E-Learning of IT Security Threats: A Game Prototype for Children

Jana Fruth, Carsten Schulze, Marleen Rohde, Jana Dittmann

E-learning of IT Security Threats: a Game Prototype for Children

Jana Fruth, Carsten Schulze, Marleen Rohde, and Jana Dittmann

Otto-von-Guericke-University of Magdeburg
PO Box 4120, 39016 Magdeburg, Germany
{fruth, dittmann}@ovgu.de
{carsten.schulze, marleen.rohde}@st.ovgu.de

Abstract. In this paper an e-learning game prototype for primary school children (aged between 7 and 9 years) is introduced. The game teaches children about IT security threats , which they encounter using the Internet. The game is separated into three mini games: virus infection of the computer, inviting somebody in social networks, chatting with strangers. The game design used metaphors and based on standard guidelines of infantile learning environments (e.g. paradigm of simplicity, multidimensional stimuli, characters). Furthermore, the results of a user study of 36 primary school children are presented. In the future, the prototype would be extended by additional metaphors.

Keywords: e-learning, IT security threats, internet, game, children

1 Introduction and Motivation

Nowadays more and more children are using personal computers and the Internet. More than half of the primary-school pupils (6 to 10 years old) use these technologies regularly [13]. Surfing the Internet may expose children to many threats and risks, such as malicious codes infecting their personal computers, or their personal data being spied on [12, 13]. There are various concepts to raise children's awareness to IT security threats. Most parents set rules for their children's Internet usage (e.g. time limits). At school children are taught about the proper usage of personal computers by their teachers in computer science or IT classes. Furthermore, many different initiatives and websites offer information for both the parents and their children about IT security threats (see Section 2). However, according to research results and personal experiences those concepts are not reaching the children [12, 13]. To overcome this problem this article introduces an educational game prototype for children based on subjects of IT security. This method for raising children's awareness can also be adopted for safety (physical integrity) related subjects. The educational game prototype can be extended to cover subjects referring to safety related aspects of mobile toys like robots. The article is structured as follows: in Section 2 a short overview of the state of the art of methods for raising the awareness to safety and IT security related topics are illustrated. In Section 3 the educational game prototype

"InSiKids" (engl. "Internet Security for Kids") mentioned above is introduced. In Section 4 the results of the usability test that was performed with the prototype "InSiKids" is presented and discussed. The success of intermediation of IT security threats metaphors to primary school children and the confirmation of assumptions is checked. Section 5 concludes the paper and shows future prospects.

2 State of the Art

In this section the state of the art of children's psychology of learning, playing games, using the Internet are descripted. Furthermore, current techniques of computer game development and current IT security awareness raising methods for children are illustrated.

2.1 Children's Psychology

How children learn: Remo H. Largo, the Swiss paediatrician, says that children learn in different ways [11]: *Social learning:* The child imitates the behaviour of role models, like parents and other children. *Learning by experiences with the objective environment:* The child becomes acquainted with its environment by occuping itself with objectives via its motion activities and senses. So the child develops for example a comprehension for the dimension, shape or color of different objects. *Learning by education:* According to Largo the learning opportunities should be adapted to children's development-specific interests. Ideally, teachers creates the learning environment in such a way, that a child is able to gain experience and new comprehension on its own. This will be successful if a child has the comprehension for this specific learning assignment.

Why children play games: The terms 'play' and 'game' [19, 20] need to differentiated. Both, play and games are guided by rules, while rules of play (e.g. fantasy play) are flexible, games (e.g. basketball) are governed by explicit rules, which are not negotiable [17]. Various researchers [19, 22] claim, that play is being essential for children's healthy development. Its a cornerstone of children's development of cognitive, social skills, and a fundament to learn higher complex concepts if children are elder.

How they play games: *Conventional games:* Children in the primary school age prefer various games. Examples are sports (e.g. cycling), and traditional games (e.g. hide and seek). Favourite games of girls include verbal games, role playing, play with dolls [7]. Boys often play construction games and games [7] involving physically activities, like ball games [17]. *Computer and online games:* Among conventional games, computer games are an inherent part of primary school pupils leisure time. About 13% of children between 6 and 9 years play computer games every day, about 40% of them play regularly (once and/or several times a week) [3]. The majority of children in this age play not longer than one hour. The most used device are portable games consoles, such as Nintendo DS. Online games are not so common in this age. Only 15% plays online games

once a week. Offline games are more common. Nearly half of the children in this age play them. The favourite games differ between boys and girls. Boys often play 'FIFA', 'Mario Kart', and 'Pokémon'. The favourite games for girls are 'The Sims', 'Singstar', and 'Wii Sports'.

How and why children use the Internet: Aloud a survey throughout the EU [12] 60% of children aged between 6 and 9 years use the Internet. Their favourite Internet activities during their leisure time are surfing the Internet, viewing websites for children, watching films and videos online. It's not so common that peers in this age communicate via social networks. Girls are more active in social networks than boys. Only 5% of the 6 to 7 years old and 13% of the 8 to 9 years old are a member of a social network community [3]. Furthermore more often, primary school children are invited by their teachers, to use the Internet to do their homework.

2.2 Development of Computer Games for Children

Modern game development is an iterative process [6]: firstly game ideas are generated and formalised, afterwards the game is tested and test results are evaluated. The iterative process has to repeated, if the evaluation indentifies some problems with the game design. A modern game design should have six core elements [18]: challenge, goals, rewards, rules, interactivity, and decision making. Game designers usually distinguish between demographic groups, differ in age and gender [21]. Amongst other factors, specific skills of a demographic group define a user specific game design. The group of 'kids', children aged between 7 and 9 years, are very interested in computer game playing, usually have reading skills, and start logical thought. The challenge for a game designer for those kids is to avoid overwhelming them with too much information (see passage "Children as Users"). For the development of computer games programmer could choose various game engines[1]. A common game engine is the XNA Game Studio 4.0 [15]. Its an programming environment provided by Microsoft, which includes the XNA Framework. It allows an easy game development of small game projects, with a comparative small implementation effort in comparison to standard game implementations. Amongst other functions XNA provides the window managment, the display of 2D and 3D graphics, the handling of user inputs (keyboard, game controller) and the output of sound. The game described in Chapter 3 is developed using the XNA framework because of the easy way of 2D game implementation. In our opinion the use of 2D games with a simple visual design are adaquat to allow learning without distracting children.

Children as Users: The way children think differs a lot from adults. Children in general are used to thinking in a world of fantasy and dream of magic [14]. Furthermore, young children have problems reading long and especially complicated texts [16]. Therefore, texts should be short, easy to understand and the information has to be limited. If the children are overwhelmed with too much information, they will easily feel frustrated, lose their concentration

[1] http://www.indiedb.com/engines, last access: 14. June 2013

on the task at hand [4]. To support the learning process of children the use of multimedia is appropriate [14]. The use of metaphors ensures that the children will be able to understand the complex information. Those metaphors should wrap the complex information (IT security) into something the children know from their daily life [16]. The prototype "InSiKids" realises this metaphorical approach for a target audience of primary school pupils aged between 7 and 9 years `(see Section 3)`. The game prototype was evaluated with test methods adapted to children ("thinking aloud technique", "active intervention method" and "retrospection" method) [9]. But gender particularities must be observed. Research results of the developmental psychology validate developmental differences in cognitive skills between girls and boys [4] `(see Section 4)`. Girls in comparison to boys tend to have better verbal skills (e.g. spelling, writing, linguistic understanding), while boys tend to have an affinity for technics resulting in comparatively more interest in the functionality of technical devices [4].

2.3 Awareness Methods to IT Security Threats for Children

To raise the children's awareness to problems and questions of IT security while using the Internet various procurement methods exist:
Parents and school: IT security is a complex subject, which children mainly learn about by asking their parents and friends (see peers) or while taking computer science / IT classes at school [12, 13]. Most parents arrange specific rules with their children, e.g. time limits for using the Internet [10]. At school the children are often instructed only on how to use computers, but rarely the risks and threats they can encounter [13]. ***Peers:*** Children learn while interacting with their friends (peers). The interaction with qualified others is essential in learning new things [5]. ***Initiatives:*** Many initiatives have been formed to convey the crucial knowledge about IT security to children as well as their parents. Initiatives like the website 'klickSafe'[2] focus on increasing the awareness of Internet users in general to possible threats and conveying the appropriate behaviour in such critical situations. The website 'fragFinn.de'[3] is a ***web search engine*** especially developed for children, which provides a safe way searching the internet. Another approach to convey this subject to children as the target audience is the use of websites containing ***games, comics and quizzes***. This approach is relatively wide spread since it takes advantage of things children like, such as 'Sheeplive'[4]. Even though these subjects have been widely discussed before the stated projects seem to fail to convey the crucial information to their target audience [12, 13]. Therefore, new approaches have to be taken. The e-learning game prototype, introduced in Section 3, is a new approach to teach children IT security threats.

[2] www.klicksafe.de, last access: 14. June 2013
[3] www.fragfinn.de, last access: 14. June 2013
[4] at.sheeplive.eu, last access: 14. June 2013

3 Game prototype: E-learning of IT Security for Children

Based on standard guidelines of infantile learning environments (e.g. paradigm of simplicity, multidimensional stimuli, characters, simple descriptions) the game prototype was developed [16, 14]. Key feature of this prototype are the utilized metaphors for the security threats, which should relate the abstract threads to known everyday situations for the children.

User specific game design: In the game the children become part of the company of hero characters. Every character stands for a mini-game about a particular security threat (chatting, publishing of personal information, malicious codes) (see Table 1). A mascot provides advice and explanation through the game. The text was presented in speech bubbles as in comic or manga with a big font size. The mini-games were keep short to prevent exhaustion.

Fig. 1. Main menu

Fig. 2. Social network game

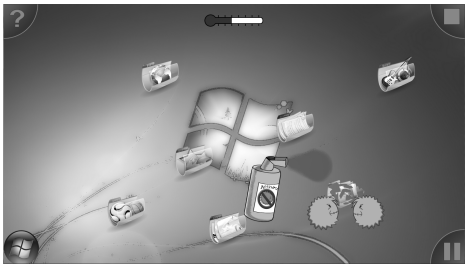

Fig. 3. Virus game

Fig. 4. Chat room game

Technical description of game prototype: The game is implemented with hand drawn two dimension (2D) sprites[5] and backgrounds. In the field of game development sprites are an established technique, which allows the easy creation and handling of geometries in comparison to other techniques. Only point and click user interaction method was implemented to keep the interaction simple. The user interface is designed using the well-known icons from music

[5] In the field of game development a "sprite" is defined as, an 2D image or an anmiation, which is included into a larger game scene [18].

players. If the infantile player successfully finishes a mini game, he earns a medal, which is placed on the character icon button in the main menu. Furthermore, children can easily navigate between the mini games through the corresponding icon of the character or through scrolling with the arrow buttons (see Fig. 1). In the following two sections the creation and realisation of the metaphors is further described. **Design of IT Security Threat Metaphors:** Metaphors are essential for teaching children about abstract security threats and appropriate precautions. Children cannot associate a computer virus, as they do not touch or see (problem of non-suitable warning messages of virus scanner for children) the threat to their security and safety. Therefore, the goal is to develop suitable metaphors to form proper environment for the children to raise their awareness of security threats. In addition, the metaphor must be chosen age-based for maximum learning success but not every metaphor can be realized in an educational game. Using the Internet children are threatened by the same threats as adults but children are more susceptible to threats because of their stage of development. Thus the threats in Table 1 are gathered without limitation. Afterwards, the threats are rated on the basis of media use of children [3, 2] and the following three are chosen to be implemented in the educational game: Social network: publishing of personal data, Chat rooms: strangers in the Internet, and Malicious codes: viruses. **Realisation of Metaphors in the Game Prototype:** To generate meta-phors for threats, the appropriate precautions are collected and set into the age-based context. Around the threat and precaution a metaphor is developed to provide the children with situations they could relate to. At the beginning of the mini games the mascot gives a short introduction to the situation of the character and provides the player with a task. The children are provided with additional information about the consequences of their choices, e.g. if you misplace your party invitations, the party could be over crowded with strangers. The ***social network game*** is designed as visual novel. The character and her conscience embodied by little devil and little angel propose different solutions to place the birthday party invitations in school (see Fig. 2) a. In the ***virus game*** the children should react to a virus infection which was displayed as desktop-icon eating monsters (see Fig. 3). They could try to use a spray to distroy the viruses, but these keep spawning until all data, which is symbolised by the desktop icons being destroyed. The solution to win is to shut down the system. The ***chat room game*** was designed as a memory game. Five characters are presented to the children, so they could memorize them. Afterwards they had to interview a randomly chosen out of the five and then guess which the chosen character was (see Fig. 4).

4 User Study

The educational game prototype "InSiKids" is designed for primary-school pupils aged between 7 and 9. To evaluate the knowledge transfer via the games and the knowledge, which is present prior to the test, an online questionnaire developed

by using the LimeSurvey Framework[6] has been used. By reason of absence of a pre test with a time interval to the main test, only knowledge not learning effects could be measured. ***Test environment:*** The usability test of "InSiKids" took place at the trilingual international primary school in Magdeburg. The children are familar with their school environment so the stress during the test are decreased [16]. The children could use their own personal laptops[7] and had been gaining experience with computers for over a year. The usability test was performed within two third grade classes. The number of pupils was 17 respectively 19 in each class. The results of the test are not representative, because of the small size of the test group (36 pupils). Therefore, only tendencies for knowledge transfer effects for the game prototype could derived from the test results.

Test Realisation: Testing the game prototype was done in different phases: ***Preparation*** was done by installing the game to the children's laptops prior to the test. ***Introduction:*** The team and the prototype were introduced to the children. The operating concept and the test procedure in general were introduced and explained to them. The duration of this phase should not exeed 10 minutes, because children tend to lose their concentration rather quickly. ***Game testing:*** The children could start playing the games. They were free to start with which game they wanted to play the most. The children were only admonished to play every game at least once. This phase lasts for approximately 25 minutes. In the process of testing the team split in groups which were distributed to the two classes. Two team members stayed in each class to answer the children's questions and take notes on their behavior while playing. ***Break:*** With a duration of 15 minutes for recreation. ***Questionnaire:*** With a duration of approximately 20 minutes the children evaluated the games via an online questionnaire. ***Certificates and Conclusion:*** Certificates were handed out to the children, on which they could have their names signed on and thus could join the company of heroes. Mentioning the certificates to the children resulted in a higher motivation to play the games and to learn about the presented IT security subjects.

Test Results: The test results of the evaluation of the educational game prototype using descriptive statistics [8] are presented. The evaluation results are collected by a non-standardized questionnaire, which was self-developed. The questions presented are categorized into four categories: *sociodemographic characteristics* (age, gender) and questions considering *previous knowledge* (use of different technical devices and frequency ot use of the Internet), questions about the *three mini games* (virus, social network, chat rooms), and the *personal consternation* of the test persons concerning IT security threats. The test results were separated into gender groups, which can be reasoned by cognitive differences between girls and boys based on the findings of developmental psychology [4]. 34 children participated in the test. Four data sets were invalid, so 30 valid

[6] www.limesurvey.org, last access: 14. June 2013
[7] www.intel.com/content/www/us/en/intel-learning-series/classmatepc-convertible.html, last access: 14. June 2013

data sets (20 female, 10 male) were evaluated. To provide comparable results for groups differing in size the collected data was normalized. ***Sociodemographic characteristics***: the girls average age was 8,4 years and the boys average age was 8,8 years. ***Previous knowledge:*** At home boys (60%) are predominantly use laptops while girls predominantly use personal computers (50%) instead of other technical devices. The boys (50%, 4-6 times a week) use the Internet more often than the girls (50%, 2-3 times a week). 15% of the girls do not use the Internet while all interviewed boys use the Internet between one and six times a week. In the following the results of the comprehension questions to the ***three mini games*** (virus, social network, chat) are presented. The questions are analysed by using a rating system. Correct answers are coded with a score of 2 (more relevant) or 1 (relevant), and incorrect answers with a score of 0. In case a child gets a score of zero in one group of questions, he could not achieve a higher score. This is based on the assumption, that the metaphors and the communication of the knowledge about IT security threats fail. It should be measured if the teaching of metaphors of IT security threats were successful. Because of the missing pre test, only knowledge effects not learning effects could be measures. Besides the illustration of test results via block diagrams, the data is also statistically analysed [8]. The *independent two-sample t-test* verifies the relationship of the means of two population on basis on the means of two independent samples. In our case, the t-test is used to identify differences between the test results of girls and boys. *Cohen's d effect size* determines the practical relevance of significant results for small samples and is defined as: <0,3 minor, 0,3-0,5 middle, >0,5 major, >0,7 strong. In the mini game ***"virus"*** the children could achieve an overall score of seven (see Fig. 5). The polynominal trend lines in Figures 5 - 7 symbolise the distribution of the sample data. In comparison to the boys, the answers of the girls are more variant. The t-test results and the minor effect size of Cohen's d (0,26) show no indication for a difference between the results of girls and boys. ***"social network"*** game an overall score of seven could be achieved (see Fig. 6). The scores of the girls as well as the boys are accumulated in the middle and higher range. In comparison to the boys in average girls achieve higher scores. The t-test results are not significant. But the middle effect size of Cohen's d (0,73) show an indication for a difference between the results of girls and boys. In the ***"chat"*** game an overall score of four could be achieved. In this game the distribution of the score is relatively homogeneous for both groups (see Fig. 7). T-test and Cohen's effect size (0,21) are not significant.

Discussion: In this section the test results are discussed and our findings are represented. The test goal were to measure if the teaching of metaphors of IT security threats to the assessed children were successful. Due to the missing of a pre test only knowledge effects could be measured instead of learning effects. The results of the virus and the chat game are no significant. Only the results for the social network game indicate a higher knowledge of girls in comparison to the boys. It can be explained by the well designed metaphor of the social network threat, which seem to address the girls more than the boys. Otherwise, in comparison to the boys, girls use more often social networks. This fact can

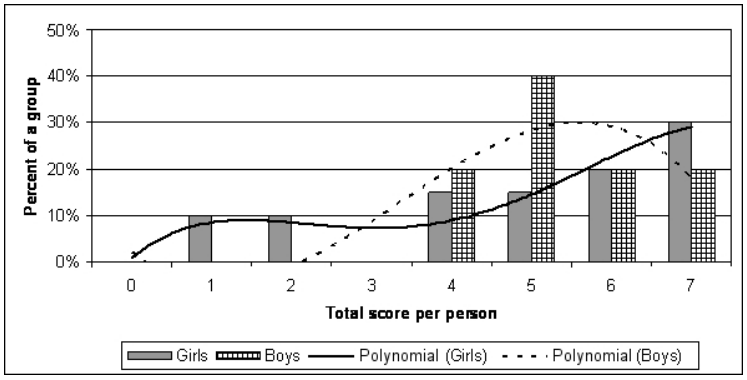

Fig. 5. Test results: computer virus game

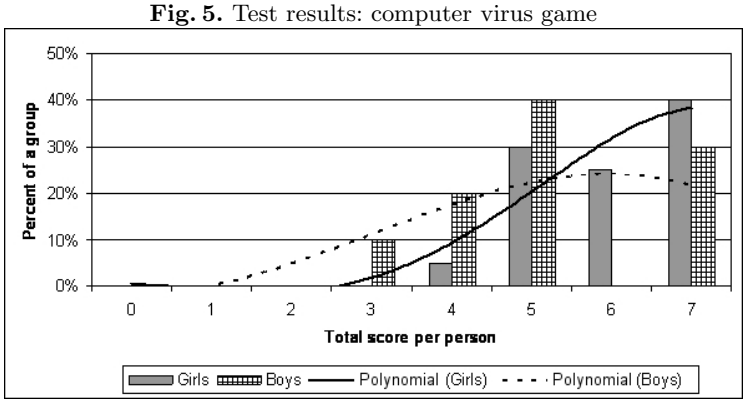

Fig. 6. Test results: social network game

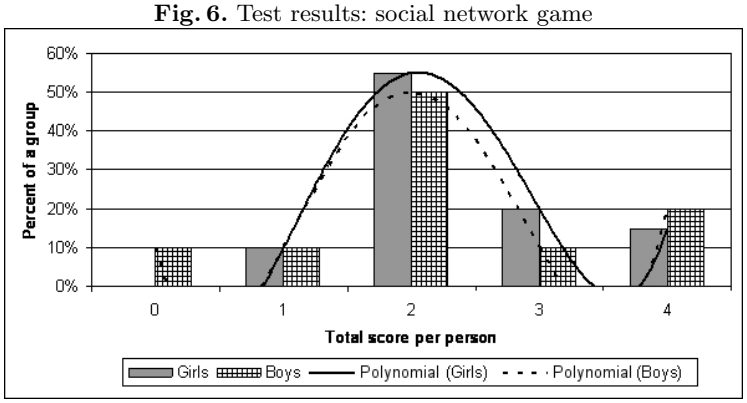

Fig. 7. Test results: chat game

be a reason for girls better results. **Lessons learnt:** ***User study:*** It needs a lot of planning to realise a user study. Enough time has to be planned for preparation, realisation of the test and analysis of the test results. *Test preparing:*

include the search of a suitable test environment (e.g. a school), test persons (e.g. pupils), and assisting personal (e.g. class teachers). Amongst others, the information leaflets (e.g. parent's letter of agreement), the questionnaire, and the technical systems have to be prepared. *Test realisation*: From our experience, it is benificial to have the help of persons, who are familiar with the children. They could facialitate a smooth test process. It's helpful to have sufficient personal for different tasks during the test. In our test only two people had to monitor children's behaviour and to assist pupils by playing the game. *Analysis*: Amongst other things, it has to be determined while preparing the test, what kind of property (e.g. knowledge) should be measured. For example, learning effects could be measured if a certain time period has to be elapsed between a pre test and the main test. The consultation of experts of empirical analysis, such as psychologists, could help to plan an scientific evaluation with representative results.

5 Conclusion and Future Work

The user study with 36 primary school children shows, the metaphors for exemplary IT security threats (virus infection of the computer, inviting somebody in social networks, chatting with strangers) partially support children's way of playful learning. In the future, the e-learning game prototype 'InSiKids' is to be extended and improved in ***design, content and techniques***, respectively. The latter can be done in synchronizing and adding sound effects to the games to enhance the learning effect. Clues to help the children solve the tasks can be extended and a reference page to look up terms and definitions could be implemented. Due to the prototype's mini game structure more games should be easily added. The medals which can be won in the games could be extended to a bronze, silver and gold medal according to how well the children did solving the task. Additionally, new metaphors for existing and other IT security threats are to be designed and relalised in the prototype. The concept of teaching of IT security threats via metaphors is to be extended and assigned for other user groups, e.g. teenagers. Furthermore, the ***test setup and test realisation*** is to be improved. Adapted (e.g. improved questionnaire) and improved test methods are to be used in future user studies. To consider a learning effect future studies and usability tests should be designed for long-term studies.

Acknowledgments

We want to thank the "Dreisprachige Internationale Grundschule Magdeburg", her schoolmaster Irina Horstmann, the teachers, parents and children of the third classes of the year 2012/2013, Sebastian Stellmacher, Dennis Hartmann, Michael Knuth, Volkmar Hinz, and the Acagamics e.V. Jana Fruth is funded by the German Ministry of Education and Science (BMBF), project 01IM10002A. The presented work is part of the ViERforES project [1].

Bibliography

[1] (2013), http://www.vierfores.de/, 18.06.2013

[2] Behrens, P., Rathgeb, T.: JIM-Studie 2011. Medienpädagogischer Forschungverbund Südwest, Stuttgart (2011)

[3] Behrens, P., Schmid, T., König, T., Rathgeb, T.: KIM-Studie 2010. Medienpädagogischer Forschungverbund Südwest, Stuttgart (2010)

[4] Berk, L.E.: Child Development. Pearson, 9 edn. (March 2012)

[5] Fuhrer, U.: Cultivating Minds: Identity as Meaning-Making Practice. Routledge Chapman & Hall (2004)

[6] Fullerton, T., Swain, C., Hoffman, S.: Game design workshop: A playcentric approach to creating innovative games (2008)

[7] Herrmann Laux: Was kinder heute spielen: Anknüpfungspunkte für die schule (2009)

[8] Howell, D.C.: Statistical Methods for Psychology. Wadsworth Inc Fulfillment, 8 edn. (January 2012)

[9] Kesteren, I.E.e.a.: Assessing usability evaluation methods on their effectiveness to elicit verbal comments from children subjects. In: ACM Press, pp. 41–49. ACM (2003)

[10] Kuhlmann, S., Hoppe, T., Fruth, J., Dittmann, J.: Voruntersuchungen und erste Ergebnisse zur Webseitengestaltung für die Situationsbewusste Unterstützung von Kindern in IT-Sicherheitsfragen. In: Informatik 2012, 42. Jahrestagung der Gesellschaft für Informatik. Braunschweig (2012)

[11] Largo, R.H., Beglinger, M.: Schülerjahre: Wie Kinder besser lernen (2010)

[12] Livingstone, S., Haddon, L.: EU Kids Online - Final Report (2009)

[13] Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.: EU Kids Online II - Final Report (2011)

[14] Menzel, W.e.a.: Design and evaluation of security multimedia warnings for children's smartphones (2012)

[15] Microsoft: Xna game studio 4.0 (2012), http://msdn.microsoft.com/de-de/library/bb200104\%28v=xnagamestudio.40\%29.aspx

[16] Nielsen, J.: Children's websites: Usability issues in designing for kids (2010), http://www.nngroup.com/articles/childrens-websites-usability-issues/

[17] Pellegrini, A.D.: The role of play in human development (2009)

[18] Perry, D., DeMaria, R.: David perry on game design: A brainstorming toolbox (2009)

[19] Piaget, J.: Play, dreams and imitation in childhood (1962)

[20] Rubin, K.H., Fein, G.G., Vandenberg, B.: Play. Handbook of child psychology (1983)

[21] Schell, J.: The art of game design: A book of lenses (2008)

[22] Singer, D.G., Golinkoff, R.M., Hirsh-Pasek, K.: Play=learning: How play motivates and enhances children's cognitive and social-emotional growth (2006)