IADIS International Journal on Computer Science and Information Systems
Vol. 5, No.2, pp. 1-20
ISSN: 1646-3692

PSYCHOLOGICAL CONSIDERATIONS IN SOCIAL ENGINEERING – THE Ψ-WALL AS DEFENSE

Evangelos D. Frangopoulos *School of Computing, University of South Africa (UNISA). 215, Alexandras Avenue, Athens, GR 11523, Greece.*
eMail: vfrangopoulos@hol.gr

Mariki M. Eloff *School of Computing, University of South Africa (UNISA). Theo van Wijk Building 8-100, UNISA, Pretoria, South Africa.*
eMail: eloffmm@unisa.ac.za

Lucas M. Venter *Director: Research Support, North-West University, South Africa*
email: Lucas.Venter@nwu.ac.za

ABSTRACT

In the context of Information System Security and security in general, Social Engineering (SE) attacks exploit vulnerabilities that are based on principles of human psychology. The attackers who employ such methods are identified as "Social Engineers". In conjunction with loopholes in the security structure of the organisation, SE attacks can yield results that would be difficult, if not impossible, to obtain through the use of purely technical hacking methods. As SE attacks are based on deception, they are very difficult to categorise. Hence, designing countermeasures for them is even more difficult and as such, to this day, provisions present in current security standards and best practices against SE methods are limited, indirect and rather inadequate. Thus, a more fundamental approach is called for, if effective defense methods are to be devised.
The current analysis of the psychological aspects of SE forms part of a larger effort to identify the risks emerging from the largely non-technical issues of Information Security (IS) and devise methods for their mitigation. To this end, the notion of the Ψ-wall is introduced.

KEYWORDS

Information Security, Social Engineering, Psychology, Ψ-wall.

1. INTRODUCTION

The study of Social Engineering (SE) methods of operation, shows that a strong element of psychological manipulation and exploitation is always present in all of the SE attacks that require some form of contact between the Social Engineer who is carrying out the attack and his/her target or "Mark" (Bernz, c.2000, Mitnick & Simon, 2002). (The term "Social Engineer" identifies any attacker who employs SE methods while the term "Mark" is used in SE discussions to denote any person targeted by a Social Engineer, but not necessarily one that actually becomes a victim).

The aim of this paper is to provide a better understanding of the issues involved in SE attack methodology and to propose better defenses against SE.

Section two discusses the psychology behind SE attacks and attempts to identify the psychological principles on which the methods and techniques of the said attacks are based and the way that these are applied to the field of IS.

In section three, psychological countermeasures leading to appropriate defense mechanisms are examined in an effort to provide controls for SE vulnerabilities. The concept of the "Ψ-wall" is introduced as well as possible mechanisms to support it.

Section four concludes the paper.

2. PSYCHOLOGICAL TECHNIQUES EMPLOYED BY SOCIAL ENGINEERS

The first crucial step in creating defenses is to identify the nature of the threat and the vulnerabilities it attempts to exploit. This section examines psychological tactics such as persuasion and influence techniques used to compromise information security.

2.1 Persuasion through Applied Psychology - Variations on an Old Theme

Even though the object of this work is SE methodology and its relation to information systems, the methods and attacks used today in computer-related crime, are far from new. They have been in use for at least the past 50 years using the communication media available at the time. For example, telemarketing using telephone calls has been thriving in the U.S.. Although telemarketing can be (and has been) used in ways ranging from legal to undeniably illegal, it is always based on the power of persuasion the telemarketer has over the prospective client/victim. On the other hand, it has always been a general truth that a good salesman can sell anything. The salesman's abilities are not dependent on the merchandise. Again it is the power of persuasion that comes into play. Con artists have been thriving since the dawn of mankind using their power to influence other people. Politicians and cult leaders have been doing the same thing for thousands of years. In all of the above cases there is a common factor in the methods used: the exploitation of human nature. Influence and persuasion methods have been successful because they exploit the same basic property: human psychology. Thus, the bottom line is that although technology evolves and provides societies with different channels of communication, the basic human psychological characteristics have remained the same as

they have been for centuries. Hence, modern SE attacks are based on those unchanging psychological traits that are governed by the very essence of human nature.

2.2 The Psychology of Physical Attacks

Physical presence on the site under attack is, by far, the least attractive method for the Social Engineer. However, there are cases that this cannot be avoided. The main modus operandi of a Social Engineer (usually through impersonation) is to blend in with the surroundings and use such psychological manipulation techniques that are necessary for achieving his/her goal.

Carefully orchestrated gestures, facial grimaces and body language are essential before even "first contact" is made. For example, in order to follow an organisation's employee through security-controlled gates successfully (a technique known as “tail-gating”), the Social Engineer must have the right timing but also the right attitude towards both the person being followed in, as well as the security guard who may be present. Exploiting the natural tendency of people to be nice or the equally normal positive pre-disposition towards handsome people of the opposite sex, the Social Engineer can go a long way. Porting him/herself with the air of authority or, at least, ease, the Social Engineer can surpass most first-contact checks and exploit those mental shortcuts that will allow him/her to move around the target premises unchallenged. If challenged, the Social Engineer will have to be prepared to provide some information (obtained in the earlier phases of the attack) that will back up or explain the reasons for his/her presence on the premises.

There are at least three techniques that can be used efficiently by the Social Engineer in physical attacks:

Exploitation of the human tendency to be helpful. A Social Engineer impersonating an employee in a hurry for a meeting who is also carrying a large load, may pretend to be fumbling for his/her badge or authentication token while the security officer instinctively rushes to his/her help. Another, pretending to be a courier for a large company holding a number of boxes, may ask for someone to "hold that door" for him to pass through etc. In most cases, simply because everyone is conditioned to offer their help to fellow people in need, this conditioned response overrides the call of reason that dictates to carry on with the security check, with obvious results.

False appeal to authority. All hierarchical structures are based on the authority of higher level personnel upon lower level personnel. Unfortunately, this authority, although originally delegated in order to make the function of the structure possible, is frequently abused in order to be treated differently from anyone else. Frequently VIP members of staff will try to "pull rank" in order not to have to wait in line to be authenticated or, even worse, to be allowed access when they have forgotten their authentication token (ID card, smart card etc). The lower-ranking personnel responsible for security at points of entry etc, will usually succumb to the minimal of pressure because they are not willing to challenge someone who could get displeased with their "overzealous" behaviour and affect their own standing in the structure. This situation clearly presents an oxymoron since lower-level personnel who are responsible for security and perform prescribed procedures are only doing what is required of them according to their job description, and should be appraised for that, instead of being reprimanded. Such a situation can be exploited by a Social Engineer who can either impersonate someone with authority, or claim to be acting for, or on behalf of, such a person.

Exploitation of "Low Involvement" personnel. Harl (1997) introduces the idea of "Involvement" as a contributing factor to the success (or not) of a SE attack. People who are highly involved in the system that the Social Engineer is trying to compromise (such as administrators, computer security officers, computer technicians and users who are well accustomed to the use of the system) have to have strong arguments presented to them by the attacker in order to be persuaded. Weak arguments act as warning signs to them and may bring the attack to an early and unsuccessful end. On the contrary, night-shift guards, cleaners, and even office-hours receptionists are classed as "Low Involvement" employees because they have very low interest in what a Social Engineer may actually ask them to do and weak arguments may actually prove very successful with them as shown by Mitnick and Simon (2002, pp. 150-155). In this fashion, a member of the cleaning staff may be persuaded to allow a Social Engineer after-hour access to a site or run an errand for him/her that could provide the Social Engineer with essential information for an attack. Furthermore, a receptionist (a position that requires the employee to be particularly courteous, polite and helpful) may unwittingly provide the attacking Social Engineer with critical information or even access to restricted areas after some careful manipulation (Mitnick & Simon, 2002, p.162).

In all cases, a physical attack on the target premises requires meticulous preparation. It also demands the attacker to acquire a state of elevated psychological resilience that is necessary to withstand the pressure inherent to such an attempt, as well as the special ability to constantly monitor and actively manipulate the psychological status of the potential challenger to allow the planned attack to unfold. All of the above are not always possible, hence the attacker must also have an escape plan from the premises in case things do not turn out as expected. It can thus be argued that strict physical security at the entrances as well as at the exits of the premises may constitute an effective measure towards better control of SE attacks at the physical level.

2.3 Persuasion Tactics

SE attacks eventually have to employ persuasion tactics in order to achieve the desired result. There are two routes to persuasion: the *Direct* or *Central Route* and the *Peripheral Route* (Rusch, ca 1999).

The Direct Route is systematic and uses logical arguments in order to stimulate a favourable response from the person being persuaded and / or prompt this person to take the action desired by the persuader. This technique is unfavourable to SE tactics because there simply is no logic behind a request to reveal sensitive information to unauthorised persons.

The Peripheral Route is the tool preferred by Social Engineers who invariably use this technique to misrepresent their objectives. Mental shortcuts, peripheral cues and distraction techniques are applied in order to trigger acceptance without thinking and reasoning.

In psychological terms, such persuasion can not be considered equivalent to brainwashing. However, strictly speaking, it still is a form of manipulation of a human's mind by another individual in an attempt to achieve an opinion shift, without the manipulated person being aware of what caused his/her opinion shift (Sutphen, nd). Sutphen, in the same article, also argues that the basis of persuasion is always to access one's "Right Brain". In an oversimplified attempt to explore the mechanisms of persuasion, it is stated that while the left half of the human brain is responsible for analysis and logic, the right half is responsible for creativity and imagination. Thus, persuasion techniques attempt to distract and keep busy the

left half of the brain in an effort to find a shortcut to accessing the right half. An example of such a technique would be to present the Mark with an arguably dangerous situation that needs to be analysed and assessed by the left half of the brain. This leaves the task of simultaneously processing the main request (that could lead to the disclosure of sensitive information) to the right half of the brain, which is more prone to the suggestion that it would be "ok" to comply with this request. As an example, a Social Engineer posing as an bank IT staff member could call a Mark in the middle of the night and state that unusual activity is being monitored with respect to the Mark's account, with sums of money continually being transferred out of the account. The Social Engineer could then offer to help reverse the transfers and block the account if only the Mark gave him/her the password needed to access the account. At the same time the Social Engineer does not forget to state that it would be irregular to do so and that he/she "is risking his/her job by doing that". While in a state of shock and confusion, the Mark could conceivably fall for such an attack.

Guidelines, for aspiring Social Engineers are provided by Bernz (ca 2000) in the form of a tutorial. Tips and tricks of the trade are given and although this text will definitely not win any literary competitions, it does drive its main points home rather successfully. Many SE techniques are discussed and almost all of them are based on the application of practical psychology methods in order to persuade the Mark to release sensitive information.

In Grangers' commentary of the above reference (Granger, 2001) there are several persuasion tactics identified:

Impersonation. This technique can be applied over the phone or in a physical attack. Depending on the type of Mark, different approaches can be taken. Usual roles for impersonation over the phone include an administrator or technician from the company's IT department calling a user, a distressed user calling the company help desk, an executive requesting information or a trusted third party (like the president's secretary) requesting information for the president etc. In physical attacks, the role faked is usually that of an employee, of a person of authority within the organisation or a person acting on behalf of one, a repairman urgently called in to fix a problem, an external IT technician paying a support visit, a delivery person delivering urgent, important or bulky items etc. A good impersonation act combined with other techniques can prove very fruitful for the attacker.

Ingratiation. If the Mark of the attack is given a good opportunity to gain favour with or be favourably accepted by persons of power within the organisation, he/she will be more willing to go the extra length and do something that he/she is not really supposed to be doing. A Social Engineer posing as a person of importance has a lot to gain by exploiting this principle. If one also considers the opposite side of the coin, which is the fear of the Mark that the person of power asking for the favour will begin harbouring ill feelings for him/her if the request is not granted, it is made even more obvious that the Mark will fairly easily succumb to the Social Engineer's request.

Conformity. No one likes to be different than everybody else as this could make him/her look out-of-place or even obnoxious. The attacker capitalises on this concept by offering to the Mark those mental shortcuts that justify actions that would seem unreasonable at first. The attacker will let the Mark know that what is being requested of him/her, has already been provided by the Mark's peers or even superiors. The mental shortcut in this case is that if everybody else is doing it, it must be the right thing to do. This information, however, has not been independently acquired and verified by the Mark but it is the product of, usually, indirect hinting on the part of the attacker. A simple, direct statement like: "I have already obtained such information from your colleagues, why don't you give it to me also?" will probably raise

an alarm in the Mark's mind. If however this information is indirectly allowed to surface in a way such as: "When I was talking about the same subject to Ms. Smith (the Mark's superior) she let me understand that…", the Mark will feel more at ease and will be more willing to accept that by releasing he requested pieces of information, he/she is only doing what everybody else has already done.

Diffusion of Responsibility. The attacking Social Engineer will, as a matter of course, ask for sensitive information or require the Mark to perform some kind of action. The Mark will almost certainly hesitate due to the nature of the request, in part because of the responsibility that the Mark feels he/she has to protect the information and/or to uphold certain rules and regulations by not taking the requested action. The challenge for the Social Engineer is to alleviate that burden in order to make the Mark feel comfortable with the situation and proceed as it is requested of him/her. The techniques of diffusing the responsibility include elements of the Conformity technique discussed above, as well as tactics based on what the psychological effect of who the Social Engineer pretends to be with respect to the Mark's position in the hierarchy. If the Mark is convinced that he/she is conversing with the IT manager or one of his/her superiors, the Mark feels less stressed talking about sensitive pieces of data. If the Mark also feels that he/she is doing nothing significantly different than what peers and colleagues are doing, the personal portion of responsibility that the Mark has, suddenly feels as less of a burden.

Friendliness. Although friendliness and saying "please" and "thank you" with a smile, does not suffice for a successful SE attack, it is one important component that must not be overlooked. The Mark not only wants to believe the person on the phone and wants to help out, but, also, it is always more difficult to be "sceptical" or "obnoxious" enough to decide to challenge the caller if the caller is really polite, outgoing and open-hearted. ("If the caller is all of the above, then he/she must be a good guy/girl!"). Even friendliness though has its limits and a good Social Engineer always knows how to not become unnaturally friendly and when to stop extracting information. Stopping at the right time and perhaps "leaving a door open" for use at a later time is always a good practice during SE attacks. This also forms the basis of a relation-building technique employed by Social Engineers where initial contacts are always friendly and not overly demanding, so that trust is gradually built. This attack culminates when the Social Engineer has become enough of a "phone-pal" with the Mark and is being trusted enough to ask the really important questions that are answered by the Mark without a hint of hesitation.

In addition to the above tactics, Makosky (1985) suggests the following three persuasion techniques:

Appeal to or creation of needs according to Maslow's hierarchy of needs (Maslow, 1987): Physiological, Safety, Love and Belonging, Esteem, and Self-actualisation). The attacking Social Engineer will address as many types of the Mark's needs as possible. Flattery may appeal to the Mark's need for Love and Belonging or it will boost the Esteem factor. An urgent phonecall, in the middle of the night, warning of impending financial loss as a consequence of account compromise will definitely strike against the Mark's need for safety, forcing the person under attack to take action while under shock or confusion. Similarly, a request made on behalf of a potentially very angry supervisor or, worse, employer, will immediately hit on the Mark's physiological needs, as the potential of a reprimand that could eventually lead to job loss, automatically increases.

Social and prestige suggestion. While social suggestion is almost identical to the Conformity tactic already mentioned, prestige suggestion has to do with a well-known,

respected person or a person of authority making a recommendation or request. Common usage of this technique is made by Social Engineers who frequently use the names of respected individuals who are well-known to the Mark, in the "name-dropping" phases of their attack. In the SE scenario, the request does not actually have to come from the well-known individual, it suffices to just let subtle hints surface, suggesting that the respected individual has already complied or is in agreement with the request being presented to the Mark.

Use of loaded words and images. A word used in the right context can have an expected positive or negative effect. For example, a sentence phrased as "can you fetch that document for me" instead of "can you find/bring that document for me" will almost certainly have a negative effect on the Mark on the receiving end of that request. This will put the Mark in a rather defensive state of semi-confusion that could help in making him/her more open to suggestion. To make the situation even worse for the Mark, any further suggestion aimed towards the visualisation of an angry boss or another unpleasant situation, could aggravate the Mark's state of confusion and the vicious cycle will continue at the Mark's expense. Hence, even though it might seem as an awkward notion at first, an attacker may indeed choose to use a negatively loaded word such as “fetch” in order to effectively manipulate his Mark.

Finally, Cialdini (2001) presents another persuasion technique with instant persuasion results:

Providing a reason. As described by the author, the desired effect is obtained through the use of the word "because". i.e. simply providing a reason -any reason- for making a request. Cialdini describes an experiment performed by a Harvard researcher named Ellen Langer who kept trying to bypass the lines at the photocopier machine by phrasing her request in three different ways. The first version was: "Excuse me, I have five pages. May I use the Xerox machine because I'm in a rush?" A legitimate reason was given for this request and the request was successful 94% of the time. In the second version, no reason was given: "Excuse me, I have five pages. May I use the Xerox machine?". This request was only successful 60% of the time. One could assume that giving additional information that justifies the request in the form of a reason for it, was responsible for the different success rates. However, the third request formulation was: "Excuse me, I have five pages. May I use the Xerox machine because I have to make some copies?" This version of the request had a success rate of 93%. Clearly enough, neither a real reason was given nor additional information presented that justified the request. The "reason" given was simply a statement of the blatantly obvious. It is concluded that the presence of the word "because" was responsible for triggering the effect of what Cialdini calls "Human Automaticity". The mere use of the word "because" was sufficient to extract a positive response from people and it did not even matter that there was no substantial reason given. In practical terms, this indeed was "instant persuasion". It is also a trick that leaves the victims of SE attacks wandering "what just happened"!.

2.4 Influence Techniques

Cialdini (2001) identifies six fundamental psychological principles: reciprocation, consistency, social proof, liking, authority and scarcity. As these principles direct human behaviour, they effectively give rise to influence techniques that are being efficiently put to use by "*compliance practitioners*" to power their tactics. (The term "compliance practitioners" is used by Cialdini to generally identify those people who try to make others comply with their wishes. Clearly, Social Engineers form a subset of this group)..

Reciprocation. One of the basic principles of human society is that if someone gives something to someone else, then the right thing for the recipient to do is to somehow return the favour. This stems from the reciprocal nature of human society and goes back to the formation of the first human groups. The members of those groups had to share food and skills in order to survive. These basic principles evolved into the interdependencies of modern societies. Clearly, the action of giving and then expecting something in return, on average, characterises all humans. The ways that this principle can be exploited by Social Engineers are many and range from the basic to the really intricate. "Free" offers on the Internet are very common. Most of the time, offers such as screensavers or background images are given away with the sole intention of persuading the recipient to register an email address in order to receive the free offer. At its most innocent form this technique is used to build up an e-mailing list to be used for promotional material or, worse, to be sold to others for the same use. Apart from the resulting spam mail flooding one's inbox, this type of attack is not a security threat and quite popular and successful. Free email services allow one to create an email address, register as requested, only to abandon the address at a later stage when spam becomes a nuisance. However, the Social Engineer may introduce a new twist to this story by directing the offer to particular targets and instead of providing just a piece of well-meaning software, entice the Mark to install software that could perform a secondary spying function in addition to its advertised primary function.

The principle of Reciprocation is also applied in the so-called "Reverse SE" attacks: Such an attack begins with a Social Engineer who either creates a problem and waits for the Mark to fall for it, or somehow convinces the Mark that a fictitious problem exists. When the attacker then appears to solve the problem, the Mark feels indebted and grants him/her the requested favours.

In an even more subtle form of reciprocation, the Social Engineer may make an almost unreasonable request, knowing that it will not be granted. By then making a lighter and less unreasonable request, the Social Engineer augments the odds of this second request being granted, compared to the situation where the second request was the only one being made. Although seemingly unreasonable, there is logic behind this sequence. It should be clear that the Social Engineer's target was to not have the first request granted. The first request was only made to predispose the Mark according to the Social Engineer's plan. When the first request is turned down, the fact that the Social Engineer continues with a less demanding request, constitutes a concession on the Social Engineer's part. The Mark then feels obliged to reciprocate with a concession of his/her own because of the natural tendency to co-operate in the bounds of our societal interaction. Another example is a child who actually wants a hamster, but starts by asking the parents for a horse!

Commitment and Consistency. It is a known psychological fact that people are mostly consistent within their words, beliefs, attitudes and actions, providing consistency and useful shortcuts. These shortcuts make daily life easier because if one remains consistent with previous choices, the load of re-processing all the data in similar situations as they arise is avoided. One simply sticks to earlier decisions. As far as commitment is concerned, one has to just examine the positive load that the word "committed" carries in everyday conversations. If someone is characterised as "committed", then that someone can implicitly be trusted, is considered to be a person who brings results, is highly dependable etc.

The Social Engineer makes good use of this principle by subtly manipulating the Mark so that he/she gradually finds him/herself in such a position that turning down the Social Engineer's request is not an option. This entrapment is based solely on the Mark's previous

conduct towards the Social Engineer. In order for the Mark to be consistent towards the Social Engineer, assuming that the Mark has already granted the Social Engineer's inconsequential small favours, the Mark must keep granting the Social Engineer favours that are being gradually built up over many phone calls and an extended period of time. Doing otherwise, will make the Mark look inconsistent with respect to prior behaviour. In this case, the driving force behind the Mark's obsession with consistency is not, so much, what the public reaction would be if the fact that the Mark is inconsistent was brought to light, but rather the fact that if the Mark turns down the Social Engineer's request, this would force the Mark to holistically re-evaluate his/her position and evolved relation with the Social Engineer, since first contact was made. Not only can this make the whole mental-shortcut-based-on-previous-experience structure collapse (Cialdini, 2001), but it really is not an option in the Mark's mind, since the Mark has to put his/her weight behind previous choices in order to remain psychologically balanced.

This attitude is further enforced by the fact that when person A asks person B for a favour and B grants it, A becomes part of B's personal history of good deeds that contributes to self-esteem. B (who granted the favour) will *have* to like A from that point onwards because B has to justify his/her action by convincing him/herself that this was the right thing to do as A "is a really nice person". It should also be noted that at the time of the favour being granted, B does not have to like A in order to grant the favour, but other reasons may lead B to this decision. Another interesting point is that none of the above necessarily holds true for A. A does not need to like B to ask for the favour, neither B becomes likeable by A after the favour is granted. On the contrary, it is possible for A to develop a dislike for B in order to justify that it was not a favour being granted but that somehow, B being a worse person than A, was obliged to grant A's request.

All that is required from the Social Engineer in order to "cash in" on such attitudes is careful planning. A commitment in the form of a promise on the part of the Mark (direct, implied or even suggested) may be called upon by the Social Engineer in order to "nudge" the Mark at times of hesitation ("Aaaah… but you promised!").

Social Proof. According to Cialdini (2001, p.100) "*we determine what is correct by finding out what other people think is correct*". In part, this principle has already been discussed under Conformity, above. SE techniques based on the principle of Social Proof are most influential on a Mark, under conditions of either a) uncertainty or b) similarity. In the first case, if the situation is so ambiguous that the Mark does not know what to do, providing information on the actions of others will most certainly turn the Mark in the same direction (see Conformity above). In the second case on the other hand, since people are more inclined to follow the lead of others, similar to them, the work of a Social Engineer can be significantly facilitated or significantly impeded.

In a direct attack, the Mark may hesitate in providing the Social Engineer with the requested information. This hesitation indicates uncertainty and the Social Engineer will provide such conformity-related information to the Mark, that he/she will be nudged in the desired direction.

Indirectly, the Social Engineer may benefit by lax security that allows users (i.e. potential targets) to function haphazardly with respect to security measures. This is a regenerative process that is fueled by similarity and leads to an increasingly insecure work environment. More and more users follow the example of others before them and develop disrespect towards security measures. On the other hand, if the proper security policies and directives are applied and the correct incentives are given to workers in order to uphold security and be

rewarded for it, the regenerative effect due to similarity will become positive and lead to augmented security.

Liking. People tend to respond favourably to other people with whom they share some common interest, hobby, birthplace etc. This natural tendency of ordinary people to like and to seek out others with whom they share common characteristics, allows the Social Engineer to achieve his/her goal by pretending to be a person with characteristics similar to the Mark's. Consequently, the Mark instantly develops a positive attitude towards the attacker.

Generalising, people prefer to respond positively to those who they know and like. It is thus imperative that a Social Engineer become "liked" by the potential Mark. Apart from similarity, the most obvious aspect of all, that of physical beauty, is probably the most important factor for which people like other people. Whether it is conditioning or natural selection, research has shown (Cialdini, 2001) that physical attractiveness has an immediate effect on others, who instantly like those blessed with it. An attractive person will most probably also be considered to be kinder, more intelligent, more talented and, of course, more trustworthy than he/she really is. As a result, attractive people can be more persuasive than others

Liking can be achieved by familiarity over repeated contact (this was also mentioned under Friendliness, above). Also, if the circumstances under which contact takes place are positive rather than negative, liking is much more certain to be achieved sooner than later.

In SE attacks, these techniques are used to boost the level of liking that the Mark holds for the attacking Social Engineer. In physical attacks, the external appearance of the attacker plays a major part in the success of the attack. In attacks over the phone and the Internet, a deep, resounding voice can contribute to the success of the attack. Additionally, "chatting-up" the Mark in order to establish some common points of reference on which to build a trust relationship can make or break a successful attack. Stretching out the contacts in time can also help a Social Engineer build a trust relationship over the phone with the Mark and use that trust build-up when the attack culminates.

Authority. A false appeal to authority is one of the preferred methods of operation in SE attacks. The reason for its success is based on the respect that the average person has for authority. Furthermore, persons of authority are considered to normally possess high levels of knowledge, wisdom and power. Hence, a mental shortcut can be established by deferring the complexity and responsibility of decision to such persons. This, in effect constitutes an automatic response to persons of authority. Alarmingly, though, as it is also discussed in the above reference, this automatic response tends to be to the symbols of authority and not necessarily to its credential-backed substance. Such symbols have been shown by research (Cialdini, 2001, p. 201) to be titles, clothing and automobiles. These symbols, used by the Social Engineer and combined with the right attitude and composure, can effectively project a convincing, albeit false, image of authority that will evoke an automatic response from the targeted Mark. Further, the Mark tends to underestimate the effect of authority pressure on his/her behaviour, thus making the attack more difficult to identify and protect against.

Scarcity. According to this principle, a higher value is assigned to goods and services that become less available. As this happens, their apparent value increases and so does the appreciation of their quality. Psychological Reactance theory dictates humans respond to loss of freedom by stronger desire (Cialdini, 2001, pp.208-218). Hence, something that becomes scarce also becomes more desirable.

Although it is clear that the scarcity principle applies more to deception based on fraudulent on-line auctions, the same principle can be used to enhance the effect of many other

types of SE attacks. For example, in the case of the "well-meaning" e-banking employee who wakes up the Mark in the middle of the night to inform him/her that money is being transferred out of his/her account and subsequently makes a request for the Mark's password to block the transaction, an extra piece of information about how the Social Engineer is risking his/her position in the bank to help the Mark is also usually supplied. Apart from the sense of gratitude that the Social Engineer is trying to conjure, the element of scarcity of the supplied service is also indirectly invoked. The Mark realises that if he/she hesitates to give the requested information to the Social Engineer, the offer may be swiftly withdrawn because of the impending risk of job loss for the bank employee / Social Engineer. This scarcity element makes the quality and sincerity of the offer to appear higher, and thus provides the Mark with a mental shortcut and the Social Engineer with the information he/she is after.

In the case of "phishing" attacks over email, Internet Relay Chat (IRC) etc, an offer valid "for a limited time only" or "for the first X replies received" may trick the Mark into thoughtlessly and impulsively submitting personal information that will be used to impersonate him/her during a later phase of the SE attack or, even worse, be used to directly gain access to a system.

2.6 Exploitation of Attitudes and Beliefs

Apart from the tactics of influence and persuasion already discussed, Social Engineers make use of several shortcomings in the function of the systems they target for compromise.

One such shortcoming is the lack of the flow of information about an attack in large, and mostly authoritarian, hierarchies. This is a well-known situation among Social Engineers and attackers who justifiably consider most hierarchies of this type to be governed by what is called in Hacker-jargon the "SNAFU" principle. According to TheFreeDictionary (2010), the acronym originates “from a WWII Army acronym for 'Situation Normal: All ****ed Up': True communication is possible only between equals, because inferiors are more consistently rewarded for telling their superiors pleasant lies than for telling the truth”. Despite the annoying vulgarity of the acronym, this principle describes a situation that has definitely been holding true for millenia. It is a well-known fact that military couriers in the times of the ancient Persian empire were either treated as honoured guests when they brought news of victory from the battlefield, or summarily executed if they brought news of defeat. (This might well be the source of the expression “don’t shoot the messenger” that survives until the present time). In today's terms, it is not unusual to treat someone who raises an alarm, as if he/she is the cause of the alarm! In this most ostrich-like behaviour, ordinarily vigilant employees feel compelled to "turn a blind eye" and ignore the observed signs of a security breach. This is the same type of hierarchy where an impersonation attack by a Social Engineer based on a false appeal to authority, would be more successful. Consequently, the hierarchy's decision-makers become progressively disconnected from reality, leading to the systemic failure of the hierarchy itself. A term currently gaining acceptance that is used to describe such situations that lead to chaos is "Discordianism". This is a philosophy / religion / joke that was created around 1958 in order to reflect, "formally" describe and discuss the principles of chaos, confusion and disorder in the world (University of Virginia, 2005).

Another attitude exploit stems from the conventional fact that when two parties engage in a transaction or communication, this is done "in good faith", unless, of course, there are serious indications to the contrary. As it holds true in any case of pre-meditated deceit, the deceiver

(the Social Engineer for the purposes of this work) has the Mark at a disadvantage. The Mark's attitude of initially acting in good faith by default, effectively delays the triggering of mental alarms and consequently impedes reaction and an efficient response to a SE attack. This is an issue that must be addressed by effective counter-measures that function by making potential targets less naïve and gullible, thus minimising their reaction time to raise alarms.

2.7 Alternative Routes

If a Mark can not be persuaded to relinquish the requested data or perform the actions required of him, there always exist harsher ways of getting him/her to comply. Extortion has always been such a way. Although, strictly speaking, extortion does not constitute a SE attack per se, it is more than just conceivable that sensitive information concerning the Mark can be collected through SE methods (or even simple Internet searches, nowadays) and subsequently be used against him/her in an attempt to extort further information. It is no secret that Private Investigators have been using SE tactics to gather information on their subjects, long before the term was coined to describe the principle under which these tactics worked. Regarding the subject of extortion itself, further discussion is beyond the scope of this work.

2.8 Old Tricks, New Dogs

All of the techniques described in the current section of the paper are e-variations on a very old theme. Marketers, politicians, advertisers, sales people and con artists have been using them for ages to convince their Marks to respond positively to their suggestions. Amazingly, although these methods were identified and brought to light decades ago, they are still very successful and the fact that computer-age Social Engineers use them, is a testament to their effectiveness. The average user, in any Information System context, is thus very vulnerable and the principal means of defense are proactive education and distribution of information relevant to these methods of attack.

3. PROTECTION AGAINST SE ATTACKS AND THE INTRODUCTION OF Ψ-WALL

In this part of the paper, an attempt is made to draw from the above analysis of the psychological aspects of SE methodology and devise an improved strategy for strengthening defenses against SE.

When preparing defenses against attackers who employ SE techniques and methods, the focus should not only be on strengthening physical security, detailing a firewall policy, adding protection to servers accessible over the Internet and securing internal network connections and file access. Security should also address direct attacks against legitimate users of the computer systems, but building a firewall to prevent such attacks, is much more difficult.

As long as people are accessible through a phone line or email, then they are vulnerable to SE attacks. In addition to creating stronger security policies and implementing controls on physical security and data protection, if SE attacks are to be blocked, it is more important to increase awareness regarding SE methods of operation and even educating users on how to

turn the tables on the attackers. In effect, this approach constitutes the psychological equivalent of a firewall, or "Ψ-wall" (From the greek letter "Ψ" -correctly pronounced "Psee" but more frequently as "Psi"- that serves as an internationally accepted shorthand notation for "psychology").

3.1 Increasing Awareness (through Constructive Brain-Washing?)

Since SE attacks are based on psychological manipulation and influence / persuasion tactics, the only way to block them is to inform the users on applied psychology techniques and alert them to the tricks of the trade as these evolve. As is the usual requirement with all security policies and practices, the responsibility for the implementation of such policies lies with the management. A strong commitment to continual research, enforcement of new directives and re-evaluation, must precede any related effort if the effort is to bear fruit.

Although security policies must be in place and an incessant cycle of effectiveness measurements and updates must be established, most importantly, it is the Users that must be educated and constantly be re-educated, in order to keep up with the rate of evolution of threats based on SE methods.

The attack on the problem must be two-fold. First, the issue of security must be presented in such a way that it becomes a very high priority for the average user. Second, after making security "second nature" to the users, the weapons to fight this battle against SE should be handed out in the form of practical tips, tricks and methods designed to nullify the success rate of SE attacks.

One way to direct the attitude change of users towards making security a very high, if not their first, priority, is to "bombard" them with pro-security messages. These messages must be *variations* on the same theme, always urging users to make security their priority. It is common empirical knowledge that the least effective type of message directed to a user is the one appearing everyday on his/her login screen. It was shown by Sears and Freedman (1965) that even if new ideas are not included in a message, the expectancy alone of new ideas in the message, makes the message more persuasive. In practice this means that if security-related messages are re-phrased and re-introduced, they become more persuasive than just re-stating a single message. Thus, the idea of producing and distributing "trinkets" such as catchy mouse pads, coffee mugs, pens, calendars etc, bearing well-designed pro-security messages, should be quite successful in promoting security as a necessity that must be upheld by everybody.

The above method is only the first step in creating an effective Ψ-wall. It must get the message through that all security issues cannot be addressed by technical measures alone. The second step is to make all employees aware of the methods employed by Social Engineers. This can be in the form of short enactment videos in the usual "Discovery channel" hands-on-experience format. The video clips can be distributed over the corporate network or shown in staff meetings and any other gathering opportunity. Although there should be security awareness sessions per se, these airings do not have to be limited to dedicated meetings but should take place as frequently as possible. Such a visually rich method is much more effective than any other kind of textual distribution because, in our day and age, the motto "One picture is worth a thousand words" is stronger than ever.

3.2 Psychological Defenses (the Brick and Mortar of the Ψ-wall)

One of the main targets of the awareness programs must be to address techniques against SE attacks exploiting the psychological characteristics of humans. The authors start with defense recommendations for influence techniques as presented by Cialdini (2001) and adapt them for the scope of this work. Before a defense can be raised, though, the attack must be identified as such.

Despite the nature of the attack (be it physical or over the telephone), when interaction between the Social Engineer and the Mark takes place, there are tell-tale signs that the attacked employee should always be on the lookout for and constantly use as "filters" for any and all claims made by an unknown requester.

These, typically, are:

- Requests for forbidden information
- Refusal to give contact information
- Logical "holes" and small mistakes
- Name-dropping
- Rushing
- Intimidation
- Naïvety
- Flattery

Although not complete, this list gives a clear indication of what to look for.

Furthermore, personnel should avoid taking mental shortcuts based on appearances that could help in the success of an impersonation attack. Hence, a person in brown uniform carrying parcels must not be assumed to be a legitimate courier and someone dressed in an expensive suit and tie is not necessarily a high-ranking executive. Mental shortcuts must consciously be blocked and first impressions must be discredited. Decisions must always be based on hard facts such as asking proof of identification. While courtesy should always be in order, proper security procedures must take precedence.

Having identified the possibility of an SE attack, defenses against influence techniques should be applied:

Reciprocation. When the psychological / social rule of reciprocation is invoked, the attacker has already granted the Mark a favour. The Mark then feels obliged to return this favour or be scorned as an ingrate. Usually, the nature of the favour will be such that the favour would not be granted based on the Mark's free will, and this is why some kind of reciprocation must be called upon. So, the dilemma the Mark finds him/herself in is between granting a favour that could lead to security breach or be scorned upon and also have an immediate reduction of his/her self-esteem. The fact that the reciprocation rule is called upon should be a dead give-away for the possibility of a SE attack. The Mark should realise that the previous favour is actually being used against him/her and thus take steps towards defusing the reciprocation rule.

It would be irrational to reject all genuine favours and all offers. This would quickly become a social problem. Nor is it easy to distinguish between a genuine and a trick offer at the time that it is granted. However, in due course the sincerity of the person making the offer or doing the favour will be proven. At that time, the original offer can be re-evaluated and if found to be insincere (in the context of the favour that is requested in return), the obligations resulting from the reciprocation rule be nullified. In retrospective, it is only genuine offers that

should be met with equivalent ones. There is no such rule or obligation for trick favours or offers.

Commitment and Consistency. According to previous discussion, the Social Engineer puts these two principles to use by subtly manipulating the Mark so that the Mark gradually finds him/herself in such a position that turning down the Social Engineer's request is not an option. This entrapment can only be reversed if the Mark pays attention to the "gut feeling" he/she has when faced with the Social Engineers request. To resist the pressure based on Commitment and Consistency, the Mark must develop the ability to continually re-evaluate the initial decision (or chain of decisions) previously made, that lead to commitment and to the situation at hand. The crucial question for the Mark to answer would be "knowing beforehand what I now know, would I have made the same initial commitment that lead to this situation had I been able to reverse the clock?" If the answer is negative, (which in such situations always is), the problem should be addressed directly and it should be explained to the Social Engineer that granting his/her request would be a breach of security and that compliance is not an option.

Social Proof. When the Social Engineer subtly or directly suggests a course of action to the Mark, he/she does so by either providing false data (Mr. So-and-so has already given me this information) or by using a true basis of conformity and at the same time twisting it to serve his/her purpose. In either case, a convenient mental shortcut is forced upon the Mark in order to have him/her comply with the Social Engineer's request. In effect, the Mark is supplied with false social proof data. The only possible defense against this technique is for the Mark to first evaluate the validity of the data presented by the Social Engineer and then take into perspective that even if this data is true, the actions of his/her peers simply do not form the only basis for his/her decisions and subsequent actions.

Liking. Social Engineers are willing to spend a lot of effort in building a portrayed persona that is well-liked by the Mark in order to befriend the Mark and thus soften the impact of a request and increase the probability of compliance. Thus, the potential victim of such an attack must be aware of this technique and be alert to the potential situation of developing an undue liking for a requester. The potential victim must be sensitive both to the extent of the liking as well as how fast this has come to occur.

Anybody can befriend anyone else very fast under false pretences of similarity, cooperation, association and compliance to the other's whims and desires. Other methods include flattery or, simply, graceful social interaction. Physical appearance also plays a decisive role.

Thus, upon realising that the "liking level" for a requester is unjustifiably high under the circumstances, the Mark must classify that requester as a potential Social Engineer carrying out an attack. The request must then be dissociated from the relation developed with the requester through social interaction. In this state of dissociation, the true nature of the request must be objectively judged and the potential for a breach of security resulting from complying with the request must be identified. If such a security breach is possible, needless to say, the request must be denied.

Authority. It has already been analysed, that a Social Engineer's false appeal to authority can bear fruit in the course of an attack. As far as security is concerned, all claims to authority must be challenged and all persons must be identified as to who they really are, irrespective of their position in the hierarchy of the organisation. This can be achieved by disregarding the effect of obvious status symbols such as an expensive suit or a company executive car and taking into consideration only hard evidence, like a secure ID badge etc, in order to

authenticate the individual. In order to accomplish this task, the correct procedures must be in place so that employees can protect themselves against spiteful, retaliatory attacks, by simply sticking to procedures and "going by the book".

Scarcity. The reactions to this psychological principle are difficult to control. This is because these reactions have an element of emotional arousal and while in this state, straight thinking is practically impossible. Perhaps the only means of defense would be to use this emotional arousal as an indication of a possible SE attack. Steps can then be taken to suppress the arousal and attempt to rationalise the situation. If the interaction with the Social Engineer takes place in real time, the element of rushing will also probably be very strongly present. The combination of these two signs put together may help to surely identify and efficiently resist the attack.

3.3 Supporting Physical Measures

One of the initial arguments of this paper was that current IS security standards and best practices do not deal effectively with the aspect of human psychology and its role in IS. Under no circumstances should this be misinterpreted and the proposed physical and technical measures be rejected. Such measures are essential and do effectively support the general effort. A physical attack on the target premises requires meticulous preparation on the part of the Social Engineer. It demands that the attacker acquires such a state of elevated psychological resilience as is necessary to withstand the pressure inherent to the attempt. Furthermore, the attacker must have attained a special ability to constantly monitor and actively manipulate the psychological status of any potential challenger in order to allow the planned attack to unfold. Clearly, all of the above are not always possible, hence the assailant must also have an escape plan from the premises in case things do not turn out as expected. If strict physical security is applied both on entering as well as leaving an establishment's premises, this could constitute an effective measure towards better control of SE attacks at the physical level. Other physical measures such as entrance and exit turnstiles or the obligation for all members of staff to wear double-sided badges with clearly visible ID pictures could also diminish the psychological manipulation edge that the attacker might have upon the Marks.

3.4 Security Compliance Measurement

Measuring the degree of effectiveness of any implemented security measure is difficult to begin with. Nevertheless, this constitutes an important factor in the continual re-assessment of the current security policy and a most valuable guide in pinpointing problem issues and addressing them.

In principle, the effect of SE attacks is difficult to operationalise. Collins (2000, p. 68) defines Operationalisation as the process of transforming a theoretical concept into an empirical variable, i.e. making the defined concept measurable. Consequently, measuring the effectiveness of a set of countermeasures designed to block SE attacks (the Ψ-wall) is at least as difficult as operationalising the effects of the SE attacks themselves. This is mainly due to the non-descriptive nature of controls against SE that are based on purely psychological techniques.

In short, how can issues like the psychological effect of an awareness campaign on individuals or the actual effect of the psychology-laden process against a potential SE attack be measured?

To operationalise a concept such as the effectiveness of the proposed Ψ-wall (in other words the level of defense against SE attacks), it is imperative to identify all of its dimensions or "indicators", where "*an indicator is an observable measure*" (Collins, 2000, p.68). However, the operationalisation of the effectiveness of the Ψ-wall goes beyond the scope of this paper and constitutes a subject which is currently under research.

3.5 Promotion of Higher Ethical Standards in the Workplace

Reekie (2004) introduces the need for the creation of a set of ethical obligations stemming from the organisation's responsibility to the client, as well as its responsibility to itself to protect its interests. Additionally, the need for inclusion of relevant countermeasures in security policy implementation is supported.

In the context of guarding against SE attacks, the promotion of ethical standards in the workplace is of paramount importance. SE attacks count on some aspect of human psychology to produce results. Whether this aspect is fear of authority, the natural willingness to help, the application of convenient mental shortcuts, the reluctance to become disliked etc, the SE attacks work because people are simply left to their own devices as far as their reaction to an attacking Social Engineer is concerned.

By promoting ethical standards in the workplace, feelings like (but not limited to) fear of powerful people of authority, ingratiation and the feeling of risking being disliked when challenging a fellow employee who might be a potential attacker, will be reduced. In a work environment where ethical standards form the basis for everyday activities, there is no space left for acts of intimidation, coercion or exploitation. Thus, the attacker is faced with a greater challenge than expected or planned for.

Furthermore, in an ethically-bound environment, incident reporting becomes more efficient as the effectiveness of proper channels of communication between the base of the organisation and its highest levels increases. This invariably leads to better defense against SE attacks.

3.6 Monitoring Social Engineering Attempts

All SE attempts should be reported and logged centrally, evaluated and the countermeasures coordinated. Reporting procedures for security incidents as well as the formation of a coordination centre is also prescribed in the directives of the ISO/IEC 27002:2005 standard (ISO/IEC, 2005). However, in the context of this standard, the coordination centre and reporting procedures may not cater as efficiently as possible for the particular case of SE attacks given that immediate response and even guile are required in order to beat the attacker in his/her own game. The evaluation of the relevant ISO/EC 27002:2005 controls though, is, again, beyond the scope of this paper and have been examined by Frangopoulos (2007). Ideally, the existence of such a centre will assist in identifying problem areas within the organisation and will also help those responsible for security *to identify the nature* of the attacking Social Engineer's interest. This in itself is of great importance because it can give clear indications regarding what the motives behind the SE attacks are. Concise reports made

by the SE attack monitoring authority could give the management information on important issues such as a secret project being compromised or that attempts are made to extract financial information before a takeover etc.

The most difficult part is for personnel to identify a SE attack as one and report it. Ideally, it would also be very useful to let the attack run its course in an effort to identify its ultimate target. This, however, is clearly beyond the abilities of the average employee. Manipulating the manipulator would be a challenge for even the most cunning expert on counteracting SE attacks.

Thus the most reasonable expectation would just be for the average employee to be able to identify an attack and report it as a result of the whole security education, training and awareness program. The employees manning the monitoring and evaluation centre though, should be highly specialised security professionals who can sift through all the reports, weed out the false ones and extract information of value to the management or the top levels of the hierarchy. Furthermore, they should be able to predict (to some degree) future attacks based on forming patterns and thus call for raised levels of alertness and strengthening of security measures. Most importantly, they would form the mortar holding together the Ψ-wall.

The issues discussed in this section can be placed into perspective by figure 1.

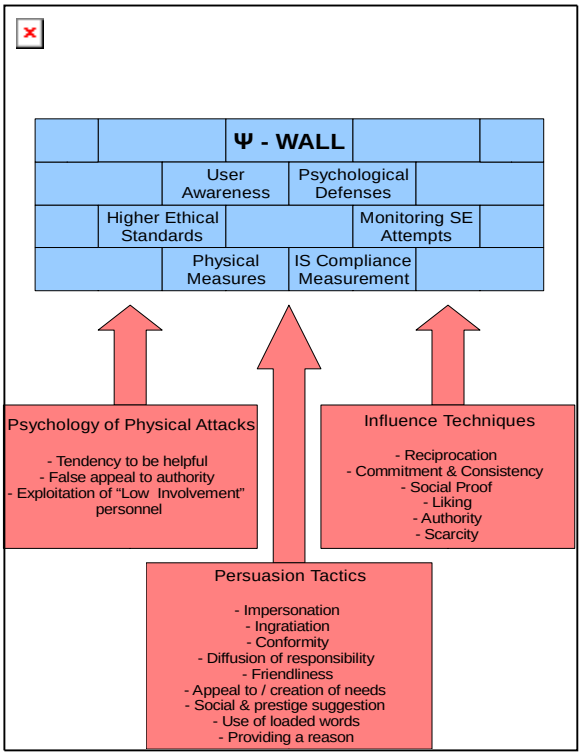

Figure 1. The Ψ-wall principle

4. CONCLUSION

In this paper the fundamental psychological aspects of SE were presented. The common psychological loopholes that Social Engineers exploit as well as the techniques that they use were analysed. This analysis was backed by a presentation of the most important Persuasion tactics and Influence techniques as modern psychology accepts them.

Due to the complicated and highly non-technical nature of SE attacks, it is argued that in order to defend against them, an organisation must invest upon its human resources and, most importantly, their psychology. Traditional technical measures simply do not offer sufficient provisions to stop non-technical attacks such as SE ones. Thus, a case is presented in support of psychological defenses with the objective of strengthening security policies and improving security mentality and practices in an attempt to provide better protection against SE attacks.

It thus follows that a "psychological Firewall" or "Ψ-wall" must be built mainly through awareness and psychological training programs. The objective of the programs should be to expose the employees to the reality of SE attacks before they actually have to face one. Mastery of psychological defenses against these attacks can be taught to a certain extent, as is the ability to at least identify them.

The issues of measurement and compliance were addressed through the proposed use of operationalisation methods and the identification of relevant indicators.

It was also maintained that raising ethical standards in the workplace can help against SE attacks as many of the psychological barriers of employees that the Social Engineers thrive upon simply fall apart.

Finally, the importance of auditing and penetration testing was stressed as a means of raising alertness, and the need for a central point of coordination against SE attacks was highlighted.

In the case of SE attacks, the war is fought between the mind of the attacker and that of his victim. If there is a chance to counter the acts of the Social Engineer, the potential victim must acquire the ability to recognise and resist the psychological "nudges" of the attacker as well as to raise an alarm. In effect, it is the human psyche that becomes the last line of defense in this battle.

REFERENCES

BERNZ, c. 2000. *The complete social engineering faq! By Bernz* [online]. Available from URL: http://packetstorm.rlz.cl/docs/social-engineering/socialen.txt [Last access on Dec 13, 2010]

CIALDINI, R. B. 2001. *Influence: science and practice - 4th ed.* Massachussets: Allyn & Bacon.

COLLINS, K. J. et al. 2000. *Research in the Social Sciences, Only study guide for RSC201-H.* Pretoria: University of South Africa.

FRANGOPOULOS, E. D. 2007. Social Engineering and the ISO/IEC 17799:2005 Security Standard: A Study on Effectiveness, MSc Dissertation, University of South Africa.

GRANGER, S. 2002. *Social Engineering Fundamentals, Part II: Combat Strategies* [online]. Available from URL: http://www.securityfocus.com/infocus/1533 [Last access on Oct 10, 2004], Also available from URL: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies [Last access on Dec 13, 2010]

HARL, 1997. *People Hacking: The Psychology of Social Engineering* [online]. Available from URL: http://packetstorm.rlz.cl/docs/social-engineering/aaatalk.html [Last access on Dec 13, 2010]

ISO/IEC. 2005. International Standard ISO/IEC 27002:2005. Information technology -- Security techniques -- Code of practice for information security management. Geneva: ISO Copyright Office.

MAKOSKY, V. P. 1985. Identifying major techniques of persuasion. In: *Teaching of Psychology*, 12, pp. 42-43

MASLOW, A. 1987. *Motivation and Personality*, 3rd edition. New York: Harper Collins Publishers.

MITNICK, K. and SIMON, W.L. 2002. *The Art of Deception. Controlling the Human Element of Security*. Indianapolis: Wiley Publishing Inc.

REEKIE, C. M. 2004. The emergence of obligation rights in ethical information security awareness. In: *Peer-reviewed Proceedings of the ISSA enabling tomorrow Conference 2004 - Research Papers Section*. June 2004. ISBN 1-86854-522-9

RUSCH, J. J. [ca 1999]. *The "Social Engineering" of Internet Fraud* [online]. Available from URL: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm [Last access on Dec 13, 2010]

SEARS, D. O. and FREEDMAN, J. L. 1965. Effects of Expected Familiarity with Arguments Upon Opinion Change and Selective Exposure. In: *Journal of Personality and Social Psychology*. **2** (3) 420-426.

SUTPHEN, R. [No date]. *Battle for Your Mind: Introduction* [online]. Available from URL: http://www.sibyllinewicca.org/lib_psychology/lib_p_brain.htm [Last access on Aug 8, 2004], Expanded version available from URL: http://www.scribd.com/doc/36364981/Hypnosis-Dick-Sutphen-The-Battle-for-Your-Mind-Mass-Mind-Control-Techniques [Last access on Dec 13, 2010]

THE FREE DICTIONARY. 2010. *TheFreeDictionary* [online]. Available from URL: http://encyclopedia2.thefreedictionary.com/SNAFU+principle [Last access on Dec 13,2010]

UNIVERSITY OF VIRGINIA, 2005. *The Religious Movements Homepage Project - Discordianism* [online]. Available from URL: http://religiousmovements.lib.virginia.edu/nrms/disc.html [Last access on Feb 22, 2007]