International Journal of Advances in Software Engineering & Research Methodology
Volume 3 : Issue 1 [ISSN 2374-1619]
Publication Date : 31 August, 2016

Cyber criminal hunting/invigilation as a new approach to counter-social engineering

Leonard J. Mselle

***Abstract*—The rapid advancements of technology whereby mobile phones combined with software tools used to foster connectivity and the expansion of electronic services for financial transactions, commerce, education, medicine, entertainments and communication in various forms has increased the scope of the terrain of social engineering attackers and expanded both the scope and severity of threats. So far the security techniques proposed do not conform with the severity and the nature of treats. In this paper social engineering techniques to counter social engineering are proposed.**

***Keywords*—social engineering, cyber criminal hunting, social engineering/cyber criminal invigilation**

I. Introduction

Any attempt to gain confidence or entry into a system/site under false pretence is called penetration or hacking. Penetration or hacking can be achieved through electronic means in combination with 'social engineering'. Social engineering is based upon the building of an inappropriate trust relationship with individuals, and can be used against those within an organization. Social engineering attacks can be either dispersed or direct. Attackers prepare well, learning about an organisation's structure and language in advance. Their approaches create a plausible context. They may exploit the willingness of employees to assist others; take advantage of an employee's poor safeguards in using the internet, to introduce malware; to gain unauthorized access to the system to steal information about organizations or individuals details [1].

The rapid advancements of technology whereby mobile phones combined with software tools used to foster connectivity and the expansion of electronic services for financial transactions, commerce, education, medicine, entertainments and communication in various forms has increased the scope of the terrain of social engineering attackers and expanded both the scope and severity of threats. Social engineers can now operate through mobile phone and associated technologies in a more versatile and effective way than they would need to operate in the computer-based internet. Most defensive measures proposed by corporations were not aware of the recent growth of mobile phone applications and their associated services. With this growth, there is a need for cyber security organs to change their approaches in order to be effective in the changed environment.

Leonard J. Mselle
College of Informatics and Virtual Education, The University of Dodoma Tanzania

Since our lives, both corporate and individual, have increasingly migrated into mobile electronic realm, the security methods and techniques we use to counter social engineering must change to conform with the new challenges.

So far the concern and pace for this change does not seem to have been adopted with the urgency that the matter demands. As an example, CPNI [1] proposes:

> "The most effective countermeasure against social engineering is education: employees should be made aware of social engineering and the value of the information they hold. Organisations should also consider implementing policy and procedural steps such as software controls for employees' internet access, effective filtering across internet gateways, developing internet access policy, protective marking systems for sensitive documents, employee reporting mechanisms and ensuring their website information does not offer information of use to the social engineer."

Much as one may agree that education is the most effective counter measure for social engineering, CPNI's proposal is basically exclusively pro-organizational, ignoring the fact that with proliferation of mobile phones and its associated solutions/products, individuals have become "organizations of sort". This proposal is completely devoid of the new technological, business and life reality concerning cyber space. The need for INDIVIDUALS being armed with techniques for countering social engineering is now just as big as it is for corporations.

The urgency for more emphasis on ***devising individual ssocial engineering counter measure*** could be justified by the following paragraph:

> "On the 30th. December, 2015 Tanzania Regulatory Authority (TCRA) issued a general communiqué (press release) announcing that it had received complaints amounting to 42 from customers on cyber crime incidents within one month in which mobile telephone number-spoofing was carried out to steal people's money or tarnish people's images [2]".

A review of records pertaining to money theft cases through mobile phones reported in Dodoma Municipal is over 2000. Almost all of these case are dormant because the police force complains that mobile carrier companies are not forthcoming in assisting the investigation processes which could lead to arraignment of the culprits. These cases are just some of those categorized as being carried out through electronic social engineering techniques.

This situation is now common all over the world [2, 3 & 4]. There is a need therefore to devise new protection approaches for the regulators and propose counter social

engineering measure to empower the individual users to better protect themselves. In this direction, cyber-criminal hutting posture is proposed.

II. Social engineering invigilation to counter social engineering (Cybercriminal hunting posture by CERTs and users)

So far, cyber criminal hunting/invigilation is a non-existent category. Generally, when theft through mobile telephone or any other electronic means is carried out, the victim reports to the police/CERT. Police and CERT are supposed to try to record the nature of the crime and promise the victim that measures to identify and arraign the culprit will be taken. Much as they may want to identify and catch the suspects, the police or CERT ability to arraign a cybercriminal suspect is severely compromised. This can mainly be attributed to the following factors;

1. Police/CERT and victims have largely considered cyber crime in the same terms of traditional crimes where physical evidence such as seeing, hearing, movement, an electronic link/document, and the like, can help the police/CERT to mount an-after-the-event pursuit. In case of mobile cyber crime there is an absolute distance separation. The criminal's physical characteristics such as appearance, movement, document, link, etc. are completely hidden to the victim and the police/CERT. The means used to carry out the crime (telephone and SIM card and the operation) are either too easy to dispose off or too cumbersome to recover. Apart from the carrier companies, it is almost impossible to get a lead from a third party person who might provide the corroborating information and/or evidence . All these complicate the ability by the police/CERT to effectively launch an investigative agenda that can lead to catching the criminal.
2. Victims who happen to report mobile/electronic money theft to the police/CERT, do so with the main aim of recovering what they have lost. Without intending, the emphasis on recovery of the stolen money and incrimination stimulates defensive attitude among the key players who are the mobile operators and the banks. While the victim is eager to recover his/her money, the police/CERT are eager to establish a crime and the operator is eager to avoid responsibility. This conflicting posture places too much emphasis on incrimination, recovery and arraignment at the expense of protection, deterrence and disabling the criminal operational comfort, which should be the main aim of the regulator. As this mind set dominates the scene, it leaves criminals to continue scamming other victims unhindered and unbothered. The cost of cyber crime to criminals is thus minimal since the environment remains constantly friendly.
3. While the police and the untrained users are mainly interested in establishing the crime, the regulator is more interested in deterrence and maintaining a fair and normal working environment that is maximally hostile and dangerous for the criminals. These two different frames of reference breed some elements of incompatibility in the preference and the course of action for each event among the parties (the victims, the police and the regulator). Such atmosphere calls for modification of protection techniques to respond according to the severity of the issues. One such approach could be cyber crime invigilation or cyber crime hunting posture.

III. Cyber criminal hunting/invigilation through social engineering approaches

In order for the regulator to achieve his main obligations; that is; to maintain a safe cyber space for business, governance, educational and entertainment operations both for corporations and individuals, the police mind-set and emphasis on arraigning the criminals, should be superseded by the invigilator's mind-set of deterrence and creating and maintaining a ***hostile operational terrain for criminals***. This may be achieved (or nearly achieved) if the regulator adopts a counter social engineering posture through social engineering. CERTs and users are advised to try some social engineering techniques to create a hostile environment for criminals which will improve the safety of doing business in Tanzanian cyber space. Such measure may include but not limited to;

A. Regulatory insider trading to counter social engineering

This entails the techniques where by users and the regulator through its agencies such as Computer Emergency Response Teams (CERTs) becoming ***cyber criminal hunters through quasi social engineering***.

To improve corporate and individuals ability to counter social engineering will require adoption of some reverse-social engineering measures by regulators, government agencies and individual users. Such measures could involve techniques whereby the CERTs assume a role of a cyber-criminal hunter by behaving quasi criminally. How can this be possible? So far, regulators through CERTs have assumed the half-police role whereby the afflicted victims are supposed to report the incident. Upon receiving the incident, CERT is supposed to rely on the report and circumstances surrounding the event for further measures, such as identifying the suspect and possible arraignment of the culprit. As it has already been stated, this position is clearly disadvantageous to operate from. If, for example, instead, the CERT assumes the powers to institute reverse

social engineering whereby the CERT professional(s) assume the "under-cover" posture and pose as a possible law breaker(s) (quasi cyber criminals) who are officially seeking to uncover some criminals but apparently behaving like normal cyber criminals who use some weaknesses from operators; and, in due course succeed to uncover some of these elements; the resultant impact would be dual;

1. Operators would be careful and continually more forthcoming in safeguarding their lines because they would be forced to be in constant watch due to this constant inspection posture which the CERT creates in the form of undercover. Creating such ambivalence would force operators to be more vigilant, which in turn will improve deterrence and protection from the part of operators.
2. In due course, the CERT would uncover the unscrupulous elements within the ranks of operator's staff which would lead pave way for eradication of such elements.

B. *Normal user becoming cyber criminal hunters/invigilators*

So far, in case of phishing, the predator (cyber criminals) collect information about possible prays. They proceed to choose the pray and select time, space and the manners to initiate their hunting. General education against phishing has focused on the pray's ability to realize that the crime is about to occur and consequently avoid being robed. This is a purely protective approach that leaves the predator to safely remain at large and proceed to plan and execute the next attack. If, for example, the users are trained and encouraged to identify/detect/invigilate for the possible predators, then, after being convinced that one is talking to a possible thief, the user is encouraged to keep up the conversation without allowing the predator to detect that the plot has been detected. In this way the following information is likely to be obtained;

1. Bank accounts used by these criminals,
2. More telephone numbers used by these criminals,
3. Money dispensing agents who collaborate with these criminals,
4. Mobile carriers which are more friendly to criminals,
5. The confidence with which criminals are operating once they identify a pray, etc.

Uncovering such facts is useful to the regulator since the regulator may use such information to alert the carrier company and advise the management to clean its house. The regulator will use such information to alert banks to enable them to arraign the insider trading personnel, etc.

Once this information is obtained, CERT and the regulator can pursue the so called meta-data post-event analysis which may lead to uncovering the insider trading among carriers, the most vulnerable carries, the reason why a certain carrier is more vulnerable and the why some carrier companies are more resilient/vulnerable than others. Some vulnerable properties of sim-banking and money dispensing agents, the most vulnerable banks and why, etc. will be uncovered and addressed. In addition, when predators sense that some of their users may be smart enough to reverse the hunting process which may lead to their arraignment, their confidence will be undermined and their cost of operation will increase. Ultimately their comfort zones will be reduced in size, consequently leading to improved cyber security.

References

[1]. Centre for the Protection of National Infrastructure (CPNI), "Social engineering: Understanding the Treat", 2013.
[2]. "TCRA Press Release" in the Daily News, of December, 30, 2015
[3]. Havey, S. (2001), Crypto, Penguin Group.
[4]. Scambray, J and Shema, M. (2009). "Hacking Exposed Web Applications", McGraw-Hill, London.

About Author (s):

I

Prof. Leonard J. Mselle, is a senior lecturer at the Department of Computer Science of the University of Dodoma. Prof. Mselle is a renown world class researcher in the areas of computer programming, programming languages and cyber security. He has published six books in the areas of computer programming and programming languages. Prof. Mselle is the inventor of Memory Transfer Language (MTL), an artificial language used for learning and teaching programming in both low and high level languages. Prof. Mselle has presented and published more than 27 scientific papers in various conferences and international journals.