Empowering Users to become Effective Information Security and Privacy Managers in the Digital world through Computer Games

Positioning computer games as means to increase information and communication security awareness

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

Key words: IT security, Awareness, Teaching, Learning, Game-Based Learning (GBL), Game-Based Instruction (GBI), Computer Game, Non-Linear Instruction, Visualising Security, Transparency

Abstract: A general holistic understanding of information security and privacy issues is vital for the individual as well as for the society. Ambiguities concerning user's privacy, integrity and confidentiality are major obstacles towards a sound and functional electronic society. System designers ought to pay more attention to these threats in order to support the creation of reliable trust between consumers/users/producers. To empower the average computer user to gain control of their information and communication technologies (ICT) they need to have the necessary ICT security knowledge.

Since new user groups, with different kind of learning capabilities are emerging, in conjunction with an overload of information there is a need for alternative approaches to offer the necessary knowledge.

This article discusses an ongoing research on visualising security aspects using computer games as a complement to the conventional linear instruction.

Based on the findings from a series of experiments evaluating a computer game's impact on learning ICT security, the continuation towards an applicable instructional framework of general ICT security understanding is discussed.

1. INTRODUCTION

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.

There appears to be two fundamentally different views to look upon ICT security; centralised versus decentralised. In the former, the security functionalities should be 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 signing with an active action.

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[1]. 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.

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

[1] Without control, security becomes impossible.

[2] Organisational behaviour focus on three different levels; organisation, group and individual [Robbins 2000]

[3] In spite of the fact that "…good practices are not added to an organisation through regulation, incentives and monitoring." [LeGrand and Ozier 2000]

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].

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 IT 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].

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 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[6]. 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.

IT 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 IT 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.

[4] The percept trust between management and employees will aid in instilling an information security culture [Martins and Eloff 2002].

[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.

[6] Also called *cognitive styles*

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].

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 IT 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[7].

Based on this framework an applicable teaching method – a computer game to increase awareness/understanding of IT security related issues – has been developed and its impact on IT security *understanding* [8] 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[9] and ÖCB[10] together with 'Dataföreningen i Sverige'[11] 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.

[7] The framework is presented in [Näckros 2001].

[8] Since we want to investigate the amount of acquired understanding, we used Bloom's taxonomy of educational objectives [Bloom, Engelhart et al. 1956]. He distinguishes between `knowledge' and `comprehension' where `comprehension' has a higher degree of understanding than `knowledge'.

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

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

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

Cyberprotect[12] 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. SUMMARY OF METHOD

The research was carried out in four stages: literature review and related work, development of a framework for GBI, development of an educational model and evaluation of the model as instruction.

For practical reasons we chose together with our industry partners SEIS[13] and Nexus[14] to focus on explaining the concept of Public Key Infrastructure (PKI), and decided to use Garefelt and Westerlund's book on cryptology and PKI [Garefelt and Westerlund 1997] as the linear teaching strategy. The two teaching strategies were tuned to match each other in terminology and contents.

The evaluation of the instruction was carried out through experiments. The sampling strategy used included both professionals and students, but for practical reasons, we needed to divide the evaluation into one approach for the professionals – uncontrolled environment – and one approach for students – controlled environment. For the first group we only evaluated the teaching strategy with qualitative data. The second group's evaluation was conducted as two experiments with pretest – post-test and control group design. Each participant's *learning preference*[15] were evaluated. The collected data were analysed with qualitative and quantitative methods.

This research is multi-disciplinary, containing theories within IT security, learning, knowledge, instruction and game design. Figure 1 is an informal mind-map, 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 projects' research. Lines indicate relations.

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

[13] SEIS is a Swedish association that promotes electronic information communication in Sweden.

[14] Nexus AB is a Swedish company that markets e-commerce solutions.

[15] In this research, we distinguished between a persons learning preference – Gordon Pask called this conceptual competence [Pask and Scott 1972] – *serialists* learn from details to wholes and *holists* from wholes to details.

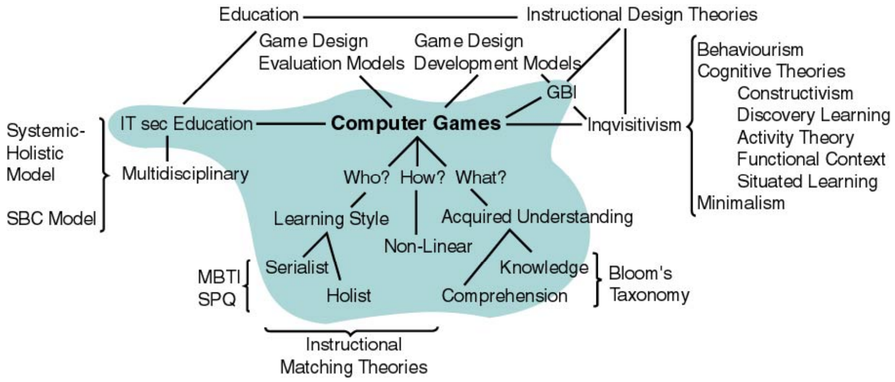

Figure 1. Graphical overview of the research [Näckros 2001] p.9

5. SUMMARY OF THE INSTRUCTION

Using Macromedia Authorware[16], a high-level authoring tool, we have developed a computer game as a non-linear instruction. The intention of the game was to make the 'players' understand the fundamentals of PKI. In order to separate the PKI area from reality, we chose to place the game in a surrealistic cartoon-like environment – the Paradise (as seen in figure 2). The actors are Adam, Eve and the Snake[17] and above them, there is a cloud in which all of the participants trust. Adam and Eve need to communicate with each other in a secure way, without the Snake finding out the contents.

By trial and error, the player will understand and become aware of how to achieve confidentiality, integrity, authenticity and non-repudiation within a computerised publicly available environment, and therefore we introduced a network into the Paradise.

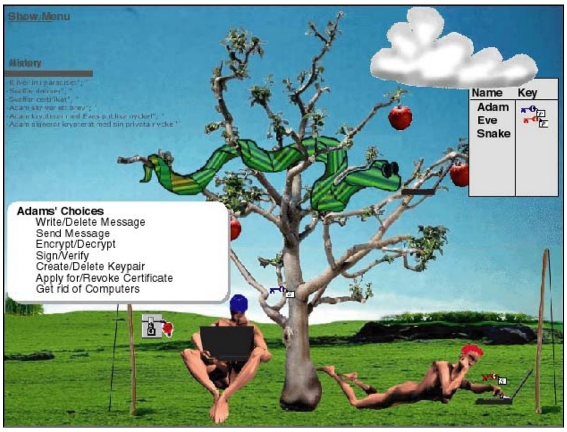

Figure 2. Paradise scenario

Through the graphical interface, the player can reach a vocabulary, a demonstration mode and ask for an assignment to solve e.g. help Adam to send Eve a message, in such way that Eve can be sure of that it has not been tampered with.

[16] http://www.macromedia.com

[17] Instead of Alice, Bob and Eve(sdropping) that is common in security education.

6. FINDINGS

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 AND FUTURE RESEARCH

The procedures that employees use in their daily work are the weakest link in the IT security chain. It is therefore important that all employees in the organisation are security aware.

7.1 Questions

This is an ongoing research and the following are to be regarded as, more or less, the continuation of the presented project.

1. Gameplay – The title of this paper claim to investigate computer games' impact on IT security learning, however, the instruction in focus lack certain game aspects such as; '*gameplay*[18]'. The 'game' may be a 'fun' alternative in learning IT security but as a game, it is quite dull. What about making the game more fun and interesting, can this have additional influence on learning?
2. Usability – A visual game/non-linear instruction uses graphical objects. There is a need for standardised instructive security symbols. How should they be designed?
3. Games – Only one non-linear instruction's impact on learning IT security has been evaluated, and this was only a prototype. Many of the participants in the experiments comment that the game needs to be improved. What about other computer games, or other kinds of games?
4. Applicability – The findings have been based on efficiency of the instruction in terms of time spent on learning and acquired understanding. Even more interesting would be to investigate the non-linear instruction's applicability. Does the level of applicability of the learner's newly acquired knowledge differ depending on the type of instruction used?
5. Mobility – Perhaps non-linear teaching methods are more appropriate than linear methods in handheld devices.
6. Users – In the introduction to this paper 'new user groups' is mentioned, they are, however, not participating in the experiments. I have evaluated the learning of undergraduates and professionals already within the computer science domain; these are perhaps not the ideal target groups. What about younger people, elderly people, different student groups, ordinary employees or individuals with different cultural background? Perhaps other individual aspects than serialist and holist are more relevant. What about individuals with different kinds of learning disabilities e.g. dyslectics?
7. Framework – Non-linear instructions are expensive to produce. A generic framework for producing these kinds of instructions would minimise the cost. How could a generic framework for developing and producing non-linear instructions look like?
8. Evaluation – There is a lack of evaluation models of educational computer games. How do one evaluate if a computer game is of high quality? How does one evaluate a non-linear instruction's impact on learning?

7.2 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

[18] Indicates how fun it is to play. Can perhaps be measured in terms in time players continue playing or how often players return to the play – *Repeat playability*.

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.

Additional experiments, on four different kinds of user groups, regarding the applicability of the non-linear instruction will be conducted during autumn 2002 and spring 2003. The model for the experiments will be to replicate the experiments Alma Whitten conducted during a usability evaluation of Network Associates PGP ver5 software [Whitten 1999].

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.

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.

Garefelt, J. and A. Westerlund (1997). (in Swedish) Kort om krypto-Nytt behov för näringsliv och samhälle. Stockholm, Sweden, Svenska Arbetsgivareföreningen.

LeGrand, C. and W. Ozier (2000). Information Security Management Elements, http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=123. 19 July 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.: pp.203-214.

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.: pp.251-258.

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. (ed.) 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.