International Journal on Advances in Engineering, Technology and Science

IJAETS, Volume: 1, Issue: 1, October 2015

Protection of Computer Networks from the Social Engineering Attacks

Hardik K. Molia[1], Hardik A Gohel[2]

[1]*Government Engineering College – Rajkot, Gujarat*
[1]hardik.molia@gmail.com
[2]*Atmiya Institute of Technology & Science – Rajkot, Gujarat, India*
[2]hagohel@gmail.com

Abstract: Social Engineering refers to the non-technical methods of breaking security of a computerized system. Social Engineering attacks target the vulnarabilities of the people rather than of the softwares. Social engineers try to break the human trust rather than discovering ways to hack the system. Social engineers take benefits of human trust, curiosity, emotions, fear, urgency, need, lack of common sense and most importantly technical unawareness. Computer networks can be made secured from the technical attacks by using most efficent and effective firewalls, antivirus softwares, intrusion detection systems etc. But it is high time to secure the networks from the social attacks too. This paper explains human factor based social attacks and some factors to analyze for the prevention and detection purpose.

Keywords: Social Engineering, Computer Networks, Phishing, Baiting, Quid Pro Quo, Pretexting, Tailgating

I. INTRODUCTION

In the era of the computerization, every organization needs to have an online as well as offline computer network based systems. From the online websites and mobile applications for the customers to the local intranet and desktop applications for the employees, every organization needs to be dependent on the computerized systems. Every organization needs to concern about the security of such systems. An organization can secure a computerized system specifically the computer networks over which its systems are running by using firewalls, antivirus softwares and intrusion detection systems which are at present proved to be the best. This is the way; systems get protection from the various technical attacks. An attack is an attempt to disturb the system in an unauthorized and/or unauthentic way. The attacker targets the vulnerabilities of the systems to damage the functionalities. Technical attacks target the software and hardware based vulnerabilities without concerning or manipulating the users directly. A lot of research work has been done and going on towards making the system more secured against various technical attacks. In recent years, a new group of attacks are increasing rapidly which are the social attacks. A social attack targets the people and their vulnerabilities like trust, curiosity, emotions and most importantly lack of technical awareness about the systems they use. Rather than hacking the software, social attacks manipulate people. Social engineering is an attempt to active social attacks to disturb the system. The difference between technical attacks and social attacks can be easily explained by an example of a thief trying to unlock a house. A thief has two choices, in first choice, he can try all the possible keys he has or try to break the lock using various tools or try to steal the key from the owner of the house. In second choice, he can try to convince the owner of the house to give the key. The former attempt is similar to the technical attacks while the later one is similar to the social attacks. This paper discusses some of the social attacks which affect security of the computer networks. Some of the factors for detection and prevention methods are also discussed.

II. TYPES OF SOCIAL ENGINEERING ATTACKS

Here are the categories of some of the well known social engineering attacks. These attacks target the human vulnerabilities to get personal, sensitive, credential information. It is not always about the lack of technical awareness. Sometimes lack of common sense plays a major role in succeeding attacks.

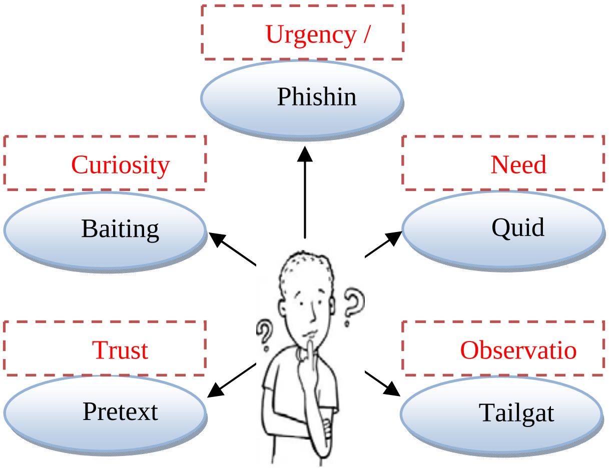

Fig. 1. Human vulnerabilities and social attacks

a. Phishing

Phishing targets the human urgency and/or fear. Phishing is an attempt to capture sensitive information through the medium of false emails, chats or websites. Phishing attacker tries to steal the information by pretending to be a well known or trusted, authentic and authorized entity. Some of the examples of phishing attacks could be: 1.An email seems to be sent form the official account of a bank, asking for the personal account information for the verification purpose, but actually it was sent by the attacker. So on replying back, an attacker gets the sensitive information sent by the user. 2. An attacker designs a fraud website which has the same GUI as of the legitimate website. User enters his credential information to the fraud website and the credential information is received by the attacker. 3. An attacker pretends to be an employee of a bank, calls a customer with a purpose of bank detail verification asking for the credential information or some personal information leading to a phone phishing attack. 4. Attackers show urgency to do some action by showing threats, urgency and sense of fear like send the information to continue accessing social networking account or charges will be applied if not registered in 24 hours.

b. Baiting

Baiting targets the human curiosity. Attackers use physical media containing malwares like USB pen drives, CDs – DVDs, Hard drives etc. to attract people to use them. An attacker leaves one of these medias at a place sure to be found by the victim. Some common places are office tables, cafeteria, bathroom, conference room, elevator etc. An example could be a company A wants to get access to the sensitive information of another company B. An attacker on behalf of company A, prepares a CD with the logo of company A and title as “Confidential Info. for project xyz” and puts somewhere in the company B. An employee of company B finds the CD. Being curious, he tries to open it. As CD has malware inside, unknowingly that employee will get his PC infected. The infection could be anything, releasing confidential data to the modification of the data, a simple access to that PC or as an entry point to the company’s whole network.

c. Quid Pro Quo

Quid Pro Quo targets the human need. Attacker asks to give something to get something. An attacker shows readiness to solve technical issues of user’s computer by asking credential information. A website allows downloading of software after login through social networking accounts. Another example could be an email asking for the personal information for winning a lottery or a gift.

d. Pretexting

Pretexting targets the human trust. An attacker prepares answers of the possible questions to be asked by the victim to gain the victim’s trust easily. At the same time, an attacker prepares a well furnished scenario to ask the victim’s information. The main purpose here is to collect information with the reason of confirming identity of an individual. A brief pre-survey about the victim could be the main reason of breaking the trust as it establishes initial legitimacy in the mind of the victim. Sometimes a convince speech with authoritative voice plays an important role in manipulating the victim’s mind.

e. Tailgating

Tailgating targets the human observation. The example could be an attacker asks for victim’s mobile phone to make an urgent call as his mobile phone has no battery, eventually attacker installs malwares to do the malicious activities. An example could be an attacker builds the friendly environment with an employee, attacker keeps talking with the employee during passing through the security counter too. Security staff assumes that the attacker is either a friend or a closed one of the employee and so they don’t check authenticity for him. Eventually, the attacker gets entry into the company premises. An attacker with a mixer of confident personality, attractive speech and impressive behavior prohibits the victims to doubt on him.

III. IMPACT OF SOCIAL ATTACKS ON COMPUTER NETWORKS

A Computer Network can be either wired or wireless, permanent or adhoc, infrastructure based or infrastructure less. At the same time, it can be a local Intranet or a part of the global Internet. Irrespective of the type, used technologies, deployed applications and ultimate purpose, one common basic requirement of every computer network is of the security. Every computer network has an administrative team to manage its hardware and software based components. The admin is the person who manages and takes care of the whole network. Every user thinks the admin as an ultimate source of information as well as the only source of help. Users generally have blind trust over the admin especially when they are facing some difficulties in accessing the network. A user gets his username and password to get various access rights of the network. This topic discusses how social attacks damage the smooth working of a computer network.

a. Phishing

Phishing attacker pretends to be the admin. In such scenario, users interact with the attacker in the similar way, with the full trust just like they have with the true admin.

At individual level, phishing attack hacks the password of an individual or of a group of users. Later on, attacker uses the hacked account with the same username and password to get access to the network. The main purpose is to do the malicious activities for which the actual user seems to be the responsible as his account is being used. At next level, attacker may access sensitivity resources or even damages resources. For example, after receiving all credential information for a bank account, attacker transfers some money to another account. After receiving all credential information for a PC, attacker collects all sensitive files.

At system level, attacker may gain unauthorized and unauthentic control over the entire network system. For example, attacker damages the way the firewall works. An attacker broadcasts malicious softwares in a network so all users get affected. An attacker may changes the security rules, blocked sites, bandwidth limitations to get prohibited access of the prohibited resources.

b. Baiting

A network is the best vehicle to spread the viruses and other malicious softwares. At individual level, whenever a user connects an external storage media, containing malwares, he is not only inviting problems for himself, but may be for all the users currently connected in the same network. At system level, when someone connects an external storage media without precautions, there are high risks as far as firewall firmware and its content, server softwares and server operating systems are concerned.

c. Quid Pro Quo

To get something done, people become often ready to give something. During data transfer, there is a high risk of getting malicious softwares along with the data in which we are interested. Software updates from unauthorized servers, pirated content from unknown sites are the examples where first we loss confidentiality of our personal information and later on our systems get damaged by malicious activities.

d. Pretexting

As far as computer networks are concerned, pretexting attack let us change functionalities of the network without thinking much. An attacker tries to convince the victim to change some security settings, to share some resources, to modify some network related settings so that future attacks can be easily performed.

e. Tailgating

A network can be damaged by a couple of click events. A simple turn off of a switch is enough to disconnect a lot of active users. Without keeping records of who is visiting the admin area; the place having servers, firewalls etc, it is not possible to keep track of the malicious activities being performed.

IV. FACTORS TO ANALYZE FOR SOCIAL ATTACKS

A lot of research work has been done to detect and prevent various computer network based technical attacks. This topic discusses how to detect and prevent social attacks with the help of software based systems. Technical attacks are difficult to perform, but at the same time comparatively easy to detect as compared to the social attacks which are easy to perform and difficult to detect. To secure the system from the technical attacks, we install the best software based systems but unfortunately to secure the system from the social attacks; it is not possible to upgrade human understanding, technical awareness and inherent nature so easily. The ultimate solution is to analyze almost all the possible activities of a user and inform him by suitable way of communication whenever required. Here is the discussion about important factors to analyze to prevent and/or detect various social attacks.

a. Phishing

Phishing attacks target personal – sensitive information, mostly the credential information. As a result, either attacker uses the credential information to do malicious activities or changes the credential information to deny owner to use the system in future. Most of the computerized systems incorporate various features like two- way authentications, SMS alerts, Email alerts etc. Whenever system detects some unusual activities, it immediately informs the owner via various medium of communication. Biometric authentication is one of the most popular and successful method of authenticating individual. An organization should analyze pattern of user's activities like,

1. Frequency of using Forgot Password option.
2. Frequency of changing the devices from which a user accesses the network.
3. Interest in use of Advance Authentication Methods like 2-Way Authentication etc.
4. Completion of various fields like backup email address, security question etc.
5. Trust factor of the resources an individual uses.
6. Frequency of accessing prohibited resources.

b. Baiting

Baiting can be prevented by avoiding excessive use of external storage media from unknown sources. It is obvious that the system can't stop it but at least based on following factors, user activities can be traced.

1. Antivirus software status and its update status.
2. User's action after insertion of external media. Does he scan the external media with Antivirus software?
3. What user does if he finds malicious softwares in external media?
4. Monitoring user's activities of data transfer over external media.

c. Quid Pro Quo

Quid Pro Quo is based on give and take concept. Most of the time users are interested in getting something without confirming about authenticity and genuineness of the source. Users don't care about what would be the side effects they may need to suffer. The system should monitor following factors to track user activities.

1. Frequency of searching downloadable resources in search engines.
2. Frequency of downloads and trust factors of the sites.
3. Frequency of doing registration to access the resources.
4. Frequency of cancelling downloads after registration.

d. Pretexting

System should monitor if certain activities are repeated in the same order of events with multiple users of the system. In such cases, following factor should be analyzed.

1. Frequency of repetition of such activities.
2. Frequency of users involved.
3. Number of affected users, Number of users who have blocked such activities.
4. Analysis of events being performed in such activities.

e. Tailgating

System's management resources must be accessible by the authentic and authorized team of members only. Biometric verification and validation should be strictly deployed by the owner. At the same time, track of people visit should be efficiently maintained. Following factor should be analyzed.

1. Frequency of unauthorized people found in the premises.
2. Frequency of technical issues found at the Admin side.
3. Frequency of change in password, forgot password, use of external media etc. by the Administration team members.

V. COUNTERMEASURES

Every organization dreams to secure its systems at best. As a result it follows following steps.

1. Vulnerability Mapping

To identify, whether our system is secured from the social attacks or not, several social vulnerability tools and techniques are used. The basic purpose behind such tools is to identify,

Personnel Strength:- The ability of an individual to detect and ignore a social attack without depending upon system intelligence. For example, an employee will never share passwords of the systems telephonically.

Systematic Strength:- The ability of the system to detect and ignore a social attack without depending upon human intelligence. For example, system automatically ignores spam emails from unknown sites asking for registration.

Mapping provides a systematic way to identify how strong our system is. Our system should be a perfect balanced of both the strengths.

2. System Protection

System needs to be modified systematically on the basis of weaknesses. The possible attacks are mapped with the existing protection schemes. The goal is to improve both the strengths while maintaining perfect balance with the system performance.

3. Awareness and Training

End users and system engineers must be aware and well trained about the newly deployed anti-social engineering schemes. The best way is to conduct training sessions and seminars to spread the awareness among the users.

VI. CONCLUSION

Social Engineering is the way an attacker damages disturbs the system or accesses resources without being a technical expert. The attackers take benefit of user unawareness, emotions, need, fear, urgency to gain illegal entry to the system. Such attacks are based on psychologically manipulation of minds which need to be detected and prevented at earliest. Every organization should try to secure its softwares from the technical attacks at the same time, its employees and customers from the social attacks.

REFERENCES

1. Rajendra Maurya. Social Engineering: Manipulating the human. Scorpio Net SecurityServices.
2. Adam Podgórecki; Jon Alexander; Rob Shields. Social Engineering. McGill-Queen's Press - MQUP
3. Gohel, Hardik “Automation of Social Media Analysis by Web Intelligence” International Journal of Science Research and Technology, vol.1, Issue 1, USA , pp17-21,2015
4. Mr Ian Mann. Hacking the Human: Social Engineering Techniques and Security Countermeasures. Gower Publishing, Ltd.
5. Johnny Long. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147
6. Gohel, Hardik. "Looking Back at the Evolution of the Internet." CSI Communications - Knowledge Digest for IT Community 38.6 (2014): 23-26.
7. Hardik, Gohel. "Design and Development of Combined Algorithm computing Technique to enhance Web Security." International Journal of Innovative and Emerging Research in Engineering (IJIERE) 2.1 (2015): 76-79.
8. Gohel, Hardik. "Deliberation of Specialized Model of Knowledge Management Approach with Multi Agent System." National Conference on Emerging Trends in Information & Communication Technology. MEFGI, Rajkot, 2013
9. Hardik, Gohel. "Design of Intelligent web based Social Media for Data Personalization." International Journal of Innovative and Emerging Research in Engineering (IJIERE) 2.1 (2015): 42-45.
10. Gohel, Hardik, and Priyanka Sharma. "Study of Quantum Computing with Significance of Machine Learning." CSI Communications - Knowledge Digest for IT Community 38.11 (2015): 21-23.
11. Gohel, Hardik “DEVELOPMENT OF SPECIALIZED OPERATORS FOR ANALYSIS OF SOCIAL MEDIA THROUGH WEB INTELLIGENCE” International Conference on E-Learning Engineering and Computer Software, 82-86, 2015.