Social Engineering

Adarsh Nair

Computer Science Department
University of Southern California
Los Angeles, California, USA

adarshna@usc.edu

***Abstract* -Nowadays corporations spend millions of dollars in complex mechanisms of system security to ensure the protection of their confidential and valuable data. But many a time the intruder gets what he wants from the victim not through the back door but by straight asking him or her for the information he needs and more often than not, this form of psychological manipulation works. My paper will study the various forms of Social Engineering attacks along with review the impact on how cognitive biases can heavily influence our day to day decisions when it comes to handling our own sensitive data. Also the various countermeasures that can be applied to help resist social engineering attacks along with the current research being done to strengthen these countermeasures will be studied.**

Index Terms - Social Engineering, Cognitive Bias, Pharming, Phishing, Dumpster Diving

I. Introduction

More often than not, humans tend to form the weakest link in a computer network. Humans tend to make mistakes, are more prone to being compromised and are hence extremely vulnerable to attack. Social-engineering refers to the malevolent exploitation of the users of a particular system such that they end up divulging confidential information with or without their knowledge. With the advent of the internet in the mid 90s social-engineering has become one of the major factors of information theft.

Social-engineering attackers can be loosely categorized into 3 categories – 'Hackers', 'Crackers','Phreakers'[1]

A. Hackers

First we have the hackers. Hackers are exceptionally gifted programmers who enjoy studying and exploring code to check for defects and loopholes. They tend to not use their capabilities for illegal purposes and bring to the administrators view the problems with the code. To them, breaking into a system is more of an intellectual high and do it for fun on most occasions.

B. Crackers

Second, we have the cracker. Crackers are similar to hackers in their programming capabilities but use it for malevolent purposes. They are also called the 'dark side hacker'.

C. Phreakers

Thirdly, we have the phreakers. These are hackers that use the telephone system to gain information from naïve users or to misuse their lines to make long distance calls at the victims expense and on most occasions are untraceable.

II. Motives

Social-engineering attackers have a variety of motives for causing an attack. Sometimes the motive may be a noble one and sometimes it may be purely evil. A lot of the times the reasons are intertwined with each other. Hackers in general can be classified [2] based on their motives.

There are the 'casual hackers' which form the largest group and are mostly motivated by curiosity and the challenge of hacking into a system. They are not as skilled as the seasoned hackers and usually employ the use of hacking tools to help their cause due to lack of expertise.

Then we have the 'political hackers', who are also called 'cyber activists' and normally align their hacking priorities with their political beleif's. This may be for a cause or an organization and they are quite skilled as compared to casual hackers.

When we consider the more seasoned hackers, we have the 'organized crime', which comprises of professional criminals who can cause a lot of damage by stealing confidential data and or top secret trade secrets. A more explicit account of the motives of the social engineering attacker are as follows : [3]

A. Financial Gain

This is done for monetary benefit by the attacker. It requires the attacker to be careful to not leave traces so that he cannot be tracked back to. As a result of which the attacker would normally use a victim as a third party so as to frame them to con the investigators.

B. Personal Interest

This is done by the user out of curiosity or certain vested interests like a personal vendetta and sometimes overlaps with the financial gain motive.

C. External Pressure

If the attacker is being forced to hack a system of one organization by another rival organization it falls under this category. Also it may be sometimes against the attackers own will and he may be forced to be doing so. This could be blackmailing or the attacker returning favor.

D. Intellectual Challenge

This is closely linked with personal interest as the attacker is breaking into a system to prove that a system is breakable or vulnerable to attack.

E. Damage Containment

The purpose of this attack is to minimize the damage done from a previous attack and to patch vulnerabilities in the system. These attacks are not always harmful in nature but the attacker can use use this to help individuals to improve their system while at the same time gather information for a future attack.

F. Politics

This is done when the attacker has certain existential belief differences with his or her victim and is usually very public in nature. For example an attack on the government website of an enemy country is a politically motivated hacking attack.

III. Cognitive Bias

'Cognitive biases' are a very powerful tool used by the attacker when it comes to social engineering. It is pattern of deviation in judgement whereby inferences about other people and situations may be drawn in an illogical fashion.[4] There are certain cognitive biases that are specific to helping the attacker when it comes to social engineering. They are [6]:

A. Halo Effect

This refers to the fact that, one is more likely to take the word of a person that is physically appealing or well spoken than of a person who has the contrary traits. As a result of which we are forming an opinion of the attacker who may appear to be clean based on pure outwardly appearance. When applied in the context of social-engineering, if we get an email or a .exe file from someone that appears to be from a trustworthy sender which in this case could be that the email was very well written albeit we may not be sure of their credentials one tends to give them the benefit of the doubt thus rendering one vulnerable.

B. Choice Supporting Bias

This is when an individual has a tendency to remember past experiences as being more positive than negative. For example ecommerce is very heavily reliant on the services provided by Amazon and eBay and the online customers trust these websites with their confidential bank information. Therefore if another site poses as Amazon or eBay there is strong likelihood that a naïve customer will key in his information in the fake website due the Choice Supporting Bias as he already has put his trust on them and would hesitate to think twice or otherwise about their credentials.

C. Exposure Effect

This cognitive bias states that people like items and people that are familiar to them. For example one who is well versed with online social networks is more likely to visit an online dating service simply because they are familiar with social media and how to interact using social media. One who has never used the the online forum as a means of meeting new people is very unlikely to trust the social media quickly. Similarly people who are not very comfortable with using the internet with refrain from making online purchases simply due to lack of trust.

D. Anchoring

This refers to the fact that one tends to focus on an identifiable or noticeable trait. That is, humans tend to focus on the first piece of information offered and that is used as the cornerstone for all future conclusions. Therefore this is usually used as part of the phishing attack as attackers create websites with identical logos thereby deceiving the user as the user focusses on the fact that the logo is identical to what is a trusted logo and henceforth tends to turn a blind eye to other discripencies which he may have noticed otherwise.

E. Ingroup Bias

This is a bias or preferential treatment given to members of your own group. Therefore if a member of a team has been compromised the chances of anyone within that same team doubting him are minimal as one does not expect that from one's own team member. With respect to social-engineering if an employee of a bank requests for confidential information about the bank that is not with him, he may ask another employee within or above his hierarchy for that information and hence can use it malevolently.

F. Confirmation Bias or Tolstoy Syndrome

This refers to ones tendency to interpret information in a way that conforms to ones preconceptions. In a social-engineering point of view, one tends to believe that if one social networking site is safe, then another website made by the same corporation will be safe as well. One wold not delve into the security of policies of the second website too much as one would assume it to similar to the first one as they are both made by the same corperation. For example Google provides a number of services but one does not tend to delve into the security policies of a new product from Google as one has already trusted them with their previous service policies.

Along with the various cognitive biases, there are other common social errors that are exploited by the attackers which can be specific to social-engineering and are :

A. Fundamental Attribution Bias

This is similar to anchoring and states that individuals generally tend to go with their first impression of a person a their final impression. Hence hackers always look at making a positive first impression against the potential victim to gain his trust and this makes it hard for one to determine the legitimacy of a connection. This is sometimes done as assuming a role of authority thus having the victim believe that the one they are speaking to is well respected and possibly, well bred.

B. *Salience Effect*

This effect suggests that the more one tends to stand out of a crowd, the more untrustworthy one becomes. As a result of which attackers tend to blend in with the crowd very well and try to not be very loud in their attack as they would like to go unnoticed which will help in them not getting caught.

C. *Pressing conformity, compliance, and obedience*

These three traits are what compels one to act a certain way which may be contrary to ones best interests but due to the pressure to conform to society one ends up acting so. Which is why attackers usually tend to assume positions of power, like that of a board member and hence when they ask a lower level employee for confidential data, the employee may divulge the information without even checking for the credentials as that is what he is expected to do in the traditional sense, that is a lower level employee is supposed to obey the orders of a higher level employee.

IV. Strategies For Attack

The variation and extent of the attack is limited only by the creativity and ingenuity of the attacker. These strategies are aimed at usually what is the weakest link in an organization, the humans. The attack cycle has 4 steps :[7]

- *Information gathering and Research*
  This phase involves researching the target and getting some background information that will help the attacker formulate his strategy for attack.

- *Developing Relationship Stage*
  This stage aims at exploiting the the fact that humans are trustworthy by nature i.e. they will trust someone unless given reason to believe otherwise and the attacker uses this fact to get close to his victim.

- *Exploitation Stage*
  This is the influencing stage where the attacker makes his attempt to retreive data from the victim by basing his attack upon the previous two stages.

- *Execution Stage*
  This is the action stage where the attacker gets the information that he needs using his various strategies which I shall get into now.

The strategies for attack which are employed in the execution stage are as follows : [5]

A. *Dumpster Diving and Forensic Analysis*

There are a lot of times when companies dump or discard information rich items like company phone books, system manuals, organizational charts, company policy manuals , calendar of meetings, printouts of sensitive data like user names and passwords, print outs of confidential source code as well as company hardware. All of these can be very useful for the attacker to study and data mine useful information as described above. Also when one deletes data from ones computer, and then discards the laptop, it is still possible to retrieve that information from the hard disk at the hands of a skilled attacker('forensic analysis'). Hence it is very important to ensure that one's confidential data is erased completely and/or otherwise stored in an encrypted format and the best thing to do would be destroy the medium that is storing the data if the data is no longer needed like for example using a shredder to destroy all hard documents.

B. *Pharming*

'Pharming' is a passive attack where the attacker lures in the victim without having to go to the victim. For example a user may go to what appears to be a legitimate website and voluntarily key in his details. Usually this is done by having the same name as the legitimate website along with an added suffix which tries to be unnoticeable in the URL. Another way of pharming an attack is by DNS poisoning. The attacker exploits the Domain Name Servers and creates false domain records and as a result of which legitimate DNS entries for a website get redirected to a malicious websites' IP address. Thus by editing the hosts file on the computer of the victim the attacker lures in the victim to his lair thereby compromising the victim.

C. *Phishing*

'Phishing' is the most common form of a social-engineering attack. Unlike Pharming where the attacker lures in the victim, in phishing the attacker seeks the victim and is usually done by impersonating a legitimate source and then gaining the victims trust. One of the most popular and well documented cases of phishing has been the 'Nigerian email scam'[8] where a supposed top level government employee of Nigeria would send an email stating that the victim has won a sum of money and that all the victim has to do is provide some basic information about him or herself that information usually being the victims bank details which would be falsely needed to transfer funds when actually it is being taken to extort money from. A slight variation of this is when the email states that the victim has to pay only a nominal fee to gain the prize and not have to divulge information. Such scams are very popular and are sent out in bulk. Invariably certain naïve users will fall prey to such scams. Common phishing scams tend to be ones posing as major online retailers like Amazon and eBay and are emails requesting to only verify your bank details and hence seem innocuous as users trust these websites with that data. Another variation is one claiming to be from the IRS saying that due to an accounting error you are owed a refund and hence need to enter the bank details to credit the money to. There are ways to protect ourselves from phishing attacks, most of which are common sense. Like it is well known that legitimate businesses will never ask for personal or financial information through email. Also legitimate businesses do not threaten consequences for not sending that information via

email. Phishing attacks usually claim that they will deactivate services or close accounts if the information is not given.

D. *Pretexting*

'Pretexting' is used in conjunction with phishing and pharming and is defined as 'the practice of getting information under false pretenses' according to the US government. It is when the attacker invents a scenario in which the victim is comfortable so as to then increase the chance of the victim divulging confidential information. It usually involves an elaborate lie which is tailored to mimic the victim's trusted environment. An example would be calls made from providers of credit cards and loans and insurance companies. Such an attacker usually has some knowledge about the victim and after establishing his or her trust will ask for the other information which the attacker desires to know. This is what was done in the 'HP spying scandal' [9] which was tailored by Patricia Dunn where she hired investigators to pose as the Board member s of HP in order to get their phone records from the telephone companies by pretexting a scene using impersonation.

E. *Quid Pro Quo*

This phrase literally translates to 'something for something'. This kind of attack is based on the fact that the attacker claims to be giving something in return for some information. A typical example[10] of this is when the attacker gets a list of direct lines to the customers of an IT help desk, he/she starts making calls to each of those numbers until he stumbles upon a customer that actually needs help. As a result of which, the victim as he needs help is more than ready to divulge information in return for solving his problem.

F. *Reverse Social-engineering*

'Reverse social-engineering' aims at getting the victim to ask questions rather that the attacker. In such attacks the attacker usually role plays an authority figure within an organization. For example the attacker may cause a problem to the victims computer to begin with.. Then the attacker will make himself known to the victim as the person who can fix the problem and during the course of their discourse the attacker can extract useful information which can be then used for a succeeding attack.

G. *Shoulder Surfing and Tailgating and Physical Reconnaissance*

'Shoulder surfing' is the attack in which the intruder uses direct observation techniques to get the information he needs. This can be done when the victim is entering his username or password and is done in a sly manner without the victim noticing. A lot of the time, a number of other social-engineering attacks lead up to this as the victim has to be comfortable with the attacker being within that close range to begin with. 'Tailgating' is when the intruder follows the victim into secure areas by walking behind him or her. 'Physical Reconnaissance' is an attack that is done by the attacker by studying the organization by observing the blueprints of the structure, the the work timings, the employee cycle, and other physically noticeable information.[11]

H. *Trojan Horse*

This attack is unique compared to the other attacks in the sense that the attacker does not come in direct contact with the victim and is instead done by leaving what is called a 'trojan horse' which is usually something that will excite the curiosity or grab the attention of the victim. For eg the attacker may leave a disk or a flash drive near the victim and hence the victim out of curiosity may decide to put it in his system to check its contents. The trojan horse in this case would be the disk or flash drive. And once the disk is inserted it can install viruses or worms and cause damage to the victims computer.

I. *Phreaking*

'Phreaking' involves hacking into the public telephony system and rerouting calls to the attackers number and then proceeding with a subsequent method of attack as the victim will now be connected to the attacker without knowing so and thereby the attacker will pretend to be the legitimate callee and extract information.[12]

J. *Mail Outs*

'Mail outs' are in some sense malevolent surveys. Surveys that are in the form of questionnaires can have the victims unknowingly divulge information like their names, phone numbers, email ID's and a lot of more all at the pretext of having to answer a false survey.[13] This is very useful for gathering information about a large set of victims in bulk.

K. *Profiling*

'Profiling' is the technique of using the hacked information and assimilating it to generate a profile of the victim.[14] By doing this the attacker is in a better position to formulate his or her strategy so as to prevent himself from getting caught as he or she will now be able to impersonate the victim based on the information gathered and generate scripts to manipulate the victim.

L. *Identity Theft*

This is an attack where the attacker may physically or virtually impersonate the victim i.e. pretend to be the victim and thereby manipulate the victims accounts. Especially because with the advent of LinkedIn, Twitter and Facebook finding personal information about the victim is not as hard as it once was and as a result of that hacking into those accounts renders the victim to be susceptible to identity theft.

V. Defense Against Social-Engineering

There is no foolproof plan against social-engineering as the weakest link in a network more often than not happens to be the human element. But there are certain countermeasures that can be employed, an improvement in policy being the

main one.[15]A well documented and accessible security policy that is thoroughly understood by the entire team is core to having a secure system. The policy should cover the following at the very least.

- *Computer System Usage* : Policy should monitor the usage of all software and hardware which is specific to the company so as to monitor inconsistent and abnormal activity.
- *Information classification and handling* : It is very important to ensure that information is classified properly to ensure that personnel cannot access information that is not in their clearance level irrespective of their hierarchical position.
- *Personnel Security* : This is policy that ensures that personnel are only allowed to areas for which they have clearance to.
- *Information Access* : This is policy at a user level, which ensures the use of passwords and usernames so that information is not directly accessible.
- *Protection from viruses* : The policy should incooperate a protection scheme to protect the data from being attacked viruses, spyware and malware.
- *Information security awareness training and compliance* : This part of the policy ensures that all the stakeholders are aware of the threats of social engineering and the various counter measures against them.
- *Compliance Monitoring* : This part of the policy ensures that the security policy is followed strictly.

As the administrator is aware of the social engineering threat, mitigating the risk of the attack becomes a lot easier. The first task of the administrator is to determine the value of the data being protected in the organization. Realizing the true value of their data will help to determine if the cost to secure a resource is more than cost of the resource itself then it may not be in the best interest of the organization to frivolously spend those resources.

Risk and Threat

A 'threat' is the type of the attack and the 'risk' is the chance or the probability that the attack will be successful. It is very important for the administrator to know how the terms risk and threat can be applied to his system.[5] Coming to risk, the risk of an attack to a top level executive at a high profile company is a lot higher than to a fresh employee at a low profile start up simply because the executive has more security clearances and therefore employing a social engineering attack on him or her is more likely. The threat, which is the type of the attack, in this case we are talking about social engineering. There are three basic security measures that are applied to tackle social-engineering – 'Physical Security', 'Personnel Security' and 'Digital Security'.

A. Physical Security

This type of protection involves ensuring that assets are protected and monitored so only authorized personnel can gain access through entry points like the front and back doors as well as all other access points. [5]

- *Auto locking doors* are especially useful against the tailgaiting threat where the intruder follows behind the legitimate user to gain access to secure areas.

- *CCTV cameras* further help in this cause as the movement of users can be monitored to ensure everyone goes through the security checks.

- *Photo ID badges* are usually RFID encoded and is linked to the user's name and employee number and is very useful for keeping track of the movement of one's employees. Also these ID's can be given clearance for only the areas they are allowed to go to thereby restricting the movement of employees along with keeping track of them.

- *Biometric Access Devices* go a step up from photo ID's where access to areas is based on fingerprint or retina scanning to ensure absolute foolproof protection to top secret areas. This when used in tandem with photo ID's provide for multi factor authentication as well.

- *Visitor badges* are used to ensure that visitors can be distinguished from the employees and usually come with a time frame after which they expire and have to be renewed if the visitor needs to continue to stay in the building.

- *Sign in sheets* are used in conjunction to visitor badges which are usually filled up at the point of entry into the building and are signed out when the visitor leaves the premesis. This is done to also ensure that everyone who has entered the secure area has left the area as well along with keeping record of the visitors contact information, where the visitor has come from and who he or she has come to visit.

B. Personnel Security

This form of mitigation is done on the personnel or employees at a workspace. It involves [5]:

- First and foremost, *background checks* on potential employees are conducted. This is to find out whether they have any criminal records so as to get an idea of the character and ethics of the hire. Ensuring that the potential employee has a clean record improves the chances that the information he is given clearance to will remain secure and that he or she will likely to not be compromised.

- Second, *Protect user information*. This is done to let the users know to not divulge their or the companies information to third parties at any cost.

- Thirdly, *Training*. This is crucial as at the end of the day social engineering attacks are done on the people of an organization and ensuring that they are well aware of the security policies will help in lowering the vulnerability to an attack. These need to be done periodically to ensure that the security updates are fresh in everyone's minds. Having mock social engineering drills can also be very helpful in this regard.

C. Digital Security

This is the last step in protecting the system against a social engineering attack and also a very important one. There are certain measures the administrator should employ to make the system resistant to an attack on the digital front or software front and they are [5]

- First, *improving the password policy*. Passwords are usually the first gateway into any secure area or for getting access to a file and ensuring that they are hard to crack is key. Having a random password generator which incooperates special characters as well as having a length requirement is quite beneficial in this regard. But this is very cumbersome for the user to remember. Hence a common ground of laying the minimum password complexity requirements while at the same time encouraging the users to not use personal information related passwords is what is done.

- Second, *having a secure firewall set up*. Configuring, maintaining and updating the firewall is key to blocking out connections that are unwarranted. This could help protect against Trojan horses and known pharming websites.

- Third, *strong Email filtering*. Ensuring that the spam filter on the users email is set up properly can help protect the user against phishing attacks, chain emails, viruses or worms that could harm or plant itself on the host computer thus converting it into a botnet of sorts.

- Fourth, *Multifactor Authentication.* This is usually implemented as two factor authentication and involves placing a check on both what one knows and what one has. Google's 2 step authentication follows this rule. Whenever you sign into your Google account, along with entering your username and password Google will send a verification code to the phone registered to your account. And therefore for signing in, the user would need to enter both the username, password as well as the verification code which expires after a short time period. This can be further extended to 3 way authentication where along with providing what you know and what you have, you have to give information on who you are which is usually in the form a biometric check.

- Fifth*, Strong Encryption*. For data that is sensitive, it is always better to encrypt it so that if your system has been compromised and the intruder has gotten hold of your data, he or she would have to decrypt it for it be of any use.

- Sixth, *Limited wireless network access*. The wireless network of an organization provides the opportunity for the intruder to breach into the secure areas without having to physically set foot into the organization. Therefore it is imperative that the administrator uses a strong encryption technique like WPA 2 to secure the network. WEP key strings have been shown to be able to be passively sniffed and cracked within several minutes [16] Along with the encryption technique, it is also important to choose a strong passphrase along with the encryption method. A RADIUS server should be used to help authenticate users into the wireless network. And finally, segmenting the wireless network onto its own subnet or VLAN will help improve the protection. This is

especially important if the wireless network is allowed to grant acces to users that are visitors and have to be disallowed later.

- Seventh, *Access Control Lists*. An access control list is a list of permissions that is attached to an object that specifies which users have access to those objects. This is especially useful when it comes to devices that are an organizations property and are given to an employee for use. ACL's are used to grant privileges to the user of that system and hence limit the employees control over the system. Therefore certain system changes cannot be made by the user and therefore are an effective protective measure.

VI. Research in Social-Engineering

Social-engineering needs to be combatted using a DID ('Defense in Depth') approach i.e. ensuring there are multiple layers of security so that if the intruder manages to break through one layer, there are additional reinforcements that can stop him or her. This gives rise to the 'onion layered' approach to social-engineering as seen in figure 1[5]. The outer layer comprises of the physical security, which is responsible for the physical access to the secure data; then we have the personnel security which is the security enforced on the network users and staff; the innermost layer of security is the digital security which is applied on the network resources.

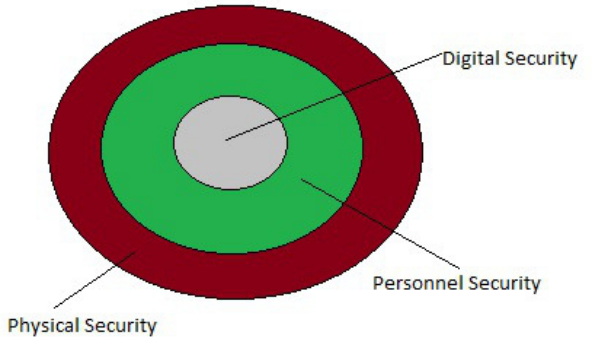

Fig. 1

An area of research that is currently being explored is that of 'Unintentional Insider Threats'[18] which was studied at CERN at Carnegie Mellon University. More often than not information may be divulged unintentionally by an employee or ex employee of an organization rather than by an individual with malevolent intentions. The reason this unintentional slip may take place can be classified into the relevant human factors and the psychosocial and sociocultural factors. The human factors begin with a case of human error which can be cause by fatigue or sleepiness or due to a discomfort or confusion at the work place or with its policies. The organization should ensure that it is able to distinguish between a malevolent intentioned threat and an UIT but at the same time should study their employees behaviour to ensure consistent patterns of slip ups aren't seen. Another factor that contributes to human error is the subjective mental workload. It is the personal feeling of being cognitively burdened by the work experience. This causes a decrease in performance as well as raises stress thus affecting ones judgement. Therefore it is imperative for the organization to ensure that their workers are kept content and hence, alert. Situation awareness, which is the knowledge about the state of a given environment is also crucial in ensuring that one does not divulge information by chance. Weak situation awareness can cause potential system failures as the employees must keep abreast with the latest attack vectors and know to perceive their attack on ones environment so as to take the necessary countermeasures in time.

Future research in social-engineering needs to be done in a three step process. First is ensuring that the users are aware of the various modes of social-engineering attacks. Second, is having a social-engineering security team than conducts tests based on these attacks on the users and stakeholders to point areas and users that are vulnerable as well as keeping note of which attacks are most efficient. Third, is the countermeasures that have to be deployed against these attacks and ensuring that all users are well informed of their vulnerabilities and the countermeasures that can be taken. Employing the onion layered approach of implementing a defense in depth model of Physical , Personnel and Digital security will be most effective in countering social-engineering along with regular meetings with the users and stakeholders to keep them abreast with the security trends will help mitigate of the nemesis, i.e. social-engineering.

One such research approach that was studied is by Lech Janczewski and Rene Fu of the University of Auckland, New Zealand [19] for identifying what are the key vulnerabilities or points of attack in a system.

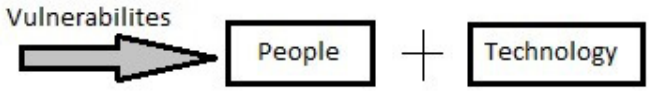

Fig. 2

As is seen in the traditional sense, the two points of attack to an organization are the people and the technology with the people being the weaker link and as a result of which the social-engineering security strategy is modeled around reducing the vulnerability of the human element as seen in Figure 2. However the security strategy itself can be a point of of vulnerability if it is still immature in its development. Hence our new vulnerability model becomes one that includes an immature security strategy as seen in figure 3. Therefore it is imperative to have a regular 'SETA' meetings(which were meetings to educate the user of the dangers prevalent and the

countermeasures for them) and to use a social-engineering task force that is capable of setting up a strong security strategy based on the onion layered model of a defence in depth approach.

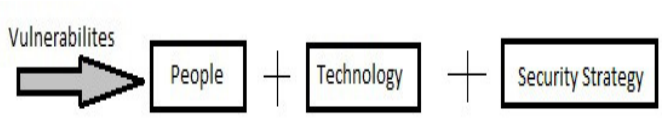

Fig.3

CERN at Carnegie Mellon has also conducted research on detailing social engineering attacks via 'Internet Relay Chats'(IRC) and Instant Messaging services(IM)[20]. IRC and IM can be used to trick unsuspecting users into downloading and executing malicious software. The malicious software is disguised as useful applications that provide free anti-virus protection, improvement in download speeds or links to adult websites. It is based on the discretion of the user to be able to identify these malevolent links and this is kind of a pharming attack as the attacker is luring the victim to click on the malicious code.

Cyber attacks cost US companies not only money but trust and good will as well. Kevin Mitnick[21] a past USC student and world renown social-engineering expert played a key role in bringing and showing social engineering attacks as a serious means of information theft and malevolent practice. I agree with Mitnick when he states that coorperations today do not spend enough resources on securing their most valuable asset which is their employees and hackers normally target four categories of employees, first, low paid employees and staff with low morale, second executive gatekeepers, third, remote office workers and fourth, new hires. Identifying these employees as most vulnerable is crucial in mitigating the social-engineering risk.

The SANS institute also proposes a 'multi level defense strategy' [22] which is a manifestation of the onion layered approach. It follows a 6 level approach to tackle social-engineering.

A. Foundation Level

This is the basis of the security policy and is designed to help the user tackle questionable requests. A well established foundation level policy will ensure that the users have no choice but to negate the hackers requests. The users should not have to think twice about getting compromised and this is where Metacognition which is the awareness of and thoughts about their or others, comes into the picture. Hence when the attacker orders the user by assuming a role of authority, instilling confidence in the user will help him or her in fending off the influence the attacker is attempting to instill on the user.

B. Parameter Level

This is the security training and awareness level which is to be employed after the policy has been set up. The user should know that the attacker will try to set up a trusted relationship and that upon gaining that the attacker will exploit the user for all kinds of information. The user needs to be well aware and hence this makes regular training imperative.

C. Fortress Level

This level takes the training step and extends that to provide resistance training to key personnel who are more susceptible to attack. And the personnel that are most susceptible are the system administrators, help desk personnel, secretaries, business assistants and the customer service representatives. It essentially includes all the personnel that would interact with the public.

D. Persistence Level

Since we are employing a multi level approach it is quite possible for the users to get lax about the policy at a certain stage. Hence the need for ongoing reminders is crucial. Regular and fresh reminders keep the users alert that an atttack can occur at any time.

E. Gotcha Level

This level is analogous to the honeypot defence mechanism applied in computer network security. It employs the use of Social-engineering Land Mines (SELM) which is a trap set to lure the attacker and study his attack so as to improve the users own social-engineering security policy.

F. Offensive Level

This is the damage control level where if in case an attack has been successful the user needs to be ready with a well thought out contingency plan to mitigate the effect of the successful attack which should involve aggressively going after the attacker and ensuring he or she is caught. Otherwise if there is no incident response, every user who deals with the attacker is on his own and fighting a new battle.

The SANS model was a heavily user centric model barring the Gotcha Level and was tailored at ensuring the user is as well prepared as possible.

VII. A Hybrid Model ?

The SANS institute multi level defense strategy albeit effective is not complete. And this is where I believe a hybrid model that incooperates the policies of both the Defence in Depth(DID) onion layered approach of Physical , Personnel and Digital security coupled with the user centric SANS multi level approach would be ideal in tacking the social-engineering problem. While the DID Onion approach takes care of technicality of the issue, i.e. dealing with the attacker

and mitigating his effect, the SANS approach is very useful for the user who is being targeted and is a much more user centric approach for tackling the social-engineering problem. With social-engineering attacks being limited only by the creativity of the attacker, the scope for research in this field is huge.

VIII. Conclusion

Social-engineering attacks are very hard to predict because they can come from internal or external sources. Future research on social engineering should be focusing on the advent of numerous information rich , data sharing social networking sites which have a very large young subscriber base who are relatively inexperienced with the social-engineering phenomenon and form easy targets to attackers. [17] Employing widespread use of SETA (Security Education, Training and Awareness) to improve the awareness among users and to develop their skills and knowledge against attacks will help mitigate the effects of social-engineering attacks.

Acknowledgment

I would like to thank Professor Clifford Neuman for taking the CSCI530 System Security class as it has been an absolute pleasure to learn under his guidance.

References

[1] Raymond, E.S.,Jargon dictionary. 2003. Available from http://catb,org/~esr/jargon/

[2] Zager, M., Who are the hackers? 2002, Infosec News. 3p.

[3] Australian Institute of Criminology, Hacking motives. 2005, Australian Institute of Criminology: Canberra. 2p

[4] Haselton, M. G., Nettle, D., & Andrews, P. W. (2005). *The evolution of cognitive bias*. In D. M. Buss (Ed.), The Handbook of Evolutionary Psychology: Hoboken, NJ, US: John Wiley & Sons Inc. pp. 724–746.

[5] Mitigating the Risk of Social Engineering Attacks by Matthew Spinapolice

[6] A study of social engineering in Online frauds. Brandon Atkins, Wilson Huang, Mouldrie Technical College, Valdosta State University

[7] Allan, A., K. Noakes-Fry, and R. Mogull, Management update: How businesses can defend against social engineering attacks, in InSide Gartner. 2005, Gartner Research: Stamford. xxi: 5p.

[8] Information Security Office, UT Dallas http://www.utdallas.edu/infosecurity/Phishing.html

[9] The story of HP pretexting scandal with discussion is available at Davani, Faraz (14 August 2011). "HP Pretexting scandal by Fraz Davani". Scribd. Retrieved 15 August 2011.

[10] "How Social Engineering Works" by PC Plus Can be found at http://www.techradar.com/us/news/internet/how-social-engineering-works-913505

[11] Allen, M., Social engineering, in GSEC practical assignment. 2006, SANS Institute: Washington. 13p.

[12] Bearman, R., A guide to social engineering, in Network Security Forum. 2004, Network Security Technology: Waco. 6p.

[13] Redmon, K.C., Mitigation of social engineering attacks in corporate America. 2005, East Carolina University: Greenville. 6p.

[14] Dolan, A., Social engineering, in GSEC practical assignment. 2004, SANS Institute: Washington. 15p.

[15] "The threat of social-engineering and your defense against it " SANS Institute InfoSec Reading Room

[16] "The feds can own your LAN too" Can be found at http://www.smallnetbuilder.com/index.phpoption=com_content&task=view&id=24251&Itemid=100

[17] Social Engineering: The Neglected Human Factor for Information Security Management - Xin (Robert) Luo, The University of NewMexico, USA, Richard Brody, The University of New Mexico, USA, Alessandro Seazzu, The University of New Mexico, USA Stephen Burd, The University of New Mexico, USA.

[18] Unintentional Insider Threats : A Foundation Study – Department of Homeland Security , Federal Infrastructure Protectiion Bureau, Carnegie Mellon University . Can be found at http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

[19] Social-engineering based attacks : Model and New Zealand perspective. Lech Janczewski and Rene Fu. University Of Auckland, New Zealand . Can be found at http://www.proceedings2010.imcsit.org/pliks/36.pdf

[20] Global Information Assurance Certification Paper . SANS Institute , Can be found at : http://www.giac.org/paper/gsec/2082/social-engineering-attacking-weakest-link/103563

[21] "Kevin Mitnick on Social-engineering hackers" By Gary Breach.

[22] "A multi level defense against social engineering" SANS Institute InfoSec Reading Room