http://dx.doi.org/10.14236/ewic/HCI2016.59

Child-Centered Security

John Dempsey
University of Central Lancashire
Preston, UK
JPDempsey@uclan.ac.uk

Brendan Cassidy
University of Central Lancashire
Preston, UK
BCassidy1@uclan.ac.uk

Gavin Sim
University of Central Lancashire
Preston, UK
GRSim@uclan.ac.uk

Children are spending more time online through the use of digital toys, games and the internet. These activities make children potentially vulnerable to security threats. This position paper puts forward an argument for and against creating a new research discipline in child-centered security, as a fusion of user-centered security and child computer interaction.

Child-centered security, child-centred security, computer security, child computer interaction.

1. INTRODUCTION

Computer security is clearly vital to the economic well-being of a nation. Within the UK, the estimated value of all e-commerce was £557 billion in 2013 (ONS, 2015), and if all this information was suddenly to become insecure then there is a huge risk of damage to the economic viability of, not only a nation, but to the entire world. It is vitally important that we protect our information and computing assets to ensure continued viability.

Children are growing up in a digital age and interact with secure systems from an early age, through schools, networks and shared devices such as tablets. For too long the end-user has been blamed for computer security breaches; yet there are no guarantees that the end-user has received the same level of education as a computer security specialist. User-centered security literature indicates that the problem was not caused by the end-user, but that the security system has been designed incorrectly in the first place (Zurko, 1996). For example, user-centered security literature might argue recent data breaches should not have been allowed to happen in the first place (Hong and Linden, 2012).

Computer security is built into most computer systems; yet computer security isn't the target of most user's task-driven goals. Understanding the goals of the user is important to enhance usability which is defined as the extent to which users can achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (BSI, 2010). Applying usability to computer security could mean: effective computer security is one that prevents security breaches; efficient computer security doesn't stop the end-user being productive; and satisfying computer security does not stop the end-user from achieving their goals.

When the end-user is a child, they have limited experience in which to build security related mental models. They may not understand the consequences of not securing their data, indeed it may not actually be possible to understand a threat that might only appear in the future. As responsible adults we want to protect our children from harm, meaning that children may not develop these mental models in a positive and constructive way.

The field of Child Computer Interaction (CCI) emerged out of HCI through the realisation of the importance of including children in the design of their own technologies and the ineffectiveness of methods used by adults to evaluate children's technologies. Children are the experts in being children, and no matter how hard an adult tries, they are no longer children. On this basis Child-Centered Security should be developed as a separate field of study, where children can inform and develop the security of systems predominantly used by children.

2. USER-CENTERED SECURITY

Children have not been ignored with the user-centered security literature, and as Zurko (2005) states any security mechanism that is incomprehensible and not integrated does not help. This statement is clearly true for both adults and children alike; this statement makes no assumptions about the ability of the user to comprehend, allowing for the different education and life experience of either an adult or a child.

Children understand that they have "special things" that need to be protected (Read and Beale, 2009); and by extension should understand about security in the physical world. They could hide their favourite toy, or sabotage the functionality of a

perfectly good toy to prevent others from playing. If they understand security in the physical world, then why should we consider them any different in the digital world?

One of the core concepts of a user-centered approach is that we should not blame the user. We wouldn't blame the child if they inadvertently removed the brake on a poorly designed pram, and we equally shouldn't blame the child if they expose a vulnerability in poorly designed security software.

3. A NEW DISCIPLINE

Read (2005) described how children are different from adults when using computers, and how they focus on activities, behaviour and concerns. Children usually don't use computers for the same reason as adults, and while they may use the same tools, the way in which they use them may be different. Schechter (2013) described children as posing an adversarial, insider threat. Children are generally not concerned about their own safety and instead focus on what they want to achieve (probably to have fun). The National Curriculum for Computing was updated (Department for Education, 2013) and safety and privacy is now taught at all key stages. It is our responsibility, as adults and as carers for children, to encourage children to become interested and invested in their own safety.

Children protect their special things (Read and Beale, 2009), but unless we study how a child might achieve this, then we are only really attempting to force children to fit in with the adult's idea of a secure system. Thus ignoring the motivational factors for the development of the CCI community.

Read and Cassidy (2012) examined how children created textual passwords and drew up some design guidelines. For any security practitioner this list of design guidelines would stand out as being a poor implementation of computer security. The guidelines would be too easy to take advantage of, and would represent a security weakness. However, not using these guidelines may cause the child to seek alternative solutions, such as writing down passwords or sharing them with others. The solution might actually be to encourage children to start using weaker passwords that can be kept secure, rather than strong passwords that are not secure.

The spectrum of knowledge, skills and abilities across children at different age ranges is wider than that for a typical adult. Children will often act in ways that were not anticipated (Read, 2005), and any computer system designed for children should make an allowance and help the child make constructive progress (where their task might be to accomplish a goal, or to simply have fun); any error messages should be appropriately derived for the child's age and development (Zurko, 2005), yet getting this wrong may cause unwanted consequences.

The spectrum of risks faced by a child is different to that faced by an adult (OECD, 2012). It does not take complex social engineering techniques to trick a child. Depending on the age of the child and their relationship with the adult, if an adult asks a child to do something then they are very likely to do it. Children have different weaknesses than adults, and can easily be tricked into giving away more than they would normally want to. Read and Cassidy (2012) observed a child shouting across the classroom for confirmation on how to spell their password; this type of behaviour introduced different vulnerabilities.

Children are one of the most qualified experts in understanding children. The CCI researcher must interpret data or design computer systems that have been informed by children and then evaluate those computer systems with children (McKnight and Read, 2011). A child-centered security approach would place the child at the centre of the system, and use them as informants to the design and evaluation of the computer system and its security.

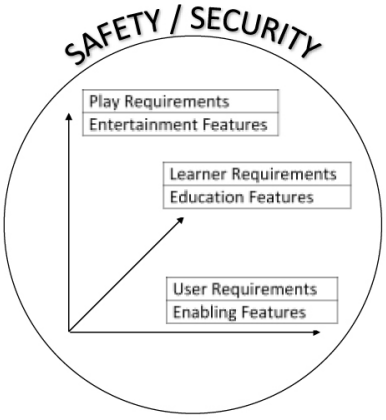

Figure 1: *An example of a potential PLUS model (adapted from Read and Bekker, 2011)*

Not only should children be used as informants into the design of safe and secure computer systems, they should also be used to evaluate those safe and secure computer systems to ensure that they meet their expectations. Discovering the best ways to evaluate computer security for children might only be achieved by applying usability models that have been designed specifically for children. For example, the PLU model is a framework used to map children's activities into a 3-dimensional space of Play, Learning and Use (Read and Bekker, 2011), and a Child-Centered Security approach might adapt such a model to include safety and security techniques (see figure 1).

4. CONCLUSION

Child-centered security should be considered a research discipline in its own right. When we introduce children to technology and computer systems, we are shaping the way that they will use technology for the future. Children are the experts in being children and could contribute imaginative and creative solutions to securing their valuable data and things.

5. REFERENCES

British Standards Institution. (2010). BS EN ISO 9241-210-2010 *Ergonomics of human-system interaction. Part 210: Human-centered design for interactive systems*. London, BSI.

Department for Education. (2013). *National curriculum in England: computing programmes of study*. Available from https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study. (31 January 2016).

Hong, J., Linden, G. (2012). Protecting against data breaches; living with mistakes. *Communications of the ACM,* Vol 55 Issue 6.

McKnight, L., Read, J. (2011). PLU-E: a proposed framework for planning and conducting evaluation studies with children. In: *BCS-HCI '11: Proceedings of the 25th BCS Conference on Human-Computer Interaction*.

Office for National Statistics. (2015). *The impact of e-commerce on the UK economy*. Available from http://www.ons.gov.uk/ons/rel/rdit2/e-commerce-and-internet-use/analysis-at-uk-level/sty-the-impact-of-e-commerce-on-the-uk-economy-.html. (31 January 2016).

Organisation for Economic Cooperation and Development (OECD). (2012). *The Protection of Children Online: Report on risks faced by children online and policies to protect them*. Available from http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf. (10th February 2016).

Read, J. (2005). The ABC of CCI (Child Computer Interaction). *Interfaces* 62: 8-9.

Read, J., Beale, R. (2009). Under my pillow: designing security for children's special things. In: *BCS-HCI '09: Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*.

Read, J., Bekker, M. (2011). The nature of child computer interaction. In: *BCS-HCI '11: Proceedings of the 25th BCS Conference on Human-Computer Interaction*.

Read, J., Cassidy, B. (2012). Designing Textual Password Systems for Children. In: *IDC '12: Proceedings of the 11th International Conference on Interaction Design and Children*.

Schechter, S. (2013). The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button! The Security and Privacy Impacts of Children and Childhood on Technology for the Home. In: *Workshop on Home Usable Privacy and Security*.

Zurko, M. (2005). User-Centered Security: Stepping Up to the Grand Challenge. In: *ACSAC '05: Proceedings of the 21st Annual Computer Security Applications Conference*.

Zurko, M., Simon, R. (1996). User-Centered Security. In: *NSPW '96: Proceedings of the 1996 workshop on New security paradigms*.