Volume 2, Issue 2, February 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fuzzy Logic based Risk model for SMS Threats in 3G Systems

Mr. Mohammad Islam*
Department of Computer Science & Engineering
Galgotia College of Engg. & Tech., Gr. Noida, India

Prof. Vineet Kumar Verma
Department of Information Technology
Noida Institute of Engg. & Tech., Gr. Noida, India.

Abstract— **Risk Analysis is a key component on the path to developing a risk model for a system. Risk Analysis enables the user to balance security against cost by understanding specific risks to the system as a whole from threats to the availability, integrity and confidentiality of its assets. Risk is the probability of loss in a system. The basic goal of risk analysis is to compute an overall level of risk that can serve as a basis of decision-making or for initiating a countermeasure. An effective method for combination of risk value would be to use a fuzzy logic approach to compute overall risk. This can be used for the combination of risk values at several stages of the risk analysis process. The research of this study is focused on the security framework of 3G mobile systems, and it is very significant to construct the secure fuzzy logic based risk model against security threats in 3G systems.**

Keywords— **Risk; assessment; fuzzy logic; security; 3G; model.**

I. INTRODUCTION

Risk analysis primarily has the following goals:

1. To determine the actual exposure of the system to risk, with the aim of rectifying the deficiencies
2. To document that risk analysis was carried out in a responsible and accountable manner and give formal proof of the amount of risk the system is exposed to. This may be part of the security requirement of the organization or a partner of the organization.

During the process of risk analysis it is very important to identify the attributes of a threat. These include:

- Attacker's goals – what type of damage does the attacker seek?
- Degree of motivation – how strongly does the attacker want to cause damage?
- Capabilities – what can the attacker do?
- Resources – how much effort can the attacker afford to invest?

II. APPROACHES TO RISK MODELING

There are two basic approaches to risk modeling.

A. Incremental Approach

In this approach, the user is placed in the active role. The user begins use of the system with a very rudimentary model in place. The rudimentary model may be constructed by using information that is already in place in the system or by asking the user some very basic questions. As the system is used the model is evolved. As the user uses the system, she may be presented with questions that help in the evolution of the model. But the user does not have to ever sit at once and answer a huge list of questions. In the rudimentary stages the decisions made by the system may not be perfect. It may be over conservative in computing the risk or may suggest more drastic countermeasures than necessary. But then the principle 'Better safe, than sorry' applies. The inferences drawn by the risk model may be more protective than they should be. However as the model matures with use of the system the model makes decisions that are more informed and more accurate. Thus, the system constantly learns and the accuracy of the model improves with time. It also puts the user in control and allows her to control the evolution of the model.

B. All-at-once Approach

In this approach, an attempt is made to construct the complete model before the use of the system can begin. All information that is required must be gathered before the model can be constructed. The user may be asked a large list of questions, on the basis of which the risk model is constructed. There is no refinement of the model as the system is used. The model remains fixed throughout the existence of the system.

III. BASIC RISK ASSESSMENT METHODOLOGY

The basic steps in the risk assessment methodology are as follows:

1. Define what constitutes the system, that is, identify the components that make up the system as a whole
2. Identify the different assets in the system
3. Identify the threats that the system is exposed to
4. Identify the vulnerabilities in the system.
5. Identify existing safeguards in the system

6. Determine the attributes of the assets and the threats.
7. Combine the information about the assets, threats and vulnerabilities to compute the risk to an asset due to a threat and combine that to compute an overall value of risk to that asset.
8. Combine the threats to the various assets to compute an overall risk value for the system.

IV. FUZZY LOGIC BASED RISK MODEL FOR SMS

A. *Fuzzy Sets and Risk Modeling*

Fuzzy systems, including fuzzy logic and fuzzy set theory, provide a rich and meaningful addition to standard logic. The mathematics generated by these theories is consistent, and fuzzy logic can be a generalization of classic logic. The applications that may be generated from or adapted to fuzzy logic are wide-ranging. Fuzzy logic provides the opportunity for modeling of conditions that are inherently imprecisely defined, despite the concerns of classical logicians. Many systems may be modeled, simulated, and even replicated with the help of fuzzy systems, especially systems that require human reasoning itself. Thus the risk model for SMS messages in cellular phones with its inherent fuzziness and element of human reasoning is an ideal candidate for application of fuzzy logic.

B. *Calculation of Risk*

1) *Fuzzy Sets for Risk*

The model measures risk to an asset on a scale of 0 to 5 with 0 being least risky and 5 being most risky. The model categorizes risk into the following fuzzy sets:

TABLE I. FUZZY SETS

Risk	Fuzzy Set
None	Fuzzy value about 0
Very Low	Fuzzy value about 1
Low	Fuzzy value about 2
High	Fuzzy value about 3
Very High	Fuzzy interval [4, 5]

The membership functions of these fuzzy sets are as shown below:

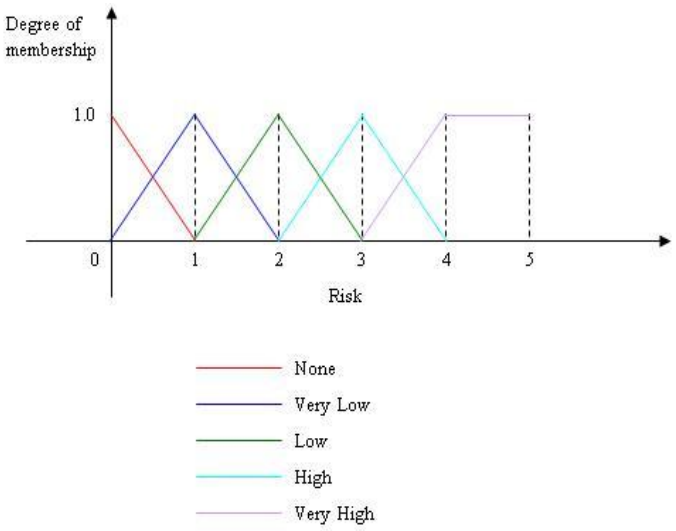

Figure 1. Membership functions for fuzzy Sets for Risk

2) *Countermeasures*

The counter measures available to a system to counter the risk due to a threat are as follows:

a) Reject:

This is the most drastic and conservative counter measure. It is applied when the message is thought to pose the gravest risk to the system, possibly threatening to render the phone unusable or threatening loss of PIM data stored in the cellular phone. It involves simply discarding the SMS message or refusing to accept it when it is delivered to the cellular phone by the cellular network.

b) Quarantine:

This is slightly less conservative than the measure described above. The received message is not rejected outright but is isolated in a sandbox. The user may after taking all the required precautions attempt to access the message or seek the assistance of a technical expert.

c) Queue:

This counter measure involves simply queuing the message for the user. The user is not instantly notified. But an icon or message may be displayed on the cellular phone to indicate that a message has been queued. This approach would be appropriate when the threat is to the privacy of the user. For example, if the user is in a meeting and does not wish to be disturbed by unimportant messages, the messages could be queued for the user to access once she has finished with the meeting. When the user checks her cellular phone after the meeting, a visual indication on the display of the device will indicate that one or more messages have been queued and the user can then read those messages.

d) Accept:

This measure is chosen only when the SMS message presents minimal risk to the system. The SMS message is accepted and the user is notified of its receipt.

3) *Calculation of Risk to Cellular Phone Usability*

Risk to cellular phone usability is calculated depending on the set of rules specified in the table below:

TABLE II. RISK TO CELLULAR PHONE USABILITY

Risk to Cellular Phone Usability		**Capability**	
		Cellular Phone	**Computer**
Degree of Motivation	Family	None	None
	Friend	None	None
	Colleague	None	Very Low
	Acquaintance	Low	High
	Competitor	High	Very High
	Enemy	High	Very High

For example, if the degree of motivation is a member of the fuzzy set 'Competitor' and the capability is a member of the fuzzy set 'Computer', the risk to the cellular phone usability will be a member of the fuzzy set 'Very High'. The membership of the risk in the fuzzy set 'Very High' is the minimum of the membership of the degree of motivation in the fuzzy set 'Competitor' and the membership of capability in the fuzzy set 'Computer'.

The value of degree of motivation can result in membership in up to two fuzzy sets for degree of motivation. Similarly, the value of capability can result in membership in up to two fuzzy sets for capability. Combination of these two possibilities for each attribute can result in four distinct results for risk. The fuzzy set representing overall risk is the union of the four individual results. It is necessary to defuzzify the resulting fuzzy set for risk to obtain a representative value for risk. This model chooses the center of gravity of the resulting fuzzy set to be the value that represents the risk to the cellular phone usability due to the incoming SMS message.

The system then selects the counter measure to counter the risk on the basis of the computer risk value using the following table:

TABLE III. COUNTERMEASURE FOR CELLULAR PHONE USABILITY

Risk Value Range	**Countermeasure**
[0, 1)	Accept
[1, 2)	Quarantine
[2, 5]	Reject

4) Calculation of Risk to Data/Information on the Cellular Device

Risk to data/information on the cellular device is calculated depending on the set of rules specified in the table below:

TABLE IV. RISK TO DATA/INFORMATION ON THE CELLULAR DEVICE

Risk to Data/Information on the Cellular Device		**Capability**	
		Cellular Phone	**Computer**
Degree of Motivation	Family	None	None
	Friend	None	None
	Colleague	None	Very Low
	Acquaintance	Low	High
	Competitor	High	Very High
	Enemy	High	Very High

For example, if the degree of motivation is a member of the fuzzy set 'Acquaintance' and the capability is a member of the fuzzy set 'Computer', the risk to the cellular phone usability will be a member of the fuzzy set 'High'. The membership of the risk in the fuzzy set 'High' is the minimum of the membership of the degree of motivation in the fuzzy set 'Acquaintance' and the membership of capability in the fuzzy set 'Computer'.

The value of degree of motivation can result in membership in up to two fuzzy sets for degree of motivation. Similarly, the value of capability can result in membership in up to two fuzzy sets for capability. Combination of these two possibilities for each attribute can result in four distinct results for risk. The fuzzy set representing overall risk is the union of the four individual results. It is necessary to defuzzify the resulting fuzzy set for risk to obtain a representative value for risk. This model chooses the center of gravity of the resulting fuzzy set to be the value that represents the risk to data/information on the cellular device due to the incoming SMS message.

The system then selects the counter measure to counter the risk on the basis of the computer risk value using the following table:

TABLE V. COUNTERMEASURE ON CELLULAR DEVICE

Risk Value Range	**Countermeasure**
[0, 1)	Accept
[1, 2)	Quarantine
[2, 5]	Reject

5) Calculation of Risk to Right to Privacy

This calculation is performed only if the user has switched the device to silent mode. This indicates that the user wishes to protect 'Right to Privacy' as an asset and wants it to be included in the computation of risk. Risk to right to privacy is calculated depending on the set of rules specified in the table below:

TABLE VI. RISK TO RIGHT TO PRIVACY OF THE USER

Risk to Right to Privacy of the User		**Capability**	
		Cellular Phone	**Computer**
Degree of Motivation	Family	Low	Low
	Friend	Low	High
	Colleague	High	High
	Acquaintance	Very High	Very High
	Competitor	Very High	Very High
	Enemy	Very High	Very High

The value of degree of motivation can result in membership in up to two fuzzy sets for degree of motivation. Similarly, the value of capability can result in membership in up to two fuzzy sets for capability. Combination of these two possibilities for each attribute can result in four distinct results for risk. The fuzzy set representing overall risk is the union of the four individual results. It is necessary to defuzzify the resulting fuzzy set for risk to obtain a representative value for risk. This model chooses the center of gravity of the resulting fuzzy set to be the value that represents the risk to right to privacy due to the incoming SMS message.

The system then selects the counter measure to counter the risk on the basis of the computer risk value using the following table:

TABLE VII. COUNTERMEASURE FOR RIGHT TO PRIVACY

Risk Value Range	**Countermeasure**
[0, 1)	Accept
[1, 4)	Queue
[4, 5]	Reject

6) Calculation of Risk to Right to Avoid Unnecessary Billing

Calculation of Risk to Right to Avoid Unnecessary Billing This calculation is performed only if the user has exceeded the allocated quota of messages for this billing cycle. Once the system detects that the user has exceed her allocated quota, it begins to protect the 'Right to Avoid Unnecessary Billing' as an asset and includes it in the computation of risk. Risk to right to avoid unnecessary billing is calculated depending on the set of rules specified in the table below:

TABLE VIII. RISK TO RIGHT TO AVOID UNNECESSARY BILLING

Risk to Right to Avoid Unnecessary Billing		**Capability**	
		Cellular Phone	**Computer**
	Family	None	Very Low
Degree of Motivation	Friend	Low	Low
	Colleague	Low	High
	Acquaintance	High	Very High
	Competitor	Very High	Very High
	Enemy	Very High	Very High

The value of degree of motivation can result in membership in up to two fuzzy sets for degree of motivation. Similarly, the value of capability can result in membership in up to two fuzzy sets for capability. Combination of these two possibilities for each attribute can result in four distinct results for risk. The fuzzy set representing overall risk is the union of the four individual results. It is necessary to defuzzify the resulting fuzzy set for risk to obtain a representative value for risk. This model chooses the center of gravity of the resulting fuzzy set to be the value that represents the risk to right to avoid unnecessary billing due to the incoming SMS message.

The system then selects the counter measure to counter the risk on the basis of the computer risk value using the following table:

TABLE IX. COUNTERMEASURE TO AVOID UNNECESSARY BILLING

Risk Value Range	**Countermeasure**
[0, 1)	Accept
[1, 4)	Queue
[4, 5]	Reject

7) Role of the User in Configuration of the Model

The model puts the user in an active mode and allows her to configure the model as it suits her best. The table mappings above are suggested values. The user can modify the tables to create a customized model. However care must be taken while reconfiguring the model because it is possible to drastically reduce security and increase system vulnerability by using spurious value in the mapping tables. This design allows the advanced user to experiment with different configurations and use what suits her best. However naive users may be better off using the default configuration of the model.

V. CONCLUSIONS

This study explains the model which emphasizes on risk analysis and assessment. This model uses fuzzy sets to explain and anaylse various factors and variables which are reasons for security threats of SMS in 3G system networks. It explains the different possible attacks on cellular systems, which include SIM cloning, eavesdropping, location tracking, SMS ping, SMS denial of service, authentication denial of service and SMS spam. It shows that the existing security schemes do not provide adequate security and that there is a need to develop new mechanisms that are better suited to the wireless environment.

It can be extended to propose a fuzzy logic based risk model to secure Short Message Service in GSM based 4G networks.

ACKNOWLEDGMENT

This work is supported by research team under Noida Institute of Engineering and Technology, Greater Noida, India. Also this work is highly appreciated by research panel at Galgotia College of Engineering and Technology, Gr. Noida, UP, India. This topic has great work to be extended when implementing risk model against security threats in 4G systems.

REFERENCES

[1] Boudriga, N.; , "Security of Mobile Communications," Signal Processing and Communications, 2007. ICSPC 2007. IEEE International Conference on , vol., no., pp.li-lii, 24-27 Nov. 2007

[2] Delac, G.; Silic, M.; Krolo, J.; , "Emerging security threats for mobile platforms," MIPRO, 2011 Proceedings of the 34th International Convention , vol., no., pp.1468-1473, 23-27 May 2011

[3] Al-Muhtadi, J.; Mickunas, D.; Campbell, R.; , "A lightweight reconfigurable security mechanism for 3G/4G mobile devices," Wireless Communications, IEEE , vol.9, no.2, pp. 60- 65, April 2002

[4] Ali, A.H.; Masrom, M.; , "Analysis and implementation of security algorithms for wireless communications," Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on, vol.2, no., pp.430-434, 26-28 Feb. 2010

[5] Yucun Yang; Weiwei He; Suili Feng; , "Security Analysis and Amendment of 3G Core Network Based on MTPsec," Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on , vol.1, no., pp.519-523, 19-20 Dec. 2008

[6] Sher, Muhammad; Magedanz, Thomas; , "3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Model," Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on , vol., no., pp.198-205, 10-13 April 2007

[7] Palomar, E.; Tapiador, J.M.E.; Hernandez-Castro, J.C.; Ribagorda, A.; , "Dealing with Sporadic Strangers, or the (Un)Suitability of Trust for Mobile P2P Security," Database and Expert Systems Applications, 2007. DEXA '07. 18th International Workshop on , vol., no., pp.779-783, 3-7 Sept. 2007

[8] Xuena Peng; Wen Yingyou; Zhao Dazhe; Zhao Hong; , "GTP Security in 3G Core Network," Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on , vol.1, no., pp.15-19, 24-25 April 2010

[9] Mun, H.; Han, K.; Kim, K.; , "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA," Wireless Telecommunications Symposium, 2009. WTS 2009 , vol., no., pp.1-8, 22-24 April 2009

[10] Shi Zhi-yong; Liu Jia; Ou Qing-bo; , "An Enhanced Secure Access Scheme Based on SIP in 3G Network," Information Engineering and Electronic Commerce, 2009. IEEC '09. International Symposium on , vol., no., pp.476-480, 16-17 May 2009

[11] Aiash, M.; Mapp, G.; Lasebae, A.; Phan, R.; , "Providing Security in 4G Systems: Unveiling the Challenges," Telecommunications (AICT), 2010 Sixth Advanced International Conference on , vol., no., pp.439-444, 9-15 May 2010

[12] Xue Ming-fu; Hu Ai-qun; , "A Security Framework for Mobile Network Based on Security Services and Trusted Terminals," Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on , vol., no., pp.1-4, 23-25 Sept. 2011

[13] Koner, C.; Bhattacharjee, P.K.; Bhunia, C.T.; Maulik, U.; , "Mutual authentication technique using three entities in 3-G mobile communications," Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on , vol., no., pp.1-5, 3-5 Nov. 2009

[14] Pontes, E.; Guelfi, A.E.; , "IDS 3G — Third generation for intrusion detection: Applying forecasts and return on security investment to cope with unwanted traffic," Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for , vol., no., pp.1-6, 9-12 Nov. 2009

[15] Harri Hansen, Security of 3G Systems from a User's Point of View, April 4, 2000.

[16] Otwell K., Aldridge B. The Role of Vulnerability in Risk Management, Computer Security Applications Conference, 1989, Fifth Annual, 1990 Page(s): 32 –38.

[17] Garrabrants W.M., Ellis A.W. III, Hoffman L.J., Kamel M., CERTS: A Comparative Evaluation Method for Risk Management Methodologies and Tools., Computer Security Applications Conference, 1990., Proceedings of the Sixth Annual , 1990 Page(s): 251 –257.

[18] Marmor-Squires A., McHugh J., Branstad M., Danner B., Nagy L., Rougeau P., Sterne D., A Risk Driven Process Model for the Development of Trusted Systems Computer Security Applications Conference, 1989., Fifth Annual , 1990 Page(s): 184 –192.

[19] John Gordon, Security Modeling, Concept Laboratories, [referred Feb. 2001].

[20] 3GPP Technical Specifications Group – Services and System Aspects – Security Working Group, ftp://ftp.3gpp.org/TSG_SA/WG3_Security, [referred Nov. 2000].

[21] Forsberg, D.; Huang Leping; Tsuyoshi, K.; Alanara, S.; , "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on , vol., no., pp.1-5, 3-7 Sept. 2007

.