Learning Security through Computer Games: Studying user behavior in a real-world situation

Kjell Näckros

[1] The Department of Computer and Systems Sciences, Stockholm University and
Royal Institute of Technology, Sweden
kjellna@dsv.su.se

Abstract. This paper discusses how learning material in the form of computer games in the area of ICT security affect ICT security usage. The findings from a conducted user-study show that computer games can be efficient learning environments when using security tools in terms of accessibility, safety, and speed. By replicating an earlier usability study, in which the participants utilised security tools to send and receive encrypted emails, the practical consequences of learning via a Game-Based Instruction were evaluated; the findings show that none of the participants who were given the chosen computer game as an instruction before the actual assignment did make any serious error when applying their security knowledge in contrast to the participants who did not receive any instruction in forehand. They also finished the assignment faster than the corresponding participants. To be able to evaluate the "practical knowledge" acquired, a model for Vital Security Functions was created that allows for comparison of security usage between high-level security applications.

Keywords: ICT Security, Education, Game-Based Instruction, GBI, Computer Games, Game-Based Learning, GBL, Knowledge, Vital Security Functions, VSF, Linear instruction, Nonlinear instruction, Learning preferences

1 Introduction

Current learning materials in ICT 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 also increase the ICT vulnerabilities in the systems they are using. Therefore it is important to find alternative and/or complementary learning materials that will stimulate learning/understanding of ICT security issues also for these individuals, in order to strengthen the viability of the system as a whole. Within ICT security, Yngström [1] p.160 has discussed that "... educators will have to pay attention to developing new educational tools, which will stimulate and support various learning preferences ..." Fred Cohen's work within scenario-based training [2] resulted in the development of security games, however, in the opinion of this author, these games did not have the nonlinear dimension and were not developed with learning preferences in mind. Is it possible that individuals having difficulties with current linear learning materials will increase their knowledge and comprehension in the area of ICT security, if a nonlinear computer game is used?

But, to develop a Game-Based Instruction (GBI) is expensive. Because it often requires more people with different types of expertise involved throughout the development process as compared to developing a conventional linear instruction. Furthermore, findings from a similar studies [3], [4], [5], investigating the theoretical knowledge acquired via GBI, indicated that the learning process itself takes more time using a GBI as compared to a linear instruction.

When evaluating an instruction within ICT security it is necessary to consider what the learners actually learn; there is a need to investigate not only the theoretical knowledge acquired but also the applicability of the acquired knowledge, i.e. how the learners apply their theoretical knowledge in real-world situations.

If the usage of computer games as instruction leads to odd or distinguished risky behaviour when applying ICT security functions in real-world situations there is a reason not to favour further usage. While if the usage indicates a distinguished "sound" ICT security behaviour e.g. conducting few "dangerous" mistakes, this type of instruction may be considered despite the overhead cost generated by the development.

To possess theoretical ICT security knowledge does not necessarily imply a better or more affordable usage of ICT security tools in practise. In fact, the opposite is possible. It is possible that theoretical information distracts or confuses many users during usage; the security application's user interface seldom maps the terminology or the principles upon which the security application is based. Different applications use different kinds of analogies to aid the user in controlling the security functions. A user with only theoretical knowledge may, for example, search for functions hidden to the normal user; the application may (or may not) handle the functions automatically, i.e. transparently to the user in favour for an easily understood working environment. The user may, for example, hesitate pushing that particular button, required by the situation, because s/he does not know the exact consequences of the action, and may lose a sense of control.

During a previous conducted study, evaluating the theoretical security knowledge acquired through GBI [3] certain user behaviours among the participants were noticed. Based on these user behaviours it may be reasonable to assume that a user with only theoretical knowledge about ICT security will tend to:

- hesitate to execute functions, because lack of information about the function in conjunction with knowledge about possible consequences, and therefore
- spend time trying to map the application's terminology with their own knowledge.
- check and recheck the result of their actions instead of take a chance.

Consequently, it may also be reasonable to assume that a user without theoretical knowledge will:

- compare the usage with other applications, instead of trying to understand the security functions.
- learn through trial and error, and because of this
- make dangerous errors

- obtain a false sense of security; the application responds as expected e.g. no alert window, telling there is something wrong or a message box telling everything is ok.

These assumptions have guided the design of the study.

This paper presents parts of the findings from research on computer games' general affect on learning outcome within ICT security (ibid.), focusing on the question; how learning material in the form of computer games in the area of ICT security affect ICT security *usage*?

2 Method

This study replicates parts of an earlier study, in which Whitten and Tygar [6] investigated 12 individuals' ability to learn and use the public key encryption tool PGP 5 from Network Associates concerning the usability aspect.

The practical consequences of using an educational computer game, the Paradise GBI [3], [5], were investigated as follows:

- User-study on a real-world assignment using an earlier study [6] as a model.
- Development of a model – for evaluating the applicability of ICT security knowledge – so called, VSF-model within PKI.
- Two different analyses of the collected data according to the VSF- model (this paper will only present the first analysis.)

The applicability of the knowledge acquired through the GBI prototype was investigated and evaluated by reconstructing parts of an earlier study [6] where the participants had to perform a real-world ICT security assignment. The results from the two studies were compared and discussed.

A framework for evaluating and comparing Vital Security Functions (VSF-model) within a high-level security tool was created and used to evaluate the results. Time was a vital factor for comparing each participant's solution to the assignment. Other collected data included age, gender, interests, and preferable learning style. During the actual real-world ICT security assignment screen recordings and observations were collected.

The analysis investigated if learners who receive learning material in the form of a computer game (the Paradise GBI) will make fewer mistakes in a real-world ICT security assignment in PKI than those who receive none. "Fewer mistakes" was put in contrast to the results from the Whitten and Tygar study in which the participants did not have previous theoretical knowledge about PKI. The analysis compares the number of dangerous errors and time to fulfil the assignment by using data from VSF State table (see section 3.2). Since, in the Whitten and Tygar study "... only one third of them were able to use PGP to correctly sign and encrypt an email message when given 90 minutes in which to do so. Furthermore, one quarter of them accidentally exposed the secret they were meant to protect in the process, by sending it in email they thought they had encrypted but had not" (ibid. p.21) it was interesting to compare how the participants in this Study differed in managing a similar assignment from the participants in the Whitten and Tygar study. The independent variable would thus be the Paradise GBI, which the participants in this Study used prior to the assignment, and the participants in the Whitten and Tygar study did not.

2.1 Methodological considerations

When reconstructing a study it is almost impossible to meet exactly the same conditions on different occasions, it is simply difficult to identify what parameters caused any possible differences between the outcomes of the studies.

- **Time** – The Whitten and Tygar study was conducted in 1998 and the second study in this thesis in 2003; it is a time difference of five years. In five years, a lot has happened within ICT and ICT usage that may influence the findings of the latter study.
- **Place** – The Whitten and Tygar study was conducted at Carnegie Mellon University, Pennsylvania, USA and this study was conducted at Stockholm University, Sweden.
- **Culture** – It is possible that the test users' cultural differences may influence the findings.
- **Purpose of the study** – The Whitten and Tygar study investigated the usability of a particular public key encryption application using two different methods. This Study investigated the applicability of the test users' pre-knowledge on a particular public key encryption application.
- **Participant's fee** – In the Whitten and Tygar study, the researchers offered $20 in cash, whereas in the latter study the participants did not receive any money.

Although, the purpose for investigation differs between the two studies, it is still possible to use the data collected to make interesting and possible comparable statements about the learning situation itself.

2.2 Defining a model

To be able to analyse and compare collected data from a security functionality perspective, there was a need to identify the Vital Security Functions (VSF) necessary to achieve secure communication of information according public key encryption concepts realised in PGP 5.

By using VSF it is possible to neglect the user interface and the different analogies that differentiate the high-level security applications and evaluate according to the purpose of the application instead. Therefore, data within this model ought to be comparable for other high-level PKI applications as well.

The first step was to identify all PKI related choices the participant was faced with at different states when achieving the assignment. During this process, a VSF Use Case diagram, see Figure 1, was sketched.

In the second step, the relations between states were identified and a VSF State diagram was created. The VSF State diagram was needed to identify the necessary order between states.

When the VSF states and the necessary order between the VSF states were identified a table for the VSFs was created in Table 1. The VSF State table shows the different VSF states, the necessary order between the states and the time when the participant reached a certain state.

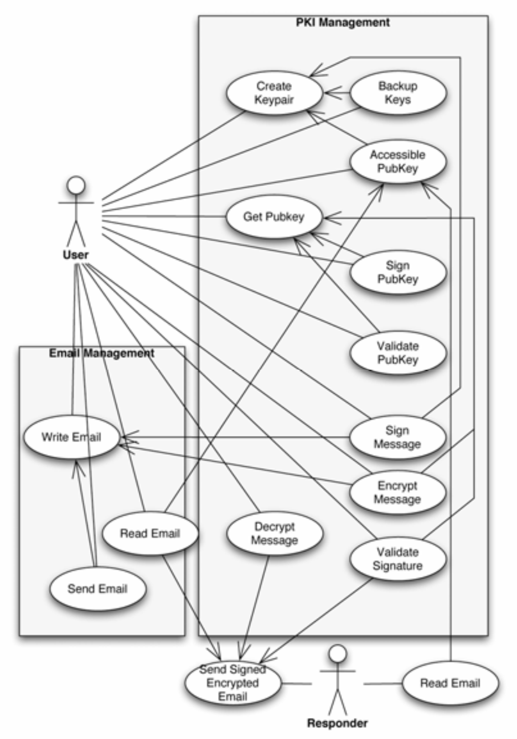


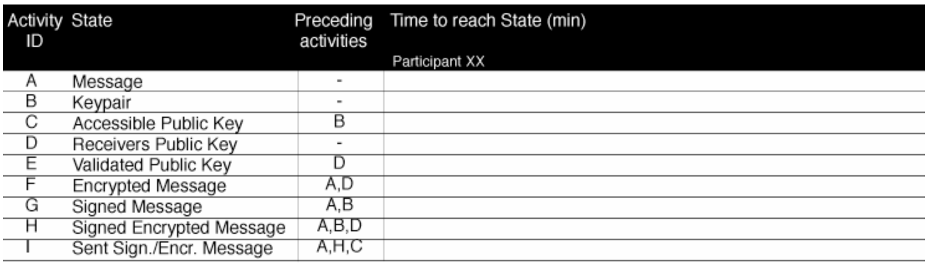
Fig. 1. Simplified VSF Use case diagram

The VSF State table is suitable when comparing and analysing numerical data, investigating for example the number of individuals that reached state “I” (accomplishing the assignment), or the average “time” for a group of individuals reaching a certain state. VSF State table is sufficient to answer if learners who receive learning material as the Paradise GBI will conduct fewer mistakes in a real-world ICT security assignment in PKI than those who receive none and is used in the analysis.

The number of participants successfully reaching state “I” in Table 1 was compared between the Whitten and Tygar study and this Study. The average of time to reach state “I” was also calculated and compared.

The number of conducted dangerous errors at the group of participants that did not finish the assignment was compared between the Whitten and Tygar study and this Study. A dangerous error during PKI usage is some act violating a basic concept of PKI e.g. making the private key publicly available to unauthorised individuals, or sending a secret message without suitable encryption applied to it.

Table 1. VSF State table



Activity ID	State	Preceding activities	Time to reach State (min)
			Participant XX
A	Message	-	
B	Keypair	-	
C	Accessible Public Key	B	
D	Receivers Public Key	-	
E	Validated Public Key	D	
F	Encrypted Message	A,D	
G	Signed Message	A,B	
H	Signed Encrypted Message	A,B,D	
I	Sent Sign./Encr. Message	A,H,C	

In the table it is also possible to see who, when and at what VSF State a participant failed the assignment.

3 Result

The findings from analysis showed:

- **Accessibility**. The Paradise GBI increased the participant's accessibility to the encryption software. The participants using the Paradise GBI before conducting the real-world ICT security assignment, all completed the security assignment within the time limit (12 out of 12), in contrast to the participants from the Whitten and Tyger study (5 out of 12 participants).
- **Safety**. The participants using the Paradise GBI before conducting the real-world ICT security assignment did not violate any basic PKI concept i.e. made no dangerous error. In the Whitten and Tygar study, 3 out of 12 participant exposed the secret message.
- **Speed**. The participants using the Paradise GBI before conducting the real-world ICT security assignment completed the assignment in average faster than the participants from the Whitten and Tygar study, and did so without being prompted from the test-monitor as in the Whitten and Tygar study.

The analysis compares data from two different studies, the Whitten and Tygar study (1998) and this Study. Subjected to analysis are mainly a) the number of dangerous errors and b) time to fulfil the assignment, using data from VSF State table.

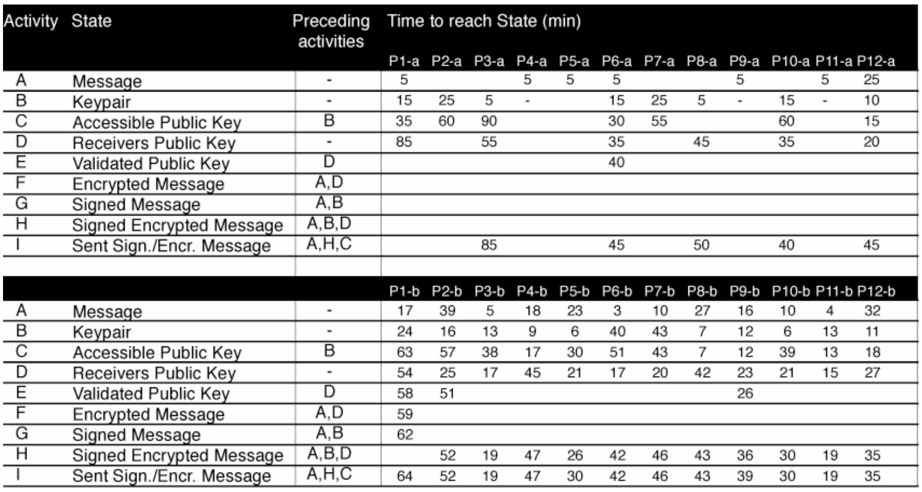
The participants' results are presented in Table 2. The twelve participants (P) in the upper area are from the Whitten and Tygar study (a) and the twelve participants in the lower area are the results from this Study (b).

Since the Whitten and Tygar study had a different research focus, each participant's transcript from that study had to be re-transcribed into the new VSF-model format and some data could not be transformed into the new format. These values are intentionally left out in the table; the activity "C" and "I", which are needed to complete the assignment are, however, included. If a value is missing at activity "C" or "I", it means that the participant failed to complete the assignment.

In the table it is also possible to see who, when and at what VSF State a participant failed the assignment.

In the Whitten and Tygar study only five participants out of twelve succeeded to fulfil the real-world ICT security assignment within the time limit of 90 minutes, “and they did so only after they had received fairly explicit email prompting from the test monitor posing as the team members” (ibid. p.18).

Table 2. Results (VSF State table); a) Whitten and Tygar study, b) current study



Activity	State	Preceding activities	Time to reach State (min)											
			P1-a	P2-a	P3-a	P4-a	P5-a	P6-a	P7-a	P8-a	P9-a	P10-a	P11-a	P12-a
A	Message	-	5			5	5	5			5		5	25
B	Keypair	-	15	25	5	-		15	25	5	-	15	-	10
C	Accessible Public Key	B	35	60	90			30	55			60		15
D	Receivers Public Key	-	85		55			35		45		35		20
E	Validated Public Key	D						40						
F	Encrypted Message	A,D												
G	Signed Message	A,B												
H	Signed Encrypted Message	A,B,D												
I	Sent Sign./Encr. Message	A,H,C			85			45		50		40		45
			P1-b	P2-b	P3-b	P4-b	P5-b	P6-b	P7-b	P8-b	P9-b	P10-b	P11-b	P12-b
A	Message	-	17	39	5	18	23	3	10	27	16	10	4	32
B	Keypair	-	24	16	13	9	6	40	43	7	12	6	13	11
C	Accessible Public Key	B	63	57	38	17	30	51	43	7	12	39	13	18
D	Receivers Public Key	-	54	25	17	45	21	17	20	42	23	21	15	27
E	Validated Public Key	D	58	51							26			
F	Encrypted Message	A,D	59											
G	Signed Message	A,B	62											
H	Signed Encrypted Message	A,B,D		52	19	47	26	42	46	43	36	30	19	35
I	Sent Sign./Encr. Message	A,H,C	64	52	19	47	30	42	46	43	39	30	19	35

In Table 2 it is shown that, of the participants that did not use the Paradise GBI before conducting the security assignment (the participants from the Whitten and Tygar study):

- 8 out of 12 participants had reached a VSF within 5 min.
- 4 out of 12 participants failed to fulfil the assignment because of violating a basic PKI concept i.e. exploiting a secret message or exploiting a private key.
- 1 out of 12 participants validated the authenticity of the receiver’s public key.
- 5 out of 12 participants finished all the necessary VSFs.
- Average time for finishing the security assignment: 58 min. (5 participants).

In Table 2 is also shown that, of the participants that used the Paradise GBI before conducting the security assignment (the participants from this Study):

- 12 out of 12 participants finished all the necessary VSFs to complete the security assignment.
- 3 out of 12 participants validated the authenticity of the receiver’s public key.
- Average time for finishing the security assignment: 42 min. (12 participants).

Generally, it seems that the Paradise GBI has had a positive effect on the participants’ usage of the PGP encryption software.

Despite a general understanding of PKI, acquired through the Paradise GBI, only 3 out of 12 participants verified the authenticity of the receiver’s public key/certificate. Most of the participants were satisfied with what appears to be the receiver’s name associated with the key, something anyone may associate with whatever name of choice. Apparently, future GBIs in PKI have to stress the importance of validating keys/certificates.

Since the PGP software has a built-in function that enables both encrypting and signing of data simultaneously, it is difficult to verify if the participants actually were aware of the distinction in practice, 11 out of 12 participants chose to use this multi-function instead of encrypting and signing separately.

4 Discussions and further research

GBI seems to have an overall positive effect on ICT security usage. In the study presented all the participants accomplished the real-world PKI assignment within the time-limit without making any dangerous error i.e. all participants in the real-world assignment managed to send and sign asymmetric encrypted data to the intended receivers in a successful way.

It was noteworthy that the participants used eleven different solutions to solve the assignment. Maybe not all participants would have completed the ICT security assignment if the possibilities to approach the assignment, were limited. It would be interesting to investigate the consequences of the ability to have the freedom of choice to conduct the assignment; what if the choices were limited. Does the freedom of choice influence the ICT security understanding and/or influence the number of dangerous errors?

During the assignment certain behaviours were also observed among the participants that could be an expression of a more "secure" and a more "insecure" behaviour, which would be interesting to study further.

Are GBI motivated to develop particularly for the area of ICT security? Because of the complex dynamic multidimensional nature of modern ICT security, it is this researcher's opinion that there is a need to be open-minded in the search for new educational means; nonlinear instructions like GBIs are definitely an interesting complement to conventional instruction in the effort to understand ICT security. GBIs are usually more expensive to develop but by using GBI frameworks, which combine design of computer games and design of instructional teaching methods, the development process can be less complex and less expensive leading to a higher amount of quality as a result which may also be evaluated and improved.

GBI is not a substitute for conventional instruction but an optional complement.

References

[1] Yngström, L. (1996) *A systemic-holistic approach to academic programmes in IT security*. Ph.d. thesis: Report series no. 96-021, issn 1101-8526, isrn su-kth/dsv/r–96/21–se, Stockholm University (SU) / Royal Institute of Technology (KTH).

[2] Cohen, F. (1998), "Fred Cohen and associates", http://all.net, (Accessed 2 Nov 2006)

[3] Näckros, K. (2002), Game-based learning within it security education. In H. Armstrong and L. Yngström, editors, Wise2: Proceedings for the IFIP TC11 WG11.8 Second World Conference on Information Security Education, pages 243–260, Perth, Australia, 2001.

School of Computer and Information Science, Edith Cowan University, Perth, Western Australia.

[4] Näckros, K. and Yngström L. (2004), Applied holistic approach for security awareness and training. In ISSA2004: Proceedings for the fourth annual conference ISSA in IT Security, Johannesburg, South Africa, 2004.

[5] Näckros, K. (2005). *Visualising Security through Computer Games: Investigating Game-Based Instruction inICT Security: an Experimental Approach*. Ph.d. thesis: Report series no. 05-014, isbn 91-7155-077-1, issn 1101-8526, isrn su-kth/dsv/r–05/14–se, Stockholm University (SU) / Royal Institute of Technology (KTH).

[6] Whitten, A. and J. D. Tygar (1998), Usability of security: a case study. Technical Report CMU-CS-98-155, Carnegie Mellon University, Pennsylvania, USA.

This Page Intentionally Left Blank