Prevention Mechanism of Information Deceit

Rana Majumdar
Asst. Prof, Amity University,
ASET, Noida

Abhishek Singhal
Asst. Prof, Amity University,
ASET, Noida

Abhay Bansal
Prof, Amity University,
ASET, Noida

ABSTRACT

Data security and extracting intelligence from data in the form of information is the area where every organization is concerned about it. Network security is concerned with who connects to and what goes across a network. Net users have to provide personal credentials like passwords or wireless keys, and the network must protect with firewalls and intrusion detection system. Information security on the other hand, is a somewhat more general concept of being sure information systems have confidentiality, integrity, and availability. This can include network security as well as cryptography, access control, physical security, and more. It covers everything from the earliest security mechanism to latest DMZ zones. Social engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques .This paper described various techniques related to social engineering attack; the countermeasures for a social engineering attack.

Keywords

VPN, IA, DMZ

1. INTRODUCTION

Network & Internet security is only one fraction of information secure. Network security means how to implement the concept of controlling access to networking environments. It is primarily in the digital area, the 1's and 0's that put on the air .The concept of achieving network security including antivirus, firewalls, VPNs and group policy security. Information oath is a surrounding umbrella that defines the requirements for information security both in the digital and the physical world. Information oath is the basis by which organization designs & decides strategy and ensuring strict implementation of the defined policy.

Information security is the process of managing risks related to processing of data, storage space, and transmission of data as well as components and required processes used for this purposes. In security world we focused on information in digital form, but emphasis should be equally given to its other forms eg. Analog or physical form [8]. From any organisations perspective, information security is most imperative, which gives impostor a complete control over the organizations data. Organization using the best security technologies by spending as much money as it can but it remains vulnerable. Now a day's technology provides various tools and techniques to protect data and information from various disasters. The organization applies those security tools and techniques like firewalls, intrusion prevention system, intrusion detection system, passwords, and registry protection, networking policy etc. The company employees follow the best security practices to make themselves and their company secure but they are the most vulnerable part in the organization. Famous security consultant Bruce Schneier said as follows, "Security is not a product, it's a process." Moreover, security is not a technology problem - it's a people and management problem. It is very well said by Bruce Schneier because it is easy for a hacker to get information by exploiting human tendency of trust by getting personalized with the employees rather than by using complicated tools and techniques. The Human approach towards breaching any company's security defence measures is known as 'Human Hacking'. This concept is describing as the development of human weakness by use of various techniques and convinces people to pour out top secret information [7].

The newly invented collective business techniques can destroy the network security wires, cripple identities, and result in significant monetary loss and at the same time the concept of social engineering techniques can overpower intrusion detection systems and easily bypass any policy based network security techniques. Additionally, the worst part of it is that social engineering techniques results in leaking private information of individuals which in turn can be used to acquire the victim's "identity" [5].

2. PSYCHOLOGY OF BELIEF

From organizations perspective, information security threats are within the organization. Core intellectual property, knowledge about organizational behavior and information on process inhabit in the mind of employees and can easily be transferred to other for creating new opportunities. Discontented employees may or might get involve with abuses like turn on the company and modify key processes, destroy information, or leave taking critical intellectual property with them. [9]This human nature can become the cause of the downfall of the organizational security measures. The art of deception is basically the knowledge exploitation of this human tendency of getting familiar with others very easily and very soon. Such knowledge is rarely captured in an adequate fashion in databases, human resource records, and organizational accounting information. An attacker tries to be familiar with the person that is an employee of an organization and who can reveal information that is of interest of the attacker and even he gets successful in getting the information that he needed. Deception techniques are commonly based on the following qualities of human nature including [1].

Researchers at the University of Pennsylvania School Of Medicine have found that telling a lie and telling the truth require different activities in the human brain. [10]

- Desire to be cooperative
- Trend to belief people
- Fear of getting into dilemma

It is evident that sections of the brain that exercises a significant role in how humans pay attention, and monitor and control errors , were, on average, more active in the volunteers when they were lying than when they were telling the truth," Langleben said. "If truth was the brain's normal 'default' response, then lying would require increased brain activity in the regions involved in inhibition and control. In order to get information, the attacker firstly needs to establish trust with the person from whom he thinks he can get some important information. A sense of hesitation in the target's voice reveals that trust has not yet been established and the victim is more likely not reveal the information. According to many authors social engineering can be defined in various ways like "the art and science of getting people to comply with your wishes" [3].

3. IMPLICATION OF COLLECTIVE COMMERCE

In order to get information, the attacker firstly needs to establish trust with the person from whom he thinks he can get some important information. A sense of hesitation in the target's voice reveals that trust has not yet been established and the victim is more likely not reveal the information. Social engineering is accomplished through many techniques including Dumpster diving, shoulder surfing etc. [4] Online Social Engineering & Persuasion [6]. If a group of people were asked to predict the outcomes of a series of coin tosses, and were told that the researchers believed predicting the future was more likely when given a monetary incentive and when the prediction wasn't shared in advance of the outcome. This gave the participants the opportunity to lie and say that they had correctly predicted the coin toss to win the money. [11]

The actual definition of data deception can be anything but the one which actually suit is Information Trickery is generally a hacker's clever manipulation of the natural human tendency to trust and desire to help. The hacker's goal is to obtain important information that will allow him/her to gain unauthorized access to a valued system in an organization and the information that resides on that system. Security is all about trust when it not comes to technology. The weakest link in the security chain is the natural human willingness to help and trust someone at his or her word, which leaves the organizations most vulnerable to attack. Many experienced security experts emphasize this fact.

Despite of various automation systems, different levels of security mechanisms, all machines and computer systems are dependent on human beings on one point of time or the other. So when it comes to human being, their default response linked with increased brain activity in the regions involved in inhibition and control. The "Will" theory, in which honesty results from the active resistance of temptation, and the "Grace" theory in which honesty is a product of lack of temptation. The results of this theory suggest that the "Grace" theory is true, because the honest participants did not show any additional neural activity when telling the truth. It is usually said that social engineering is an art that everyone does not have. This is partly true as not everyone has good social skills. However we have been trained to be good social engineers in our childhood only. As children, humans learn how to get what they want by using social engineering tactics [9].

4. RECOGNIZING AN ATTACK

Social engineering can be used to collect any information that an attacker might be interested in, such as the layout of your network, names and/or IP addresses of important servers, version numbers of operating systems and software, and security products in use internally. In reality, social engineering is probably as old as speech, and goes back to the first lie. It is still successful today because people are generally helpful, especially to someone who is nice, knowledgeable, and/or insistent. Technology is not the solution against a social engineering attack. From network security perspective every problem looks like a nail and can be solved with the help of a hammer. [5] This is a common mistake that a lot of technical security practitioners make when dealing with security issues – always focusing on technology. This is where efforts are required to raise awareness of the impact that malicious social engineering attacks have on companies as well as individuals. Many of the most devastating attacks that have made the news lately have leveraged a combination of social engineering attacks with traditional technical cleverness. It is not enough to know and understand just how to deal with technical security issues but to properly protect your company a solid understanding of the "people issue" needs to be addressed

5. SHIELDING COMMON TRADE ATTACK

So the most important question is how to shield information's from attacker. The easiest way may be to implement multi-level security in the form of passwords, user level privilege, access control mechanism etc. It raises another issue does this multitier security mechanism will be able to handle threat like human intervention and even if then unto what level. System level security also categories as technical, won't be able to handle situation like Core intellectual property, key knowledge, and information on core processes reside in the mind of employees and can be transferred easily. The following table shows different social engineering attack vulnerabilities

Table1. Company Social Engineering Attack Vector Vulnerabilities [13]

Attack vector	**Company usage**	**Comments**
Online		
E-mail	Microsoft Outlook	
Internet	Mobile users are equipped with techniques like Outlook Web Access (OWA) & Outlook client access.	

Pop-up applications		Not Implemented Yet
Instant Messaging	Provision was there to use unmanaged IM products.	
Telephone		Keep Track
PBX		
Service Desk	Not policy Based	Vulnerable.
Waste management		
Internal	Managed by individual departments.	Open & vulnerable
External	Specifically not mentioned	Not properly deployed by many Organization
Personal approaches		
Physical Security		
Office security	Officials are always accessible	No security policies enforced by Organization.
Other/Company-specific		
In-house franchisees	Managed through a franchise.	No security policy

6. PREVENT A SUCCESSFUL ATTACK

As it is quite relevant to depict common commerce techniques can be physical or psychological. Clearly Physical techniques do not require any type of persuasive power or even good communication skills. These basically include checking out dumps and trashes in organizations. Psychological techniques include persuasion and impersonation. That is to imitate as someone in authority. These techniques require a lot of confidence and very good communication skills [1].

TABLE 2. COMPARISION OF PHYSICAL AND PSYCHOLOGICAL TECHNIQUES OF SOCIAL ENGINEERING.

Parameters	**Techniques**	
	Physical Techniques	Psychological Techniques
Physical Theft	Yes	No
Need of persuasive power	Not essential	Required
Good Communication skills	Not necessary	Required
Technical knowledge	Required	Not required
Planning	Required	Required
Knowledge of company’s details	Not required	Required
Knowledge of company’s location	Required	Not Required
Exploitation of human tendency of trust	No	Yes
Use of telephone and internet	No	Yes
Difficulty level	Hard	Easy
Time taken	More	Less

This paper suggests different methods for defending against data theft attempts, including:

- Logical security controls
- Physical security
- Security policies
- Education and awareness
- Strong Knowledge
- Systematic approach
- Organizational Structure

In particular, security managers who want to improve the security awareness culture within their organization. Ensure you are equipped to deal with it - learn from experienced ethical social engineers to understand the threats you face, recognize and identify attacks, and see how to defend against social engineers. Organization/ business is only as secure as the people in it..When discussing IT security it is very common to pair up defenses with attacks. Firewalls counter network attacks, anti-virus for viruses, anti-spy ware for spy ware and so forth. So what is paired up with social engineering? What is the best way to defend against the attacker using deception, lying, and pretexting. Security managers must ensure that from employee’s perspective the social networks they build, the training they receive, and the degree of autonomy and authority all influence the level of security risks faced by an organization. Moreover, organizational structures which inhibit exposure to Information security risks are often at odds with structures for facilitating group level innovation, minimizing redundancy, maintaining individual privacy, enabling flexibility, and promoting adaptive ness & importantly to measure the degree of belief with respect to "Will Grace" theory [11].

So from safety point of view any particular representation of organizational design, performance and adaptability analysis of organization’s ability to learn, based on an understanding of the underlying culture of the organization and its decision making processes (Carley and Hill, 2001).

Here some of the listed of security risks that can be measures using data while protecting data thefts.

Intra Organizations Security
Personnel Awareness Tasks
Personnel Message Network

The security measures against intruders should follow the following liner model which emphasis on both logical & physical security control along with strict implementation of Organizations security policy.

6.1 Proposed Liner model:

Who is sharing information to whom and up to what extent?

↕

Approach should be to implement Knowledge Network

↕

Improve Education and Awareness among people

↕

If required Isolates them Mark them as Critical Employee

↕

Who knows what is it a abuse of organizations security policy

↕

Inevitable disclosure

Knowledge Information Network

↕

What information is related to what Missing Information?

Links must be checked & revisited

Needs Systematic Approach Network

↕

What knowledge is needed to do what mission?

In sequence Redundancy

Identification of Security

Critical Points

Tasks Precedence Network

Decision making processes (Carley and Hill, 2001).

This linear model will further incorporate

- **Security executive agenda**. Goals should be defined at early stage of security & methods, policies should be there to meet that Goal.
- **Risk supervision assessment**. Threats loopholes of policies should be identified & proper review mechanism must ensure how to identify & nullify these risks. Organization must review each of the social engineering threats and rationalize the danger that each presents to your organization.
- **Realize social engineering lines**. Develop, Maintain, Upgrade a written set of policies and procedures that specify how any Organization should cater situations that may be social engineering attacks. This assumes the existence of a security policy, outside the threat presented by social engineering. The rudiments identified by your social engineering risk supervision assessment will get you on track, but you will need to look at other potential threats.[12]

7. CONCLUSION

On conducting a review on the Information Trickery techniques and deception, the truth that revails even after using the best and most expensive security technologies, an organization or a company data is completely vulnerable and susceptible. It means it is very easy for a good attacker to gather information about that organization just by gaining trust and being friendly with the user, environment.

Despite of increasing awareness about security in organizations, social engineering attack is very little painted. Most people consider the social engineering as an attack on their intelligence and wit and therefore they want discuss about it anyone as they don’t want to be considered dumb or have been fooled. In order to overcome problems like this knowledge sharing , knowledge process transformation mechanism should be incorporated by the organization which ensures healthy environment thus provides more data protection.

This type of technique of capturing information is there since lone time but it came into perceive just some time before. Before people and organizations were not much aware of these security breach practices and techniques for securing information but nowadays information security is the main concern of the corporate world. This work proposed a model which emphasis on Information Network, Awareness among people, and Critical Employee & Organizational Structure for combating problems as Information Trickery. In future provision is there to use more technology to fight problem like this but most importantly it requires awareness among people, make a feeling for importance of storing data & protecting them from others not for only organizational benefits but for also their own benefits.

8. REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .

[2] ing, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the

SIGCHI Conference on Human Factors in Computing Systems

[4] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[6] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

[10] University of Pennsylvania Medical Center. "Human Brain Operates Differently In Deception And Honesty, University Of Pennsylvania Researchers Report." *Science Daily*, 13 Nov. 2001. Web. 9 Jun. 2011.

[11] Harvard University (2009, July 14). Dishonesty Involves Activity In Control-related Brain Networks, Neuroimaging Study Suggests. *Science Daily*. Retrieved June 9, 2011

[12] technet.microsoft.com/en-us/library/cc875841.aspx