Threat Language: Cognitive Exploitation in Social Engineering

Handoko[1], Dwi Anggreini Waskito Putri [2]
{handoko@lptik.unand.ac.id[1], dwi2orchid@yahoo.co.id[2]}

English Department, Universitas Andalas, Padang, Indonesia[1], Universitas Negeri Padang, Padang, Indonesia [2]

Abstract. Social engineering aims to elicit sensitive information by using various manipulation approach to exploit the victim. The increasing of social communication platform such as email, messenger, facebook, linkedin, researchgate, combined with the social psychology and cognitive linguistics become a new weapon to attack either personal or even institutional targets. This paper explores the language used by the attacker to expose psychological threat to elicit sensitive information and to direct the victim to execute the certain action. The data are taken from emails which contain threat language. This paper illustrates how an attacker uses threat language to perform social engineering. The analysis is based on social engineering attack classification (Mouton, 2016) and cognitive pragmatics (Bara, 2010). The result shows rather than using persuasive approach, the attacker uses the threat to exploit cognitive process in thinking and decision making. Moreover the research also found pattern of a social engineer email: warning, threat, and enhancement.

Keywords: Language, threat, cognitive linguistics, social engineering, exploitation.

1 Introduction

The improvement of human contact with technology using online communication have exposed them to the threatening situation. Besides the technical and infrastructure system, the human vulnerability can be manipulated by social engineering. As reported social engineering has become the highest attack used by hacker [1]–[3]. Social engineering is related to exploitation toward human cognitive aspect for certain purposes. In general, users assume that their interaction opponents can be trusted, even if they only know from email or from an online profile. In recent years, such online communication security vulnerabilities are often misused to obtain sensitive information or important information [4], [5].

Some researchers argue that the human is a vulnerability driver in the security system . Human instinct can be a security hole that can be used by hackers to expose psychological and cognitive aspect to manipulate and obtain important information [3], [6], [7]. Among other human nature that may lead them to social engineering is curiosity, politeness, greed, coercion, levity, and apathy [7].

People usually do not aware of the social engineering techniques used. Most are also unaware of the value of the information they share and the social impacts of the information [8]. Even most victims unaware they are victims of social engineering attacks because they are unable to recognize and tend to ignore it. Besides, the ability of the social engineer to direct the

IConShel 2018, September 05-06, Padang, Indonesia

DOI 10.4108/eai.5-9-2018.2281060

target to perform a certain action by developing mental space through sexual, financial, religious, and personal interest [9].

Several studies related to social engineering are more widely discussed from the computational and system security aspects. The researcher argues that social engineering has a strong interdisciplinary relationship various studies in social psychology and cognitive psychology [3], [10], [11]. Some psychological states that can be exploited including strong emotion, overloading, reciprocity, moral responsibility, integrity and consistency, power, and deceptive relationships [12]. These psychological aspects can be used to perform social engineering attacks which of course can lead to discomfort, nervousness, anxiety, and fear toward the victim.

Since social engineering studies focus a lot on thoughts and behaviors that aim to access the cognitive aspects, then the language as one medium for analyzing cognitive aspects is often used to carry out attacks through social engineering. The use of language reflects important aspects of speakers through their understanding of the communication situation at a given time. This is what allows access to cognitive aspects by using relevant linguistic features [13].

Linguistic speech features related to cognition aspects can reveal the thinking process of speakers. Knowledge of the cognitive process allows one to be able to penetrate the deepest aspects of human psychology so that they can direct someone to do something [9]. From this, it can be seen that understanding of cognitive processes can be used as a medium for social engineering.

The research on social engineering relations from the cognitive aspects, especially cognitive linguistics has not been widely discussed. The goal of this paper is to provide an overview of a cognitive and psychological aspect of language use in social engineering, especially threating language. The research focuses on linguistics form used by the social engineer to direct the victim to perform certain acts or to provide important information that can be used by the attacker to hack the system.

2 Method

The current research focuses on the use of threat language used by the social engineer to exploit the cognitive and psychological state of the target. The data are taken from emails sent by the attacker to the targets which contain threat language. The participants are invited to forward the email they received from the researcher. Then the threat languages are being extracted and analyzed by using linguistic theory, especially cognitive pragmatic, and cognitive discourse analysis regarding the significance of particular linguistic choices.

3 Analysis and Discussion

Language has become the main spotlight in cognitive studies, both related to cognitive modules, visual and memory, and to language processing and thinking [14]–[17]. Recent cognitive and psychology research focuses on language processes in the brain and how they relate to non-linguistic aspects, such as mental representation and memory [18], [19]. This includes how language is learned, how the meaning of the language can be understood and transformed into visual or mental representations of images, and how speakers can understand nonverbal aspects and translate them in the form of linguistic representation [20]–[22].

Language usage reflects an important aspect of the speaker's perception or concept which mediated by the knowledge about the communicative situation in certain time which known as context [14]. The speakers utter their intention through action, known as speech acts, according to the context of speaking. By the close relation between speech act and context, the intended meaning of the speaker can be revealed. Of course, sometimes the intended meaning may be different from the utterance, known as indirect speech acts.

The speech act initiated by the intention of the speaker to deliver the idea to someone. This intention has a critical role in the study of the cognitive process, especially in Pragmatics, which focuses on the biological foundation of linguistic performance [14], [23], [24].

A speech act can be specified into locutionary, illocutionary, and perlocutionary acts. The locutionary refers to the linguistic form of the utterance while the illocutionary refers to the intended meaning of the utterance. While locutionary and perlocutionary acts focus on the speaker performence, the perlocutionary acts concern about the consequence of the utterance [14].

Regarding threat, the use of language is closely related to Face Threatening Act (FTA) which focuses on the speaker's intention to violate the cooperative principle. The FTA may be used to threat the positive or negative face of the hearer which may affect the cognitive and psychological acceptance of the hearer [14].

Language threat can be seen in the intention of the speaker to violate the cooperative principle by using face threatening acts strategy.

(1a) *"... I adjusted the virus on a porn web-site which you have visited. When the object clicks on a play button, the device begins recording the screen and all cameras on ur device start working.*

Moreover, my program makes a remote desktop supplied with keylogger function from your device, so ***I was able to get all contacts from ur e-mail, messengers and other social networks****...."*.

Data (1a) is an excerpt from an email sent by a social engineer to manipulate the victims. The first part of the email consists of information about what the attackers do and technical processes with clear and concise language. Here the utterance is used as a pretext to build cognitive awareness and convince the victim.

In the second paragraph, the attacker continued explaining about technical processes but with the more technical term, such as "a remote desktop" and "keylogger", which may not be familiar to the victim. The use of the technical term can create blank space in mental representation and lead to confusion. It also reflects the authority of the attacker which positioned the victim as an inferior. Among the effective strategy of social engineering is to show authority [7]. The authority can be defined as power over others, including knowledge, skills, administrative position, and social status.

The threat can be seen in the utterances "I was able to get all contacts from ur e-mail, messengers and other social networks...." which shows attacker past actions. Here, the attacker tries to build the environment to trigger worry and fear or the victim toward the past action. Here, the attacker describes himself as a computer geek who can penetrate the system and can remote and execute the computer command without physically access the computer. By using a narrative discourse which describes the authority of the attacker over the victim, the social engineer will be able to convince the victim to do a certain action or to share important information.

The utterance is considered to violate the cooperative principle since it threatens the victim's face. Here, the attacker uses Face Threatening Act strategy to create fear and

distressing. From the context of the utterance, it can be seen that the attacker uses FTA to threat the positive face of the victim. The use of FTA in data (1a) is aimed to exploit the cognitive process and psychological state which may affect the way the addressee behave. It can be seen from the data that the speaker uses the declarative form to inform the victim what he able to do, yet by considering the context of the text it can be inferred that the intention of the attacker is threatening the victim.

(1b) *"...You have one day after opening my message, I put the special tracking pixel in it, so when you will open it I will know.* ***If ya want me to share proofs with ya, reply on this letter and I will send my creation to five contacts that I\'ve got from ur device****..."*

The second part of the email consists of harsh language to threat the victim by using the imperative form. It also reflects the attacker superiority over the victim. In term of grammatical structure, the attacker still commits some grammatical error and tend to use spoken form, such as "ya" and "ur".

The attacker uses cognitive psychology to exploit the victim. It can be seen from the use of threatening language to elicit and trigger fear. Attacker aims to target the nature of human who want to be appreciated and respect [15]. The issue of the pornographic still consider as taboo and people committed pornographic of related issues, such as watching porn, is considered to be embarrassing and immoral By using the social psychology, the attacker exploits the cognitive process in the victim's mind to direct the victim to execute the certain action.

Data (1b) is delivered by using the declarative form where the attacker as a speaker provide information to the addressee. However, by analyzing the context and pretext of the utterance, it can be inferred that the speaker aims to threat the addressee. The use of threat in data (1b) shows that by the authority of the attacker on technology has created the mental image of the future scene. Here, the attacker uses the future form to convince the victim of the threat. The nature of human who wants to be respected and wants to have social status can be a weak point that can be used by the social engineer to hack the system or to extract important information about the victim or the system.

(2) *"...Your mailbox has exceeded 2.GB of limited storage It is determined by the CURRENTLY 2.30GB administrator,* ***you can not send or receive new messages until you validate your email again*** *Click on the link below to complete your mailbox for 10.30 GB..."*

Data (2) also consist of threat language used direct the victim to do certain activities. Here, the victim is required to click a link which contains dangerous content, such as malware, virus, or keylogger. Some other emails may require the victim to provide sensitive information, such as username, password, or personal information [2], [3], [6].

Regarding the structure of the utterance and its relation to social engineering, there are three of their sections in delivering the threat: warning, threat, and enhancement. The warning is used to developing cognitive awareness to attracting the victim attention. Here, the attacker uses the declarative form to inform the victim that the mailbox has exceeded the storage. The next part focuses on the threat which aims to exploit the cognitive and psychological state of the victim to commit certain action. The last part is consist of compensation which aims to convince the click the available link.

It can be seen in data (2) that threat language is used to access the cognitive and psychological state of the victim. First, the attacker develops the context of speaking by mention the warning about storage limitation, then offer a solution for the problem. By evoking fear, the

attacker intends to manipulate the mind and the attention of the speaker. Then, to enhance the attack and to be more convincing, the attacker offers compensation and reward for the action.

The imperative form used in data (2) indicated that the attacker forces the victim to do the action which violates the cooperative principle. The attacker uses imperative to threaten negative face of the victim. Regarding the linguistic form of the utterance, data (2) is elaborated by using the imperative structure which contains prohibition or warning. However, by analyzing the context of the utterance, it can be seen that the illocutionary act aims to tell the addressee to execute the certain action. Here, the attacker as the speaker is not intended to inform about the technical problem but to direct the addressee do an action.

In several cases, the attacker seems to avoid longer text by using direct language and straight imperative.

(3) *Due to our system update, we urge all Account Users to verify their email by Update Account to deactivate & activate your mail. Thanks!*

Data (3) shows that the attacker uses threat language to direct the victim to click the provided link. Here, the attacker uses the same pattern as in data (2) which elaborate the text with a logical excuse, directive statement, and resolution. However, in data (3) the attacker makes the text shorter by using a complex sentence. It can be seen from the structure that the complex sentence consisting of two clauses, including declarative and imperative clause. Here, the main focus of the sentence is the imperative form which can be inferred as the speaker intention while the declarative provides information to develop logical reason as for the context of the utterance.

The attacker also uses intext link to direct the victim to the intended page. It can be deceiving for the victims since the link is not visible. Several orthographic styles also used to emphasize important aspects, including the words "Account User" and "Update Account". Here, the attacker aims to attract the attention of the speaker and build temporal mental representation. Of course, orthographic information alone is not sufficient to bring the intended meaning to the victim. However, it can lead to the associative meaning which relates the linguistics unit to the mental representation in the victim's memory.

Regarding the linguistic form of the utterance, data (3) can be categorized as an indirect speech act. The text is delivered by using the imperative form. The use of the words "urges", "deactivate", and "activate", are considered to be polite since they have a positive connotation. Moreover, the use of politeness marker "Thanks" may convince the addressee that the email is sent by the authorized person. However, by using the context of the text, it can be inferred that the focus of the utterance is not to inform the addressee about the system but to direct them to execute the clickable words.

(4) *"... Our spider detected 5 deadly trojans in your mailbox today.* ***If you left unchecked, this can lead to a total email shutdown or loss of important data****. To protect your email data, follow the URL below to scan your Email for free..."*

Data (4) is also used to conduct social engineering. Here, the attacker uses the fake authority as an antivirus provider. The used threat word "deadly trojans", "email shutdown", and "loss of important data" will bring a negative impact to the victim perception.

From the structure of the text, it can be seen that the attacker uses the same structure which includes a warning, threat, and enhancement. The warning can be seen from the word "detected" which indicates the authority. Moreover, the attacker also attempts to exploit the cognitive aspect of victim's mind by using the technical term, such as "spider" and "trojan" to build an intellectual gap between the attacker and the victim.

For the threat, the attacker uses a conditional structure to describe the worse effect of the trojans. Here, the attacker attempts to create future imagery situation to penetrate the cognitive aspect of the victim. The word “shut down” and “loss” bring a negative description of the future fact. Moreover, the use of conditional structure in data (4) indicates that the attacks push the victim to do a certain action to avoid data loss. This can be categorized as violating the cooperative principle. Her, the attacker threat the negative face of the victim by the intimidation. The resolution of the threat can be seen by the use of imperative form in the last sentence. This part can be considered to as enhancement to release the tension of the mental process. The resolution is always used in the social engineering to build trust and to convince the victim.

The locutionary act of utterance in data (4) is presented by using a declarative form. Here, the speaker seems to provide information about the system. Yet, by using the context of utterance, it can be inferred that the main objective of the speaker is not to inform but to order the addressee to click provided link.

From the data, we can see that human are using threat language to bring mental simulation for the future. The attacker delivers the threat of language to build mental representation by exploring the semantic knowledge of future scenarios. Some recent research shows that naturally, the process of thinking of humans is more likely to be future-oriented where they tend to predict the future by identifying potential threats and opportunities [2], [3], [6], [14], [19], [25].

The use of threat language is aim to exploit the cognitive process of the human mind in digesting information. As described in the analysis of the data, before the threat, the social engineer always begins the text with some sort of warning to create cognitive awareness. This part is very important to provide logical reason and build a mental image of the situation. Then, the social engineer use threat language to exploit the cognitive process by eliciting fear and worry. Of course, fear and worry will affect the mind to process information, especially linguistic information, and may affect the process of decision making. The last step used by the social engineer is to provide resolution of the threat, either by offering solution or compensation of the future action.

4 Conclusion

The use of threat language in social engineering plays important in affecting the cognitive process of thinking and decision making. There are three parts of threat email, including warning, threat, and enhancement. The warning is used to create logical reason and to develop a mental image which influences the way victims respond to the threat. The threat is used to trigger fear and worry which influences the process of thinking toward the future action. The enhancement can be a solution or reward that will be granted after the victim executes certain actions. The use of threat language is considered to violate the cooperative principle by using Face Threatening Act which aims to exploit the cognitive process of thinking and decision making.

References

[1] J. M. H. P. D, “Social engineering in cybersecurity: the evolution of a concept,” *Comput. Secur.*, 2017.

[2] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, 2014.

[3] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, “Panning for gold : Automatically analysing online social engineering attack surfaces,” *Comput. Secur.*, vol. 69, pp. 18–34, 2017.
[4] M. Junger, L. Montoya, and F. Overink, “Computers in Human Behavior Priming and warnings are not effective to prevent social engineering attacks,” *Comput. Human Behav.*, vol. 66, pp. 75–87, 2017.
[5] R. Heartfield and G. Loukas, “Detecting semantic social engineering attacks with the weakest link : Implementation and empirical evaluation of a human-as-a- security-sensor framework,” *Comput. Secur.*, vol. 76, pp. 101–127, 2018.
[6] J. M. Hatfield, “Social engineering in cybersecurity : The evolution of a concept,” *Comput. Secur.*, vol. 73, pp. 102–113, 2018.
[7] F. Mouton, L. Leenen, and H. S. Venter, “Social Engineering Attack Examples , Templates and Scenarios,” *Comput. Secur.*, 2016.
[8] D. Tayouri, “The human factor in the social media security – combining education and technology to reduce social engineering risks and damages,” *Procedia Manuf.*, vol. 3, no. Ahfe, pp. 1096–1100, 2015.
[9] H. Handoko, D. Anggreini, and I. Revita, “The Language of Social Engineering: From Persuasion to Deception,” in *Language and Civilization*, 2015, no. August, pp. 136–142.
[10] W. Tounsi and H. Rais, “A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks,” *Comput. Secur.*, 2017.
[11] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-shaer, and B. Chu, “Data-Driven Analytics for Cyber-Threat Intelligence and Information Sharing,” *Comput. Secur.*, 2017.
[12] F. Mouton *et al.*, “Towards an Ontological Model Defining the Social Engineering Domain,” 2016.
[13] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, “Necessity for ethics in social engineering research,” *Comput. Secur.*, vol. 55, pp. 114–127, 2015.
[14] B. G. Bara, *Cognitive Pragmatics: The Mental Processes of Communication*. Massachusetts: Massachusetts Institute of Technology All, 2010.
[15] S. Pinker, *Language, Cognition, and Human Nature*. Oxford: Oxford University Press, 2013.
[16] N. Chomsky, *Language and Mind*. Cambridge: Cambridge University Press, 2006.
[17] W. Croft and D. A. Cruse, *Cognitive Linguistics*, New York. Cambridge University Press, 2004.
[18] S. R. Fussell and R. J. Kreuz, “Social and Cognitive Approaches to Interpersonal Communication : Introduction and Overview,” pp. 3–18, 1994.
[19] A. Bulley, J. D. Henry, and T. Suddendorf, “Thinking about threats : Memory and prospection in human threat management,” *Conscious. Cogn.*, vol. 49, pp. 53–69, 2017.
[20] L. K. Zhanalina and A. B. Ordahanova, “Substance And Methods Of Cognitive Approach In Linguistics,” *Procedia - Soc. Behav. Sci.*, vol. 192, pp. 720–723, 2015.
[21] K. E. Sinclair, T. A. Heys, and S. D. C. Kemmis, “Anxiety and Cognitive Processes in Problem Solving,” vol. 18, no. 3, pp. 203–206, 1970.
[22] P. Cap, “ScienceDirect Applying cognitive pragmatics to Critical Discourse Studies : A proximization analysis of three public space discourses,” *J. Pragmat.*, vol. 70, pp. 16–30, 2014.
[23] H. A. Whitaker, “Concise Encyclopedia of Brain and Language,” *Concise Encyclopedia*. Elsivier, 2010.
[24] M. Kuźniak, A. Libura, and M. Szawerna, *From Conceptual Metaphor Theory to Cognitive Ethnolinguistics*, Volume 3. Frankfurt am: Peter Lang Edition.
[25] V. Evans and P. Chilton, Eds., *Language, Cognition and Space*. London: Equinox Publishing.