TOWARDS RISK BASED PREVENTION OF GROOMING ATTACKS

Dimitrios Michalopoulos and Ioannis Mavridis
University of Macedonia, Thessaloniki, Greece

Keywords: Risk modeling methods, Grooming detection.

Abstract: The increasing incidents of children sexual exploitation through cyberspace demand for proper protection with technological defense mechanisms. This paper aims to present and evaluate methods and tools that are appropriate towards the prevention of child sexual abuse through Internet based communications. Attacking categories and strategies that predators follow are analyzed and modeled. Moreover, a comparative review of existing risk modeling methods, which is based on a set of proposed criteria, is presented. This comparison results in the conclusion that only two of the reviewed risk modeling methods can be adapted on the intended grooming attack detection system: Bayesian and Markovian. The proposed approach is concluded with a discussion on particular methods and tools for accurate attack probability calculation.

1 INTRODUCTION

During recent years Internet has been growing rapidly. Along with the World Wide Web online communication forms has grown as well. Chat rooms, instant messaging IM, social networks like facebook and MySpace are becoming very popular among children and teenagers. The spend lot of time on these online communities talking with friends, classmates or strangers. At the same time many incidents of children sexual exploitation (grooming attacks) are reported (Subrahmanyam *et al.* 2006). Parents are very concerned about how safe their children are while spending hours on the internet talking on these modern communication forms. In parallel, as they are older they do not have the proper knowledge and experience for protecting their children properly.

In section 2 the issues of Internet related hazards for youth are analyzed and modeled. A comparative review of existing risk modeling methods is presented and discussed in section 3. And the paper concludes with a discussion on methods and techniques for accurate grooming attack probability calculation.

2 PROBLEM ANALYSIS

The hazards that children are exposed to while talking online vary through age and sex and can be divided into three main categories: (a) cyberbullying, (b) sexual exploitation or grooming and (c) exposing to illegal material.

Cyberbullying refers to all kind of attacks that terrify a young user with threats for his/her life, parents and friends (Bauman 2007); (Finkelhor and Ormrod 2000). The most usual types of cyberbullying are (Bauman 2007):

- Sycophantic defamation
- Assaulting and abusive messages
- Menace against life
- Social exclusion from online communication networks

Sexual exploitation or grooming attacks are performed by people who feel sexual attracted to children using modern communication methods for victim exploitation (Dean 2007). The research that has been published on this area has shown the there are similarities on grooming strategies (Subrahmanyam *et al.* 2006); (O'Connell 2003); (Stanley 2001); (Krone 2005). The types of grooming are (O'Connell 2003):

- Forming a "love" relationship
- Cyber-rape
- Fantasy enactment

Michalopoulos D. and Mavridis I. (2010).
TOWARDS RISK BASED PREVENTION OF GROOMING ATTACKS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 217-220
DOI: 10.5220/0002986702170220

Exposing to illegal material includes many types of images, video, music. Frequently, children are exposed to problematic materials motivated by predators or their own curiosity. Indeed, this category cannot be modeled: The World Wide Web is a huge source of information and children can search for inappropriate material not necessary motivated by a third person.

Figure 1 bellow presents the IM and Chat attack tree that categorizes attacks on children through internet communications:

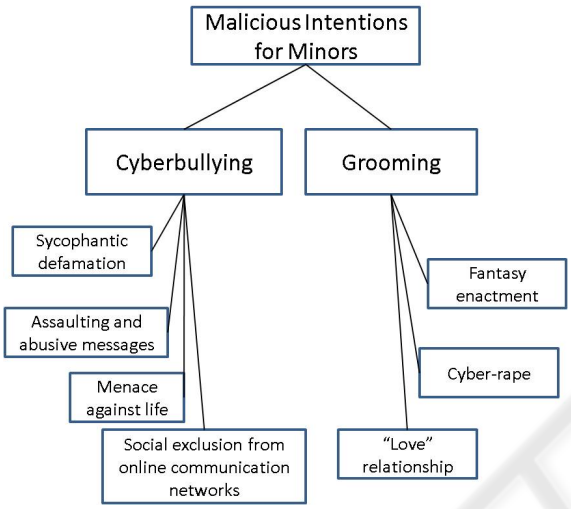

Figure 1: IM and Chat attack tree.

In this paper most of the effort is focused on grooming attacks for two reasons: At first grooming affects on children are more important and secondly cyberbullying incidents are more difficult to be detected and analyzed.

The first step for preventing grooming incidents is the analysis of how predators act and which their aims are. Similarly, O'Connell (2003) investigated grooming incidents and indicated specific stages that predators follow to perform an attack: The friendship stage, the relationship stage, the risk management stage and the sexual stage. The final one, sexual stage, includes three categories of attack as they are analyzed previously and presented at the attack tree of figure 1. For simplicity reasons the three initial stages before the sexual stage, friendship, relationship and risk management stage, are merged in one: the risk management stage including predator's preliminary actions before an attack. The possible transitions between the above stages are depicted in the state-transition diagram of figure 2, based on the published research work (Subrahmanyam *et al.* 2006); (O'Connell 2003); (Stanley 2001); (Krone 2005).

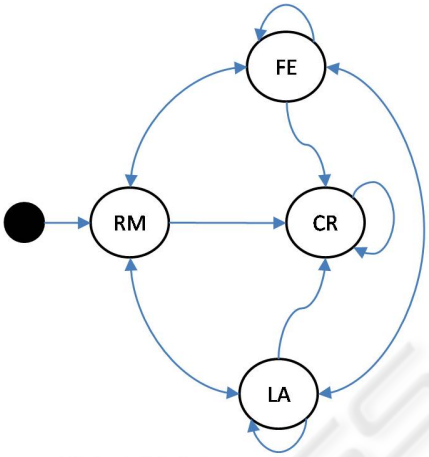

Figure 2: Grooming Attack state-transition diagram.

3 COMPARATIVE REVIEW OF RISK MODELING METHODS

The potential system detects grooming attacks and sends a warning signal in case of attack detection. Indeed, the decision of sending a warning signal or not is crucial. In case of a false positive (of false grooming attack detection with warning signal transmission) the system becomes irritating. Similarly, in case of a false negative (of grooming attack incident that was not identified) the consequences can be catastrophic for the minor user. Therefore, the decision making algorithm of the potential grooming attack detection system is going to decide if a warning signal will be send or not through a risk modeling process.

Indeed, which one of the existing risk modeling methods is proper for grooming attack detection? How risk modeling methods can be implemented on grooming detection? Which are the criteria for such an effort? Towards a risk based grooming attack prevention the following criteria are specified and proposed based on the specific needs of grooming attack detection and the published research on this area (Subrahmanyam *et al.* 2006); (O'Connell 2003); (Stanley 2001); (Krone 2005):

- C1.Memory of the previous stages is required. The performing of a grooming attack is not based only in present stage but is related to

Table 1: Comparison of Risk Modeling Methods.

	C1	C2	C3	C4	C5
Block Diagram	No	Yes	No	Yes	Towards
Attack Tree	No	Yes	No	Yes	Towards
Master Logic Diagram	No	Yes	No	Yes	Towards
Event Tree	No	Yes	No	Yes	Towards
FMEA - FMECA	Yes	Yes	Yes	Yes	Towards
Bayesian Network	Yes	No	Yes	Yes	Both
Markov Diagram	Just for the previous	No	Yes	Yes	Both
Hidden Markov Model	Just for the previous	No	Yes	No	Both
Kalman Filter	Just for the previous	No	Yes	No	Both

previous ones.

- C2.There are component dependencies – items are not physically independent as the presence of one stage is depended on the previous one.
- C3.The approach is probabilistic-quantitative. The decision making algorithm about sending or not a warning signal demands for probabilistic approach
- C4.The present state should be clear. The clearance of the present state is crucial for accuracy in attack probability calculations.
- C5.The attack flow is both towards and backwards. The attack flow is not precise, the predator may return to the previous stage, stay more type and then perform a different type of attack.

What follows is a brief review of the existing risk modeling methods with pros and cons for each one:

Block Diagram Method. This method usually approaches the physical arrangement of the items (Modarres *et al.* 1999).

Attack tree method. This method is widely used in information systems and software engineering.

Master Logic Diagram. It is mostly used in large and complex systems with several autonomous subsystems (Modarres *et al.* 1999).

Event Tree method. This method underlines the discrete states of a system. It is suitable in cases where the attack depends on the chronological order of events (Modarres *et al.* 1999).

The above three methods, called Logic trees (Block Diagram, Attack tree, Master Logic Diagram, Event Tree), are based on Logical or Qualitative evaluation (Boolean) evaluation. However, this approach is not suitable as the decision algorithm demands for probabilistic approach. Methods that are analyzed above are more focused on probabilistic – quantitative approach:

Failure Mode and Effect Analysis - FMEA. Failure Mode and Criticality Analysis - FMECA (Bouti and Kandy 1994).

Bayesian Network. This is a very powerful mathematical model for probability calculation (Krause and Clark1993).

Markov Diagrams. This model is widely used in economics, computer science, assurance etc. In many cases it is used in computer science as well. It is a stochastic method for prediction sequences of events and analyses the probability of each event to occur (Kemeny and Snell 1976); (Ayyub 2003).

Hidden Markov model. (HMM) It is similar to Markov one with the difference that the present state is unobserved (Kemeny and Snell 1976).

Kalman Filter. Similar with the Hidden Markov model, is the Kalman filter, developed by Kalman (1960).

Table 1 presents a synopsis of all above methods and how they are matching the predefined criteria. The comparison denotes that two methods match the defined criteria: Bayesian and Markovian. Indeed, the implementation of the Bayesian demands for the calculation of conditional probabilities for the transmission in each stage. Similarly, the implementation of the Markovian demands for the calculation of the transmission matrixes for each transmission.

The basic challenge is how these transmission-conditional probabilities can be calculated accurately. The proposed method for these calculations is the stochastic simulation (Modarres *et al.* 1999). The analysis of a large number of grooming incidents will lead to accurate estimations about the transmission probabilities. These

grooming incidents can be found for example on the web site www.perverted-justice.com or from live process where the researcher can pretend a minor user through chat room or IM conversations. The categorization among the attack categories will be achieved through keyword identification. Dialog analysis will indicate basic keywords that indicate the presence in specific attack stage.

4 CONCLUSIONS

The implementation of a grooming attack detection system demands for deep analysis of the methodologies that predators follow. Besides, the decision making algorithm about sending or not a warning signal, leads to a probabilistic approach for risk modeling. In this paper, most of the existing risk modeling methods are analyzed and compared according to a set of proposed criteria and in order to be implemented on the intended grooming attack detection system. Bayesian and Markovian methods seem to match the criteria. However, the implementation of each method demands for proper conditional-transmission probability calculation. For this purpose, stochastic simulation through dialog analysis is selected for use, in a large number of known grooming incidents. This dialog analysis should also include the categorization of captured dialogs into various attack categories.

The basic advantage of the intended grooming attack detection system is instant warning. The system analyzes the captured dialogs, calculates the probability of grooming attack and then decides whether to send a signal or not. Thus, parents can be warned about a possible danger on time and make all the necessary actions to prevent any catastrophe.

REFERENCES

Ayyub, B., 2003 Risk Analysis in Engineering and Economics Taylor & Francis Ltd 2003 ISBN 1584883952

Bauman, S., 2007 CyberBullying: a Virtual Menace, National Coalition Against Bullying, Melbourne, Australia,www.ncab.org.au/Assets/Files/Bauman,%20S.%20Cyberbullying.pdf accessed October 2009

Bouti A, Kadi A. D., 1994 A State-of-the-art review of FMEA/FMECA *International Journal of Reliability, Quality and Safety Engineering*, vol1 pp.515-543

Dean, S., (2007) Sexual Predators: How to recognize them on the internet and on the street - how to keep your kids away, Silver Lake Publishing.

Finkelhor, D. and Ormrod, R., 2000 Characteristics of Crimes against Juveniles, Juvenile Justice Bulletin, pp. 1-11.

Kalman, R. E., 1960 The Seminal Kalman Filter Paper http://www.cs.unc.edu/~welch/kalman/kalmanPaper.html accessed October 2009

Kemeny, J. G. and Snell, J. L., 1976 Finite Markov chains, Springer-Verlag, ISBN: 978-0-387-90192-3

Krause, P., Clark, D., 1993 Representing Uncertain Knowledge: An Artificial Intelligence Approach, *Springer*, 1 edition, ISBN-10: 0792324331

Krone, T., 2005 Queensland Police Stings in Online Chat rooms no. 301, Australian Institute of Criminology www.aic.gov.au/documents/B/C/E/%7BBCEE2309-71E3-4EFA-A533-A39661BD1D29%7Dtandi301.pdf accessed October 2009

Madan, B. B., Gogeva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S., 2002 Modeling and quantification of security attributes of software systems, Dependable Systems and Networks, *Proceedings of International Conference on Dependable Systems and Networks* vol., no. pp. 505-514

Modarres, M., Krivtsov, V., Kaminskiy, M., 1999 Reliability Engineering and Risk Analysis, Taylor & Francis Ltd New York 1999 ISBN 0824720008

O'Connell, R., (2003) A typology of child cybersexploitation and online grooming practices, Cyberspace Research Unit, University of Central Lancashire (UK), http://image.guardian.co.uk/sys-files/Society/documents/2003/07/24/Netpaedoreport.pdf accessed October 2009

Rish, I., 2001 An empirical study of the naive Bayes classifier IJCAI 2001 *Workshop on Empirical Methods in Artificial Intelligence*

Stanley, J., (2001) Child abuse and the Internet, Australian Institute of Family Studies, Melbourne, http://aifs.org.au/nch/pubs/issues/issues15/issues15.pdf accessed October 2009

Subrahmanyam, K., Smhel, K. and Greenfield, P., 2006 Connecting Developmental Constructions to the Internet: Identity presentation and Sexual Exploration in Online Teen Chat Rooms, National Science Foundation Grant

Taylor, C., Krings, A., Alves-Foss, J., 2009 Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening, http:// www.csds.uidaho.edu/papers/Taylor02a.pdf accessed October 2009