribution of the subjects' improvements is shown in Figure *2*. Each subject is put in a coordinate system; the vertical line represents the acquired 'comprehension' (improvements in questions related to 'comprehension') and the horizontal line the acquired 'knowledge' (improvements in questions related to 'knowledge'). The axes are divided by the median of the improvements in 'knowledge' and 'comprehension'. The 'knowledge quadrants', divided by the two medians, shows the four categories of subjects:

A. Those who acquired low improvements in 'knowledge' and high improvements in 'comprehension'.

B. Those who acquired high improvements in 'knowledge' and 'comprehension'.

C. Those who acquired low improvements in 'knowledge' and 'comprehension'.

D. Those who acquired high improvements in 'knowledge' and low improvements in 'comprehension'.

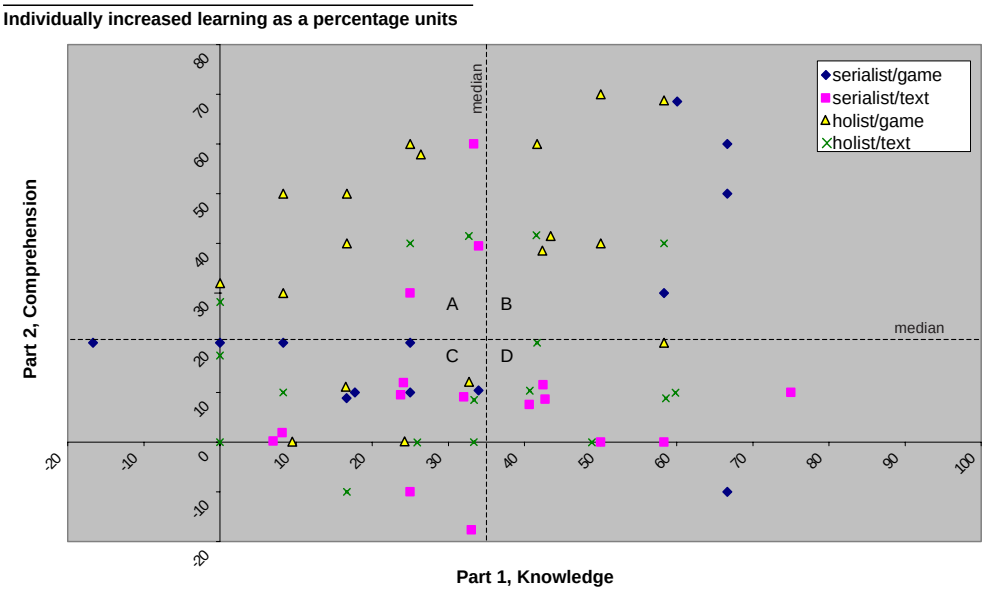

Figure 2, Distributions of Individuals in knowledge quadrants

Table 2 shows how the improvements for each subject group (100%) were distributed within the knowledge quadrants e.g. 38% of the holist-players are represented in quadrant A – high improvements in 'comprehension' and low in 'knowledge' – while only 5% are represented in quadrant D – high improvements in 'knowledge' and low in 'comprehension'.

In the table we can see that the subject groups, which received the computer game as instruction are well represented in knowledge quadrant B i.e. high improvements in 'knowledge' and high improvements in 'comprehension'. We can also see that no serialist-reader is represented in this quadrant.

Table 2, Distribution of Groups' improvements

Serialist/Game	0,00%	Serialist/Game	30,77%
Serialist/Text	20,00%	Serialist/Text	0,00%
Holist/Game	38,89%	Holist/Game	33,33%
Holist/Text	17,65%	Holist/Text	11,76%
	A	**B**	
	C	**D**	
Serialist/Game	61,54%	Serialist/Game	7,69%
Serialist/Text	40,00%	Serialist/Text	40,00%
Holist/Game	22,22%	Holist/Game	5,55%
Holist/Text	41,18%	Holist/Text	29,41%

	Mean = 31,88
Knowledge	Median = 33,33
	Mean = 22,70
Comprehension	Median = 20,00

When measuring improvements, subjects that scored a high percentage correct answer in the pretest is not shown correctly because they are likely to score lower in improvements, which could be one of the reasons that so many subjects are represented in knowledge quadrant C – low improvements in 'comprehension' and low improvements in 'knowledge'. In Figure 3 and Figure 4 the mean of each groups' acquired result in the pretest and post-test are therefore presented. The results are shown in percentage correct answers of max score. In these figures we can see that the groups' initial pre-knowledge was approximately the same but depending on the instruction they showed different amount of acquired 'knowledge' and 'comprehension' in the post-test.

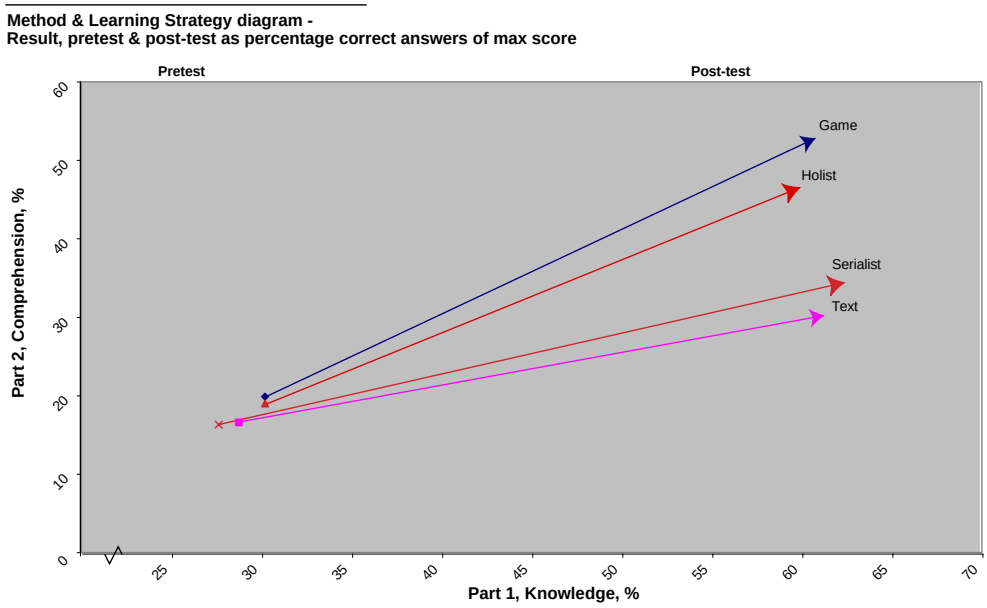

Figure 3, Results in pretest and post-test – Learning preference or Instruction

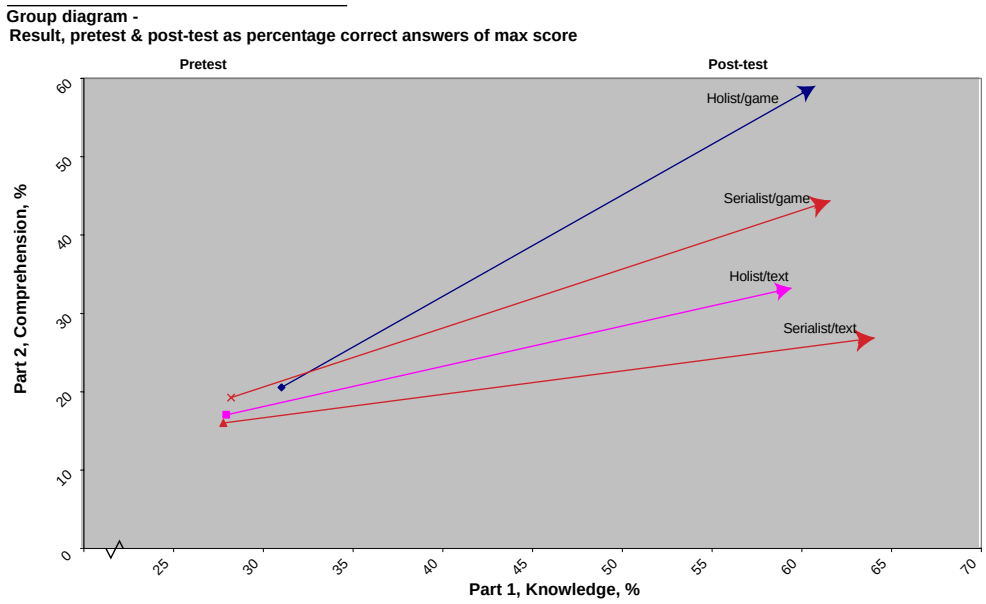

Figure 4, Results in pretest and post-test – Learning preference and Instruction

6 SUMMARY AND FURTHER RESEARCH

The conclusion from the experiments is that computer games can be a suitable non-linear teaching method when learning to understand IT security and therefore also a suitable alternative/complement to conventional linear instruction.

The conducted investigation shows that many individuals who have difficulties with understanding IT security presented in a conventional way acquire understanding more easily when a non-linear instruction are used.

One initial idea was based on that linear teaching methods have a predetermined structure set by the author/teacher and therefore the learners are more focused to remember than to actually understand i.e. ‘knowledge’ according to Bloom’s taxonomy. The findings from the experiments show that this is the case; all players acquired a better result in ‘comprehension’ than in

'knowledge' in contrast to all readers. All readers acquired better result in 'knowledge' than in 'comprehension' in contrast to all players.

There was a difference in how people acquire knowledge in the most *efficient* way, depending on the learning preference i.e. holists seem to be more focused to understand, and serialists seem to be more focused to remember. Readers with serialistic learning preferences acquired more of 'knowledge' than holistic readers in spite of the fact that the holists spent in average 52% more time on reading than the serialists.

Qualitatively, individuals with low prior knowledge and explorative in nature tend to increase their 'comprehension' more when using computer games as instruction than reading a text.

The evaluation forms from students are throughout positive about the game prototype and they enjoyed the learning process more than reading a book or even classroom teaching. Although, some students pointed out that professional made design and graphics would really improve their learning capabilities.

The evaluation with the professionals showed a different picture. The game has to astonish the players, with graphics and sound. The more expensive it looks, the more people will consider spending time with it.

An interesting finding was that even if the subject disliked the game – but continued anyway – s/he still acquired a higher amount of understanding than the subjects in the control group did.

7 CONTINUATION

Due to the findings from the experiments in combination with the positive feedback from the students, the game(s) will continue to be developed and improved e.g. Improved graphics and design, More scaleable, Smaller units, Module based, net-based, work in complement with linear instructions, independent of viewer e.g. hand computers.

Visualising security - To ease the usability of IT security products, and the education of such, a database with a collection of graphical security objects regarding colour, shape, symbol following international standards and recommendations will be compiled.

I will continuously conduct a follow-up on similar educational non-linear instructions and research within IT security. At the moment, I am participating in evaluating the use of net-based role-playing anti-hacking games for multiple computers.

During 2003 an additional study regarding the applicability of the non-linear instruction has been conducted. The model for the investigation has been to replicate parts of the experiments Alma Whitten conducted during a usability evaluation of Network Associates PGP ver5 software (Whitten 1999). The collected data is being analysed at the present and will probably also be presented at the conference.

My ambition is to develop and provide an IT security awareness toolkit for producing educational material i.e. both linear and non-linear instructions. During the development of 'the paradise game', I had to develop, compile and use a number of technologies, tools, models and frameworks. These have to be compiled and improved in order to be more general and cover the whole development cycle.

8 REFERENCES

Bloom, B. S., M. Engelhart, et al. (1956). Taxonomy of educational objectives : the classification of educational goals, Handbook 1, Cognitive Domain. New York, Longmans.

LeGrand, C. and W. Ozier (2000). Information Security Management Elements, Audit and Control. **2002**.

Martins, A. and J. Eloff (2002). Information Security Culture. IFIP TC11, 17th International Conference on Information Security (SEC2002), Ain Shams University, Cairo, Egypt, Kluwer Academic Publishers Group, Netherlands.

Näckros, K. (2000). Using Computer Games in IT Security Education - preliminary results of a study. Nordsec2000: Proceedings of the fifth Nordic Workshop on Secure IT systems - encouraging co-operation, Reykjavik, Iceland.

Näckros, K. (2001). Game-Based Instruction within IT Security Education. Department of Computer & Systems Sciences(DSV), Report Series: No-01-018-DSV-SU. Kista, Sweden, Stockholm University (SU)/ Royal Institute of Technology(KTH).

Pask, G. (1976). "Styles and strategies of learning." British Journal of Educational Psychology **46**: pp. 128-148.

Pask, G. and B. C. E. Scott (1972). "Learning strategies and individual competence." International Journal of Man-Machine Studies **4**: pp. 217-253.

Robbins, S. P. (2000). Essentials of organizational behavior. Upper Saddle River, N.J., Prentice Hall.

Turkle, S. (1990). Style as Substance in Educational Computing. The information society: evolving landscapes. J. Berleur. New York Heidelberg, North York, Ontario, Springer**:** pp. 145-160.

Whitten, A. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 9th USENIX Security Symposium.

Yngström, L. (1996). A systemic-holistic approach to academic programmes in IT security. Report series - Department of Computer & Systems Sciences 96:021. Stockholm, Sweden, Stockholm University & Royal Institute of Technology**:** 176 s.