ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Deception Detection under Fuzzified Communication Media Syndromes

MR.S.Rajkumar*
Research Scholar/ Bharathiar University
Assistant Professor / CSE
Nehru Institute of Engineering & Technology
Coimbatore, Tamilnadu, India.
rajkumar_proff@rediffmail.com

MRS.V.Narayani
Research Scholar
Department of Computer Science
St.Xavier's College
Tirunelveli, Tamilnadu, India.
narayaniv79@rediffmail.com

DR.S.P.Victor
Associate Professor and Head
Department of Computer Science
St.Xavier's College, Tirunelveli, Tamilnadu, India.
victorsp@rediffmail.com

Abstract: Nowadays every transaction in this realistic world is encapsulated by recent communication media components. It is an essential part in our life to keep ourselves away from vulnerable security risks and issues. The art of deception also change its face with a modern artistic fashion. This paper deals with an investigation for identifying the deception under the fuzzified environment. An experiment was conducted involving alarmed and unalarmed receivers. Results were discussed with possible implications. In future we will focus on empirical analysis for deception detection.

Keywords: Deception, detection, syndromes, fuzzification, phising.

I. INTRODUCTION

A. Information Technology in Real life:

We use the term information technology or IT to refer to an entire industry. In actuality, information technology is the use of computers and software to manage information. In some companies, this is referred to as Management Information Services (or MIS) or simply as Information Services (or IS). The information technology department of a large company would be responsible for storing information, protecting information, processing the information, transmitting the information as necessary, and later retrieving information as necessary.

Information technology is concerned with improvements in a variety of human and organizational problem-solving endeavors through the design, development, and use of technologically based systems and processes that enhance the efficiency and effectiveness of information in a variety of strategic, tactical, and operational situations [1]. Ideally, this is accomplished through critical attention to the information needs of humans in problem-solving tasks and in the provision of technological aids, including electronic communication and computer-based systems of hardware and software and associated processes. Information technology complements and enhances traditional engineering through emphasis on the information basis for engineering.

The knowledge and skills required in information technology come from the applied engineering sciences, especially information, computer, and systems engineering sciences, and from professional practice. Professional activities in information technology and in the acquisition of information technology systems range from requirements definition or specification, to conceptual and functional design and development of communication and computer-based systems for information support. They are concerned with such topics as architectural definition and evaluation. These activities include integration of new systems into functionally operational existing systems and maintenance of the result as user needs change over time. This human interaction with systems and processes, and the associated information processing activities, may take several diverse forms [2].

B. Online Shopping:

Online shopping is the process whereby consumers directly buy goods or services from a seller in real-time, without an intermediary service, over the Internet. It is a form of electronic commerce. An online shop, e-shop, e-store, internet shop, webshop, webstore, online store, or virtual store evokes the physical analogy of buying products or services at a bricks-and-mortar retailer or in a shopping centre [3]. The process is called Business-to-Consumer (B2C) online shopping. When a business buys from another business it is called Business-to-Business (B2B) online shopping [4].

C. Phising:

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

This paper is organized as follows:

(i) Compare theoretical and computer aided Deception Detection[5]
(ii) Research Design Model and Strategies
(iii) Experiment Methodology
(iv) Result and Result analysis

D. Theoretical Deception Detection:

Deception is a major relational transgression that often leads to feelings of betrayal and distrust between relational partners. Deception violates relational rules and is considered to be a negative violation of expectations. Most people expect friends, relational partners, and even strangers to be truthful most of the time. If people expected most conversations to be untruthful, talking and communicating with others would require distraction and misdirection to acquire reliable information. On a given day, it is likely that most human beings will either deceive or be deceived by another person. A significant amount of deception occurs between romantic and relational partners [6].

E. Computer Aided Deception Detection:

Serious online crimes like fraud can be prosecuted in courts. For less serious matters, virtual communities are societies, and societies can establish their own rules and laws for behavior of their members. Members who engage in disruptive or damaging forms of deception can have privileges revoked, including automatically as by "killfiles" for ignoring messages of certain people. Less serious forms of deception can often be effectively punished by ignoring it or ostracizing the perpetrator just as with real-world communities; this is effective against "trolls", people deceiving to be provocative (Ravia, 2004). In moderated newsgroups, the moderator can delete postings they consider to be deceptive and/or disruptive. On the other hand, deception involving unfair exploitation is often best handled by exposure and publicity, like that of "shills" or people deceptively advancing their personal financial interests.

II. MATERIALS AND METHODS

Deceiver emphasize on social cues, immediacy, engagement, conversational demand and spontaneity lashing in entire conversation with abnormal increased or decreased level of variation in emotions.

Table 1: Deception Detection Possibility

Components	DC	VC	AC	TC	E-mail
Gestures	VH	H	VL	VL	VL
Language	H	H	AVG	AVG	VH
Response	H	H	H	AVG	AVG
Repetition Analysis	VL	VH	H	H	H
Mislead	H	H	VL	VL	VL

VH-VERY HIGH,H-HIGH,AVG-AVERAGE
VL-VERY LOW,L-LOW

A. Strategies:

S1: DDRate (Direct Communication) > DDRate(Video conference)>DDRate(Audio chat)>DDRate(Text Mail/ chat)
S2: Prior alarmed people DDRate is greater than non alarmed persons DDRate.
S3: False alarm plays a vital role in identifying deceptions.

B. Research Methodology:

We can formulate these strategies in order to construct a methodology as follows:

(i) Direct communication
(ii) Video conference
(iii) Audio chat + Alarms = 2 Suspect Genuine
(iv) Text chat
(v) Email

*DDRate – Deception Detection Rate

III. EXPERIMENT AND RESULTS

We can implement the methodology through an experiment on the students of BE-CSE at NIET, Coimbatore with the participants are allowed to use
LCD Projectors
Computer systems
Internet connection
MM Headset & microphone
Email- authorization through net

The entire datum are recorded and saved and archived. Totally 100 students were used in which each set containing 20 students for 5 variations with half alarmed and another half unalarmed.

A. Assessment Technique:

Detection accuracy = Lies detected/ No. of lies occurred
Total no. of lies is gathered from Deceiver side itself.
Direct communication – enquiry for indisciplinary action from student side.
Video conference – enquiry for weekend leave without prior intimation by the student to the department.
Audio chat – Information through phone for intimation Sunday as working day for a special class on Internet programming paper.

Email/sms – Intimating the students to register their names for free lunch at XYZ Hotel through anonymous mail.

Items dealing with the experiment can be measured on a 5-point scale from

a. strongly disagree
b. disagree
c. refusal / dilemma
d. agree
e. strongly agree

For the questionnaire based schema on fuzzified communication media interfaces.

The duration for each individual is 15 minutes. The receivers were monitored through several hidden observation units such as cameras, tape recorders and recorded documents. The overall deception detection rate was 22.4% for all the variations.

Table 2: Deception Detection scenario

S.No	**Communication media modes**	**Overall Deception Detection**	**Alarmed set**	**Unalarmed set**
1	Direct communication	38.5%	56%	21%
2	Video conference	31.5%	44%	19%
3	Audio chat	24%	36%	12%
4	Text chat/sms	13%	20%	6%
5	Email	6%	10%	2%
	Average	22.6%	33.2%	12%

IV. DISCUSSION

The strategies were tested using a oneway analysis of variance, with $\alpha <.05$ being set as the level of statistical significance, with an N of 100. There were statistically significant differences for media, so Strategy 1 was supported. There were statistically significant differences for warnings, with warned receivers being more accurate at detection deception than receivers who were not warned. S2 was supported. There were no statistically significant differences for S3, and since it was in null form, this Strategy is not rejected. Unwarned interviewers had an average of 0.10 false alarms.

V. CONCLUSION

Media plays a vital role in detecting the deceptions. Direct communication mode can be analyzed with the gestures feeling the waves of opponent in an exact/accurate mode, whereas video conference can be handled with proper care. The repetitive plays varying the speed of presentation analysis is an additional skill present in video conference while audio chat focuses on the pitch stress and pause time gaps of communication response as its primary factors. SMS or Email is blind folded in detecting deceptions.

Alarmed or unalarmed also plays the secondary factor for this analysis. In most of the cases alarmed people unnecessarily suspect all the options or available factors to keep themselves always “aware” which consumes time and rest of the time produces lack of deception detection.

Subjects in our case ABCD students are unaware of few technically advanced psychometric deceptive keywords. In future we will try with experts in this same area.

VI. REFERENCES

[1]. Steve Woznaik, Kevin D.Mitnick, Willaim L.Simon, 2002. “The art of deception: controlling the human element of security”. Wiley; 1 edition.

[2]. Zuckerman, M.,DePaulo, B.M. and Rosenthal, R.”Verbal and Nonverbal Communication of Deception”.In L.Berkowitz (Ed)(1981)

[3]. Burgoon, J.K., and Qin,T. “The Dynamic Nature of Deceptive Verbal Communication”. Journal of Language and Social Psychology, 2006, vol25 (1), 1-22.

[4]. Bond,c.,F. “A world of lies: the global deception research team”, Journal of Cross-culture Psychology, 2006, Vol.37(1), 60-74.

[5]. Pennebaker,J.W,Mehl,M.R.&Niederhoffer,K. ”Psychological aspects of natural language use: our words, ourselves”. Annual Review of Psychology, 2003, 54,547-577

[6]. Whissell,C., Fournier,M.,Pelland,R., Weir, D.,& Makaree,K. ”A comparison of Classfiifcation methods for predicting deception in computer-mediated communication”. Journal of Management Information systems, 2004,20(4),139-165.

Short Biodata of the Author

Mr.S.Rajkumar completed his M.E–CSE at Sathyabama University, Chennai and currently doing his Ph.D in the area of Computational Science. He is a Research Scholar of Bharathiar University and working as a HOD/CSE at NIET Coimbatore.

Ms.V.Narayani completed her M.C.A in M.S University, Tirunelveli and M.Phil in Mother Teresa University, Kodaikanal. She submitted her thesis in the area of Data Mining.

Dr. S. P. Victor earned his M.C.A. degree from Bharathidasan University, Tiruchirappalli. The M. S. University, Tirunelveli, awarded him Ph.D. degree in Computer Science for his research in Parallel Algorithms. He is the Head of the Department of Computer Science, and the Director of the Computer Science Research centre, St. Xavier’s college (Autonomous), Palayamkottai, Tirunelveli. The M.S. University, Tirunelveli and Bharathiar University, Coimbatore have recognized him as a research guide. He has published research papers in international, national journals and conference proceedings. He has organized Conferences and Seminars at national and state level.