FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS OF SOFTWARE IN INFORMATION SECURITY

GARIMA VASHISHTHA

DR. RAJESH PATHAK

HOD Deptt. Of Computer Science, & Engg.

GNIT Institute of Technology,

Gautam Budh Nagar, U.P.

Reseach Scholar, CMJ University, Shillong, Meghalaya

INTRODUCTION

Young people do not tend to use the term cyber bullying', and there are strong norms towards 'seeing the joke' where online behavior is concerned. The context of offline relationships is crucial in deciding whether certain actions online are acceptable or not - for instance, posting 'joke' or embarrassing photos or videos of friends or acquaintances online. The particular implications of online exposure are not significant for young people. They often do not distinguish between doing something embarrassing or harmful to someone and putting an image of this online. The authors conclude:

First, young people conceptualise risk in terms of immediate, quantifiable consequences of behaviour. Young people's concepts of risk are largely formed through the stories in the news media and were negotiated in terms of the likelihood of a negative consequence, including being caught. So, for example, where activities such as plagiarism, activities equating to adult definitions of 'cyberbullying' and lax attitudes to privacy are concerned, young people feel relatively free from consequence, and therefore do not consider such activities to be 'risky'. Second, young people do not reflect on their online behaviour. This extends to young people's lack of awareness of the implications of online exposure of themselves and others, a limited concept of the audience who may be viewing their activities online, and the extent to which they are willing to take information accessed online at face value. Overall, these findings suggest that young people's technical expertise can often exceed their understanding. This is the gap which policy must bridge to ensure that young people are not needlessly putting themselves at risk online and instead can get the most out of what the internet has to offer.

IJAER

CEOP: Online Social Networks 68

Margaret Brennan, 2006. This is described as a "preliminary" report and is based on a series of 16 "stakeholder workshops" held over 4 days. There were both Youth and Adult stakeholders. The observations and conclusions are in line with others. The Report ends, honestly enough: "At present, much of our knowledge on the topic of safeguarding children in social networks is anecdotal rather than empirically-based. Safeguarding interventions will only be effective if they are grounded in a real and evidenced knowledge base - this requires further research to fill existing knowledge gaps on risk factors and possible interventions in social networking environments."

Eurobarometer. : Towards a safer use of the Internet in the EU - a parent's perspective69

This is work commissioned by the EU Safer Internet Program in late 2008. It was conducted by Gallup and covered the use of the Internet and mobile phones by children. The survey scope was limited to *parents* as opposed to children. A total of 12, 750 parents from 27 EU countries was randomly selected. Most interviews were by telephone.

The quantitative aspects of the Report are given above. Below are some of the findings from the more qualitative work:

Concerns and awareness about online risks

The biggest risk in parents' eyes (65%) was that their child might see sexually or violently explicit images on the Internet: 45% were *very* worried.

In terms of inappropriate contact, parents were most worried that their child could become a victim of online grooming (60%); other concerns were that their child could be bullied online by other children (54%) or bullied by others over a mobile phone link (49%). Parents were the least worried that their child might reveal personal or private information when using the Internet: only a quarter said they were *very* worried and 21% were *rather* worried. Parents in France, Spain, Portugal, Greece and Cyprus worried the most that their child might see inappropriate content, make contact with someone intent on grooming or bullying, or reveal personal information. Parents in Denmark, Sweden and Slovakia had the least concern there.

Parents who did not use the Internet themselves, but who said that their child did use it, most frequently answered that they were *very worried* about the risks faced by their child when using the Internet and mobile phones.

Parents answering a question about their 6-10 yearold or their 11-14 year-old more frequently said they were *very worried* about the risks their child faced when using the Internet and mobile phones. *Offering assistance to children in case of problems* Only a minority of the respondents said that when their child asked for their help with an Internet related problem, this was due to: contact online by a stranger (4%), harassment (4%) or bullying online (3%), or the existence of sexually or violently explicit images on the Internet (4%). Almost three out of 10 Dutch parents (28%) and a quarter of the parents in the UK (24%) said that, when their child asked for their help, this was because they had been contacted by a stranger, were bullied or harassed online or saw violently or sexually explicit images online.

Older children, who asked their parents for help, more often did so for any of the reasons listed above (e.g. 7% of the 15-17 year-olds asked their parents for help because they were harassed online compared to 1% of the 6-10 year-olds).

Strategies for parental supervision when children use the Internet

Three-quarters of parents – with a child who accessed the Internet at home – said they always or very frequently talked with their son or daughter about what they had been doing online. A majority of the parents (61%) took care that they – always or very frequently – stayed nearby when their child used the Internet, while one-third said that they sat next to their child when they used the Internet. Parents in almost all Member States were the least likely to regularly check whether their child had a profile on a social networking site (30%) or the messages in their child_s email or IM account (24%).

Parents in the UK and some southern European countries – Portugal, Italy and Spain – were more likely to regularly supervise their child when using the Internet (e.g. stay nearby or sit next to their child) and to check what their child had done online (e.g. check the history file or e-mail account).

Parents in Lithuania and Estonia, on the other hand, were each time among the most likely to answer that they never supervised or checked their child's Internet-related activities. The 15-17 year-olds were subject to less parental supervision than the 11-14 year-olds and the 6-10 year-olds, but this reduction was more noticeable in the supervision of children using the Internet than for the monitoring of children's online activities (e.g. checking the history file or e-mail).

Half of the parents participating in this survey answered that they had installed filtering software on the computer that their child used at home.

Monitoring software was not as popular, but was still used by almost four out of 10 parents (37%). Parents in all of the EU27 Member States most often thought of the police when asked how they would report illegal or harmful content seen on the Internet – 92% gave this response. Four out of 10 parents (38%) would report such content to a hotline set up for this purpose and one-third mentioned non-profit

or other associations. Parents who did not use the Internet were more likely not to know how they would report illegal or harmful content seen on the Internet. For example, almost one-fifth of the parents who did not use the Internet did not know they could report illegal content to a hotline set up for this purpose compared to 12% of the parents who did use the Internet.

Sources for information and advice about safer use of the Internet

Family and friends were the most popular source of information or advice for parents about monitoring and filtering tools and safe use of the Internet: 71% of parents had turned to a friend or family member to discuss Internet safety issues.

Four out of 10 parents had browsed the Internet an found information or advice about safer Internet on various websites, and a similar proportion (36%) Internet Crime Lit Review/Sommer/LSE/p 91 counted on Internet service providers (ISPs) to get such information.

Berkman: Enhancing Child Safety and Online Technologies - Internet Safety Technical Task Force

This is a 2008 US report commissioned by 50 attorneys general from the 50 states of the union. It produced a Literature Review of relevant research in the field of youth online safety in the United States, which documents what is known and what remains to be studied about the issue and a report from its Technology Advisory Board, reviewing the 40 technologies submitted to the Task Force. An interesting feature of the Report is its critique of research methodologies and the way in which statistics may be abused. "The methodology of a study is its most important quality. The size of a sample population matters less than how the population was sampled in relation to the questions being asked. The questions that qualitative studies can address differ from those that can be addressed quantitatively, but both are equally valid and important.

…Presenting statistical findings is difficult, because those who are unfamiliar with quantitative methodology may misinterpret the data and read more deeply into the claims than the data supports. For example, correlation is not the same as causation, and when two variables are correlated, the data cannot tell you whether one causes the other or whether an additional mediating variable that affects both is involved. In presenting the findings of different studies, the Literature Review tries also to provide a roadmap for understanding what these studies mean and also includes some background" The study looks at "sexual solicitation and internet-initiated offline encounters", "online harassment" and "problematic content". Among the findings:

Bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline.

IJAER

o Much of the research based on law-enforcement cases involving Internet-related child exploitation predated the rise of social networks. This research found that cases typically involved post-pubescent youth who were aware that they were meeting an adult male for the purpose of engaging in sexual activity.

o Youth report sexual solicitation of minors by minors more frequently, but these incidents, too, are understudied

o The Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors' exposure. Unwanted exposure to pornography does occur online, but those most likely to be exposed are those seeking it out, such as older male minors.

o Minors are not equally at risk online. Those who are most at risk often engage in risky behaviour and have difficulties in other parts of their lives. The psychosocial makeup of and family dynamics surrounding particular minors are better predictors of risk than the use of specific media or technologies.

o Although much is known about these issues, many areas still require further research. For example, too little is known about the interplay among risks and the role that minors themselves play in contributing to unsafe environments.

REFERENCES

Adam Barth, Collin Jackson, and John C. Mitchell. Robust defenses for cross-site request forgery. In 15th ACM Conference on Computer and Communications Security (CCS), October 2008. Rune Braathen. Crash course in X Windows security, November 1994.

http://www.ussg.iu.edu/usail/external/recommended/Xsecure.html.

Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, and Fran_cois Yergeau. Extensible Markup Language (XML) 1.0 (Fourth Edition), section 4.2.2.

http: //www.w3.org/TR/REC-xml/#sec-external-ent.

The Chromium Authors. Sandbox, 2008.

http://dev.chromium.org/developers, design-documents/sandbox.

Click Quality and Security Teams. The anatomy of Clickbot.A. In Proceedings of HotBots 2007, 2007. Chris Grier, Shuo Tang, and Samuel T. King. Secure web browsing with the op web browser. In IEEE Symposium on Security and Privacy, 2008. Sotiris Ioannidis and Steven M. Bellovin. Building a secure web browser. In Proceedings of the USENIX Annual Technical Conference, Freenix Track, June 2001. Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting browsers from DNS rebinding attacks. In Proceedings of the 14th ACM Conference on Computer and Communications David LeBlanc. Practical Windows sandboxing, July 2007. http://blogs.msdn.com/david_leblanc/

IJAER

Microsoft. Dynamic-link library redirection. http:// msdn.microsoft.com/en-us/library/ms682600.aspx.

Microsoft. Migitating cross-site scripting with HTTP-only cookies. http://msdn.microsoft.com/ en-us/library/ms533046.aspx. Microsoft. Naming a _le. http://msdn2.microsoft.com/en-us/library/aa365247(VS.85).aspx.

Mitre. CVE-2006-7228, 2006.

Mitre. CVE-2007-3743, 2007.

Mitre. CVE-2007-3893, 2007.

Mitre. CVE-2008-3360, 2008.

Niels Provos, Markus Friedl, and Peter Honeyman. Preventing privilege escalation. In 12th USENIX Security Symposium, August 2003.

Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose. All your iFRAMEs point to us. In Proceedings of the 17th USENIX Security Symposium, July 2008.

[20] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, K. Wang, and Nagendra Modadugu.The ghost in the browser - analysis of web-based malware. In Proceedings of HotBots 2007, April 2007. Charles Reis, Brian Bershad, Steven D. Gribble, and Henry M. Levy. Using processes to improve the reliability of browser-based applications. Technical report, 2007. University of Washington Technical Report UW-CSE-2007-12-01.

SecurityFocus. PCRE Regular Expression Library Multiple Security Vulnerabilities, 2007. http://www.securityfocus.com/bid/26346.

Marc Silbey and Peter Brundrett. Understanding and working in Protected Mode Internet Explorer, 2006.http://msdn.microsoft.com/en-us/library/ bb250462.aspx.

Gregory Steuck. XXE (Xml eXternal Entity) attack, October 2002. http://www.securiteam.com/ securitynews/6D0100A5PU.html.

VMWare. Browser appliance. http://www.vmware.

Andy Zeigler. IE8 and Loosely-Coupled IE, March

Tzer-Shyong Chen1, Fuh-Gwo Jeng , and Yu-Chia Liu “Hacking tricks toward security on network environments”, Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies of IEEE

IJAER