Mobile cyber-bullying: A proposal for a pre-emptive approach to risk mitigation by employing digital forensic readiness

Stephen M Serra
Information and Computer Architectures Research Group (ICSA)
Department of Computer Science
University of Pretoria
Email: stephen.serra@gmail.com

HS Venter
Information and Computer Architecture Research Group (ICSA)
Department of Computer Science
University of Pretoria
hventer@cs.up.ac.za

Abstract— The new age of mobile communication brought on by the internet has meant that people now have mobile access to a wealth of information and services. Although the benefits of mobile information access are acknowledged through the empowering influence over its audience, a concern is noted with reference to largely uncensored forums offering mobile communication exchange to children.

The proliferation of mobile technologies available, in conjunction with applications facilitating social networking, has steadily increased the attack surface minors are exposed to in an online environment. Most minors engaging in online activities do so through mobile technologies such as the cell phone. This device, as a consequence of its mobility, offers access to the internet that circumvents controls of supervision. This paper presents an approach that offers an alternative to existing solutions, available to the commercial market, that are driven by static configurations. The proposed solution seeks to avail a state of digital forensic readiness in order to deliver a proactive solution, this is accomplished through risk profiling of a user through usage which dictates the level of protection accordingly. It is suggested that this proposal will benefit children engaging in online interactions through the implementation of proactive strategies.

Keywords-internet, cell phone, children, uncensored forums, cyber bullying, digital forensic readiness

I. INTRODUCTION

Having a profound influence in the lives of most members of a typical family, the internet continues to provide a service that offers a myriad of information as well as communication gateways to all including even the youngest family members.

The risk of online access to minors has steadily increased due to the ever increasing means of accessibility coupled with uncensored content, anonymity and the generation gap between parents and their more computer literate children [1]. Seamless accessibility to the online environment of the internet is made possible by the predominant technology in use by children today, the cell phone. Although a common technology carried by most teens today, the cell phone is not the first mobile technology to cause disruption [2]. Pagers were the mobile technology of choice in the 90's that introduced a mechanism through which harassment could be delivered. While it is evident that some effort in risk reduction has been implemented by mobile network operators in an attempt to curb the risk to underage participants of the network, further work is needed to keep children safe while engaging in online activity, especially with reference to cyber-bullying [3]. Currently parental control systems are only evident in two of the four mobile network operators evaluated. One of the two mobile network operators that do offer parental controls do not address user-to-user messages and access to user-generated content [4]. Measures that have been suggested up to date appear to be directed more at inappropriate content and user-defined blacklists of chat-rooms. There are no 'home-grown' solutions that have been directed by local studies and research. This would lead to solutions that may not be totally effective for the local demographic. A perspective followed in this study follows the premise of a solution that is customized for an individual as opposed to blanket-wide commercial solutions that are generic and equally applied to the subscriber.

Commitment from government on the issue of cybercrime and child-safety was noted with the South African Minister of Communications' media statement on the 16 March 2010 [5],

"Recent reports of children who go missing as a result of being lured through cyberspace criminals posing as 'friends', often resulting in them being murdered is very disturbing and requires a societal response. Police have a duty to lead this crusade in ensuring those perpetrators are brought to book "

The authors are of the opinion that law enforcement involvement will aid in the effectiveness of the proposed solution.

The extent to which children of South Africa are vulnerable to cyber-bullying via cell phone usage is largely unknown. Specific, exploratory research into the extent of how the local

demographic is affected will aid in methods of remediation that are effective, both technologically and educationally. The research is directed at schools of historically disadvantaged individuals in South Africa to gauge the level of exposure brought on by cyber-bullying via the prominent form of mobile technology available, the cell phone. The research further aims to bring to the fore an element of risk management that reduces the risk through the development of a solution motivated by the results of fieldwork as well as both technology and educational directives that will also encompass collaboration with law enforcement.

Law enforcement participation in conjunction with other remediation methods centered on education and technology will work together to provide a proactive solution. Implementing a solution that preempts an attack of cyber bullying, through risk profiling, will provide a means of proactively identifying a threat or threat agent [6] thereby reducing an exposure and resultant impact on the recipient of such an attack. This method will allow law enforcement or other end-recipient of the notification to be made aware automatically allowing necessary actions to follow without having to launch on a reactive basis.

The focus and direction of this study was conceived from an observation that revealed inadequate controls in the protection of children through mobile technology.

II. BACKGROUND

This section commences with what cyber-bullying is and how it is carried out, the types of cyber-bullying that exist and the associated harmful effects of cyber-bullying. Results from Pew Research Centre publications [9] are discussed next with statistics relevant to teens, cellphones and texting.

A. Cyber-Bullying

Cyber-bullying is a manifestation of the ability to communicate anonymously, without fear of reprisal. The ability to project oneself differently in a light that may contrast one's real-life scenario may be beneficial for a timid individual that is bullied in the real-world. This individual may mask their demeanour on-line in order to seek revenge on those individuals for transgressions in the real world. [7]

Cyber-bullying may occur through a number of avenues such as web sites, blogs, discussion forums, chat, instant messaging, voice, or text [8]. This paper focuses on the threat of communication facilitated by cell phone usage directly to the victim, such as instant messaging and short message service (SMS), but takes into consideration the usage pattern of the user or potential victim into consideration.

Willard [8] identified the following types of cyber-bullying:

1. *Flaming*: Angry, rude comments.
2. *Harassment*: Repeatedly sending offensive messages.
3. *Denigration*: Spreading rumours or posting false information of others online.
4. *Outing and trickery*: Disseminating intimate private information or talking someone into disclosing private information which is then disseminated.
5. *Impersonation*: Pretending to be someone else and posting material to damage that person's reputation.
6. *Exclusion*: Intentionally excluding someone from an online group.
7. *Cyber stalking*: Creating fear by repeatedly sending offensive messages and engaging in other harmful online activities.

The harmful effects of cyber-bullying are exacerbated, in comparison to traditional schoolyard bullying, due to the fact that the harassment is continuous and does not stop. The cell phone is a direct portal to the victim due to the close association the victim has with his/her cell phone. The result of a continuous barrage of harassment may lead to the victim suffering serious consequences related to psychological challenges that could also lead to difficulties in later life.

Lenhart [9] indicates in a research report by Pew Research Centre that cell phone texting has become the preferred channel of basic communication between teens and their friends. According to Pew Research Centre, some 75% of 12-17 year olds now own cell phones, up from 45% in 2004. The research report goes on to indicate that one in three teens sends more than 100 text messages a day, or 3000 texts a month. These alarming statistics bring to the fore the mainstream use of this mode of communication and susceptibility to malicious use. Figure 1 by Lenhart [9] reflects the percentage of teens who contact their friends daily by different methods, by age. High percentages are noted for children as young as 12 to 17 years in respect of text messaging and instant messaging. Extensive use must be aligned to adequate controls to ensure non malicious use.

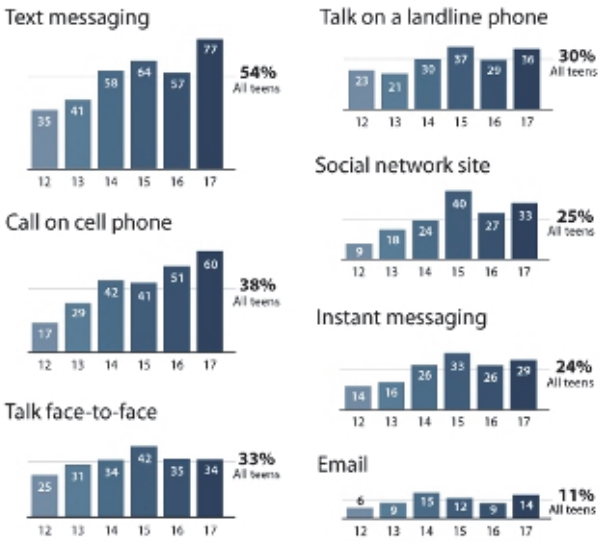

Figure 1 - percentage of teens who contact their friends daily by different methods, by age

III. INDICATORS FOR RISK REDUCTION

This section provides descriptions of why outputs of this research are fundamental to reducing the risk. While it is recognized that full risk elimination is not possible, this paper assumes the perspective that the risk must be reduced to an acceptable level.

A. Expansion of mobile technology available to minors

The rate at which mobile technology is being adopted by children is outstanding [10]. The use of mobile phones has totally revolutionized the concept of interpersonal communications between children. It has also blurred the boundaries between private and public scenarios of communication particularly when combined with social networking forums on the internet [11]. The multitude of possible channels of social interaction are available to anyone with a mobile phone introducing an element of risk that accompanies that first phone bought by a parent for the youngest member of the family. The unprecedented uptake of mobile phones by children has severely increased the potential for security compromise of a child's safety and well-being [12]. Although the provision of technology to children by parents is for the advantages of instant communication, the uninformed parent is missing a crucial factor: the largely unregulated environment that the cell phone provides access to − the internet.

B. Increasing presence of applications providing unregulated, uncensored content

Social networking sites offering real-time interaction are predominately uncensored and unregulated. Some social networking forums openly declare that they are not content providers but rather service providers [13], equating their presence to that of a Post-Office that does not inspect content but rather facilitates the movement of messages. The multitude of children using Mixit [14] and other social networking applications do so unsupervised due to the method of access afforded by mobile telephony and without monitoring by the channel provider. They are, therefore, left unscrupulously vulnerable to cyber-bullying and other threats.

Local research into the problem of cyber-bullying facilitated by mobile technology will yield relevant and effective solutions for the children of South Africa.

The existence of research into the problem area of cyber-bullying via mobile phones gives rise to the next point on the importance of risk reduction: limited research.

C. Limited research on the problem

Although the threat of cyber-bullying has received much attention recently as a result of unfortunate incidents culminating in detrimental consequences, such as the suicide of children [14], the focus still appears to be of a generalized nature with a holistic approach to what it constitutes particularly in South Africa. What is lacking is definitive research into the risk that the local population is facing through the use of the predominant means of communication, i.e. mobile technology. Research is needed to feed real-life data from local sources into the design and development of a solution that can work for the local demographic.

The existence of generic solutions versus demographic specific solutions gives rise to the next point on risk reduction: there is no solution that caters specifically to the local demographic.

D. No solution that caters for the local demographic

Solutions to the problem of cyber-bullying can be addressed from two different perspectives, i.e. education and technology. While there are elements of a solution, educational or technological, that may be common and applicable across population groups there is a need to apply specific techniques that allow for the risk profile of the victim to be factored into the solution considering age and socio-economic background. The risk profile may reveal a different level or manner of technological usage; may have a different understanding of what constitutes risk; have a different or no supporting structure and may perceive and react differently to an attack. A solution that considers the specific demographic with specific risk profile analysis will not only be more effective but also be accepted due to its consideration for the intended audience. The next section explores the proposal.

IV. THE PROPOSAL

The proposed solution will enable a risk determination to be made based on the specific risk profile of the individual user. The resultant output of the risk determination would be an explicit policy governing what the user is exposed to during an operation of communication. A neural network application resident on the mobile phone unit will enable inputs to be accepted for deliberations on ultimate actions to be taken. The learning algorithm for the neural network will be supervised. Input patterns and outputs are depicted in Figure 4 and Figure 5. A fundamental requirement of the solution is to make the operation as seamless and unobtrusive as possible. The objective is to protect the end user and prevent a situation whereby an alternative unprotected cellular phone is used to bypass protective mechanisms. The proposed method of protection will have key elements fed into it that has as its source inputs from the very audience that it is intended for, the children. This approach will ensure that the necessary variables and member functions we define as well as rules that will operate on the variables are relevant and provide the most effective result possible.

The solution will cater for all eventualities that arise as a result of online interaction, stemming from texting, instant messaging and social networking interaction, such as sources of communication requests, communication responses, individuals involved, message content and evaluation of historical message content. Illustrated below, Figure 2 represents a schematic of the model to be implemented.

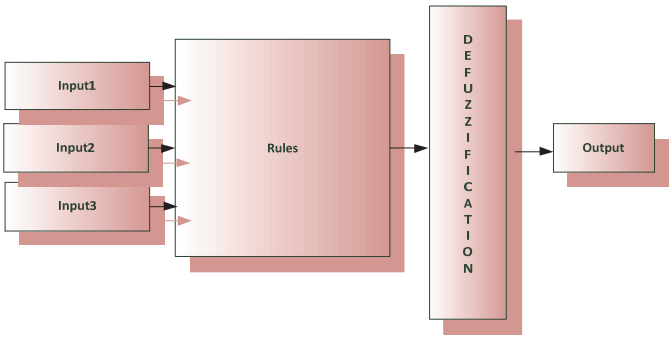

Figure 2 – Risk Model

Inputs to the system are described as follows:

Input 1 – A categorization of the state of security of an individual based on age is depicted below:

Grade 4 – The age of the user is less than 8.

Grade 3 – The age of the user is 8 to 12.

Grade 2 – The age of the user is 13 to 16.

Grade 1 – The age of the user is 17 to 18.

Input 2 – A categorization of online usage as a function of time spent online is described in the following sets: Uselist 1, Uselist 2, Uselist 3. These sets factor into the risk determination process in order to impose or relax applied policy according to certain conditions.

Uselist 1 – Online communication is excessive with 8 hours or more per week.

Uselist 2 - Online communication is moderate with less than 8 hours per week.

Uselist 3 - Online communication is low with less than 2 hours per week.

Input 3 – A categorization of the types of online access and associated risks are depicted in the sets Category1 and Category 2.

Category 1 – Online activity that enables direct communication such as texting, instant messaging and social networking. This form of interaction results in the most potential for harm.

Category 2 – Online activity that facilitates general access to information, no specific risk is associated with this form of access to users aged 16 and older.

Classes of risk output are defined as follows in Figure 3:

Unacceptably High	Critical impact to security as a result of online activity
High	Significant impact to security as a result of online activity
Moderate	Medium impact to security as a result of online activity
Negligible	Little to no impact as a result of online activity

Figure 3 – Classes of Output

The 24 inference rules that operate on the inputs described above are illustrated in Figure 4 and Figure 5.

Category 1	and	Grade 1	and	Userlist1	=	High Risk
Category 1	and	Grade 1	and	Userlist2	=	Moderate Risk
Category 1	and	Grade 1	and	Userlist3	=	Negligible Risk
Category 1	and	Grade 2	and	Userlist1	=	Unacceptably High Risk
Category 1	and	Grade 2	and	Userlist2	=	Moderate Risk
Category 1	and	Grade 2	and	Userlist3	=	Negligible Risk
Category 1	and	Grade 3	and	Userlist1	=	Unacceptably High Risk
Category 1	and	Grade 3	and	Userlist2	=	High Risk
Category 1	and	Grade 3	and	Userlist3	=	High Risk
Category 1	and	Grade 4	and	Userlist1	=	Unacceptably High Risk
Category 1	and	Grade 4	and	Userlist2	=	Unacceptably High Risk
Category 1	and	Grade 4	and	Userlist3	=	Unacceptably High Risk

Figure 4 – Inference rules for category 1 with risk outputs indicated for data provided for input 2 and input 3.

Figure 5 – Inference rules for category 2 with risk outputs indicated for data provided for input 2 and input 3

A further input to personalize the risk profile of the user and aid in the risk determination process will consider personal experiences of users gauging in the different types of online interaction.

V. CONCLUSION

In this paper we have identified and discussed the problem of inadequate controls with reference to the protection of children from cyber-bullying via the cell phone. We have further introduced the concept of dynamic problem resolution based on a proposed plan of a neural net system to dynamically identify a threat based on the risk profile of the individual user in order to resolve conflict situations where dangers are identified. The proposal in this paper is directed at protection to be implemented on the predominant technology in use, the cell phone. Further research should be considered to explore additional threat vectors to the security of users of mobile technologies.

REFERENCES

[1] Great Britain: Parliament: House of Commons: Welsh Affairs Committee, House of Commons, Digital inclusion in WalesL thirteen report of session 2008-2009, report, pg 135.

[2] Samuel C. McQuade, James P.Colt, Nancy B.B. Meyer, "Cyber-bullying: protecting kids and adults from online bullies", 2009, pg 92.

[3] Sameer Hinduja, Justim W.Patchin, "Bullying beyond the schoolyard: preventing and responding to cyberbullying", 2009, pg 5..

[4] MTN, "MTN Parental Control", 2008, http://www.mtn.co.za/MTNServices/MTNPersonalSafety/Pages/MTNParentalControl.aspx

[5] South African Police Service, "Protection of Children Against Cyber Crime A Govt Priority", 2010, http://www.saps.org.za/dynamicModules/internetsite/newsBuild.asp?myURL=959

[6] Peter Sloot, "Computational science—ICCS 2003 international conference, Part4", 2003, pg 610.

[7] Terri Bregeut, "Frequently asked questions about cyberbullying", 2007, pg 20.

[8] Nancy E.Willard, "Cyberbullying and Cyber threats – Responding to the challenge of online social aggression, threats, and distress", 2007, pg 281.

[9] Amanda Lenhart, "Teens,Cellphone and Texting", "Text Messaging Becomes Centerpiece Communication", 2010, http://pewresearch.org/pubs/1572/teens-cell-phones-text-messages

[10] Susan Brookes-Young, "Teaching With the Tools Kids Really Use Learning With Web and Mobile", 2010, pg 15.

[11] Serap Kurbanoglu, Umut Al, Phyllis Lepon-Erdogan, Yasar Tonta, Nazan Ucak, "Technological Convergence and Social Networks in Information Management", 2010, pg v.

[12] Norton Symmantec, "Cyber bullying-Anti social behaviour online", March30,2007,http://us.norton.com/library/familyresource/article.jsp?aid=pr_cyberbully

[13] Mixit, "Content and use policy, guiudelines and position statement", 2011, http://www.mixit.com/content.ap/en/legal_content

[14] Mixit, "Mobile Chat", 2011, http://www.mixit.com