Social engineering in the world of emerging communication technologies

Seppo Heikkinen, Tampere University of Technology, Finland

***Abstract*— Social engineering is the art of getting people to comply with your wishes. It takes advantage of the psychological aspects of the human mind and the social interaction patterns between people. With this approach a skilled social engineer is able to execute an efficient and cheap compromise of security without having to invest in breaking technological security measures, such as firewalls. A social engineer can also combine technological means to achieve the attack objectives. This includes contacting people by means of communication technology and luring them into executing actions, such as installing malware, which the attacker can use to further compromise the systems. This paper discusses the different aspects of social engineering and investigates the methods that have been employed in successful attacks. It also points out some characteristics of the upcoming technologies that could be used to launch attacks, so that the designers of future systems can take these into consideration.**

***Index Terms*— communication systems, psychology, security, social engineering**

I. Introduction

How many of us think twice when a repair man comes to collect a computer or a person from an outsourced cleaning company comes to clean our office? Are we just happy to answer to their smiles or do we stop to think that maybe we should check their credentials, like officially looking personnel card, and pay attention to what sort of information they are exposed to? People may not often think how much information they can reveal in a casual conversation and what might be the consequences, if we are friendly toward our fellow humans and try to help them with their problems as most of us probably have been taught to do back when we were young. It might be that the circumstances are carefully crafted by a social engineer, an individual skilled in reading people, who is after some valuable information or financial gain.

Social engineering can be understood as the art of deception. It is the science of getting the people to comply with your wishes [1]. As the social engineering relies on human to human interaction it can be used to target the weakest link of computer security, the human user. It is much easier and cheaper to try to hack the humans than the security systems. Note that social engineering as a concept is much broader, though, and is not solely limited to information security.

The idea is to exploit the emotional states of a human, during which he or she is most vulnerable to persuasion or can be deceived into doing things rather than stopping to think whether the arguments given are reasonable in the current context, i.e. the person is taking a mental shortcut. Also, as [2] shows, the individual persons do not tend to view themselves as potential targets as they might not see themselves as significant factors or possessing interesting enough information. This kind of mindset is likely to make those people susceptible for social engineering attacks. Similar views were expressed in [1], which perceives that the level of involvement plays a part in how people react to information disclosure: People with low involvement do not feel directly affected by the request and are less likely to evaluate the information request thoroughly. It is worthwhile to note that a social engineer might not be after some valuable data, he or she might be quite content if physical access is gained and some expensive hardware, like new laptop, is acquired, i.e. the ultimate objective is to carry out a simple theft. Also, the attacker is not always after getting something, but the motivation could be to get someone to do some action as well. In other words, social engineering is used to modify the behaviour of the people.

Even though in the end the companies are the ones that are likely to suffer the most losses (think, for example, industrial espionage), but also individuals can be the ultimate target of social engineering. This is prominent, for instance, in the cases of identity theft, which can result in the loss of money, reputation, or credibility.

The new emerging technologies and networks can provide new ways of contacting and affecting the decisions people make in their every day life. The people engage in social networking in various ways that are yet not fully studied. This virtual way of life provides new avenues for abuse as the mindset of the people does not change as fast, and it may be hard for a person to evaluate what is authentic and what is not. This is especially true if authenticity and usability factors do not support each others, i.e. weak design choices do not support the user decision process. This enables the clever individuals to transfer the age old psychological gimmicks into this new world in unexpected ways and guide the reasoning and actions of the people. This can be further enhanced by technical exploits or can provide avenues for injecting such exploits.

In this paper we discuss the aspects of social engineering and what types of attacks can be launched. Due to the nature of the problem it is hard to give any direct answers how to solve it, even though some potential countermeasures and principles are given here. The main motivation, however, is to raise the awareness to the potential threats, so that the designs of the future networks are aware of the consequences and can employ the suggested principles to mitigate the ill effects.

The paper is organised as follows. The next section discusses the general aspects of social engineering and the

associated attack cycle. The third section provides information on psychological factors behind the attacks. The following section introduces several different categories of attack methods. The fifth section discusses the potential flaws that the emerging systems could exhibit, thus providing avenues for attacks. In the sixth section suggestions for countermeasures and relevant principles are given. Finally, the seventh section concludes the paper.

II. General aspects

Social engineering can take many forms and can have many different kinds of goals. Basically, though, it tries to influence people to view the attacker in favourable light by taking advantage of the human interaction aspects, human behaviour patterns, and the social structures. In other words, the attacker tries to create a state of trust with the victim, thus making it easier to gather information or make the victim execute some unwitting action. It can also be as simple as making the victim to overlook policies and allow the attacker to perform an unauthorised action, such as accessing company facilities.

Employing social engineering techniques can be quite a natural thing to some in their every day life "to get the job done", but within the scope of this paper the objectives are more malicious in intent and contain incentives to get some financial gain or defame people or organizations. Even though influencing is the main modus operandi of social engineering and, along with fabrication, basis of most of the other actions, we can still make the following kind of categorisation for the actions used to attain the attack goals, although the used methods to achieve these different goals can be similar and several can follow consecutively in order to accomplish a consequence, which usually is a security compromise of some sort:

- Influencing - make people feel something
- Extracting - make people give something
- Tricking - make people do something
- Bypassing - make people allow something

The first type happens in every day situations, when people interact with other people and try to affect the way they are viewed by others. This can be rather subconscious activity and is also affected by way of speech, clothing etc., but it can be more active by nature, like when giving fabricated impressions. The second type is aimed at extracting useful information that can be used later on to better accomplish a certain goal or execute additional social engineering. This also includes acquiring physical material. The third type is clearly targeted at fooling people by giving them misinformation or otherwise creating a sense of trust, thus achieving the goal of making the victim do some unwitting action, like clicking a malicious web address or giving money. The fourth type tries to make it easier to bypass systems either electrical or physical and may require just enough confidence. This could be, for example, physical access to some facility through a door without anybody stopping. In other words, this also includes omission, so that people leave something undone.

It is worthwhile to notice that much of this categorisation is based on the semantic interpretation of the terms. As mentioned, influence could be seen being the basis of social engineering, thus every other category could be derived out of it. Tricking, for example, has a very thin line separating it from influencing, even though influencing usually is more preparatory in nature.

Another possibility is to view this from the point of a social engineering attack cycle, which consists of four different phases (see Fig. 1) [3]. First phase entails gathering of background information, which enables the attackers to better succeed in developing relationships with their targets. Once this position of trust is achieved, it is exploited by getting the target to reveal information or perform actions. When the target has completed the task, the execution of the attack cycle is complete and the attacker has achieved his goal. This can be followed by yet another cycle to gain further privileges or information as it is less conspicuous, if the attacker only tries to achieve small objectives at the time and with the same victim. In essence, the separate requests to different people can seem innocuous enough to each individual, but the combined results can have a powerful effect.

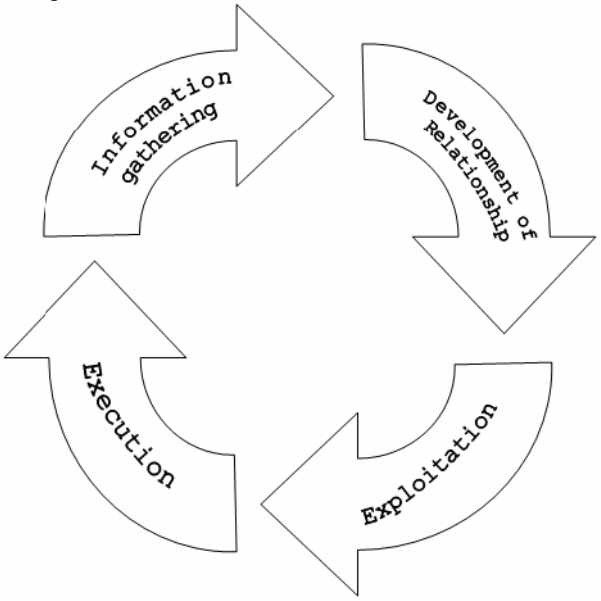

Fig. 1. Social engineering attack cycle

As an illustrative example of this cycle consider a simple case, where an attacker first gathers information, such as names, on the IT support persons and the victim. Then the attacker crafts an email, which seems to be coming from the IT support. The victim may be fooled by the correct looking message and trusts the information, which could be a warning about the need of some security update. Based on the context the victim clicks the accompanying link, which causes malware to be downloaded and installed on the victim's computer, thus completing the attack cycle.

III. Psychological triggers

There are several psychological factors that can influence the decisions people make when dealing with other individuals and a skilled social engineer is able to use any combination of them to guide the victim into a suitable emotional state. In this state he or she is not making rational decisions and instead takes mental shortcuts when evaluating information, ultimately behaving according to the

wishes of the attacker. Not all of these triggers are likely to work against a particular person, but a good social engineer is also able to read the victim's responses and change the tactics accordingly. Some of the factors can be categorised as the following [4][5]:

- Authority
- Scarcity
- Liking and similarity
- Reciprocation
- Commitment and consistency
- Social proof
- Diffusion of responsibility
- Overloading

In certain situations the people are highly likely to respond positively to the requests made by the authority (see, e.g., [6] for Milgram's famous experiment). This can be further enhanced by intimidating behaviour, which can imply that if the individual does not fulfil the request there are personal consequences, like getting fired etc. This can put the victim into a strong emotional state with lessened ability for logical thinking and evaluation of the legitimacy of the request. In technical matters the people might also view support personnel as authority, especially if they themselves are less literate with technology. The attacker can make claims or even threats that are not true, but the non-technical person does not have a way of knowing that. The scared users are likely to be less rational and can reveal information or execute actions they clearly should not.

Scarcity can be used as an excuse for expediting the evaluation process. In other words, if something is on short supply or available for a limited period of time, the victim's desire to obtain the said thing may be illogically heightened, and the sense of urgency demands quick actions. This could include, for example, a possibility to win a prize of some sort.

We tend to like people who like us or, as the saying goes, "it never hurts to be friendly". Expressing liking or similar interests might be enough to view the other person favourably and feel sympathy. This can then blur the judgement of the victim and open an avenue for social engineering attacks. A bit of flattery will further increase the possibility of the victim taking a mental shortcut especially if this is coming from a person of opposite sex. Similarly, a worker might feel that if the password is not shared with a supposed colleague within some reasonable request, they would be giving a statement of mistrust, which might be viewed as insulting, thus compromising the social relationships [2]. The same could happen even with the token based authentication mechanisms.

As stated in [7], it is a well-recognized rule of social interaction that if someone gives us something, we feel inclination to provide something in return, i.e. reciprocate. It is quite natural to help someone in belief that we may need help in the future and can rely on people we have helped before. This is especially true in corporate environments as, for example, Kevin Mitnick, a famous hacker, has perceived [8]. Similar behaviour can also be observed in the case of first making a larger request and then getting a more favourable response towards a smaller request [9].

People have a tendency of trying their best to fulfil the commitments they have made, especially in their workplaces [5]. If they do not succeed in doing what they have promised, it can cause a feeling of guilt, even though a closer evaluation might reveal that doing it might be foolish. Additional thing is that the people have a tendency to believe that people are expressing their true attitudes, i.e. the first reaction is not to suspect a lie unless there is strong evidence to the contrary [4]. Also, some may feel it is their moral duty to proceed with actions that they believe to be important and failing them could lead to dire consequences either to the company or to a supposed work colleague.

Social proof means that in bigger crowds the people are likely to observe more what others are doing and saying, thus letting others influence their own decisions [1]. This can be described as social pressure, which makes people reluctant to go against the attitudes of the majority. In other words, it is easier to "go with the flow" than to risk embarrassment. It even can be enough, if it is only implied that others have already complied.

Diffusion of responsibility means that the victim is lead to believe that the responsibility of the decision is not solely theirs. The victim can think that he or she is part of some bigger group, which is equally responsible for the actions, or the victim is lead to believe that others in the group have already provided similar information. Also, the victim may have the idea that he or she is just "following orders", hence the actual responsibility is someone else's.

Overloading can happen when the individual is flooded with information and as a result just concentrates on absorbing rather than evaluating it. This is enhanced with using technical jargon that the receiver may not be so familiar with. It might even be so that the message is utter nonsense, but contains some familiar technical terms, so that the victim thinks that the speaker is far more knowledgeable in the topic. This may, for example, grant the speaker an authority status in the eyes of the victim, thus making him or her more susceptible to requests.

IV. Attack methods

There are several methods a social engineer can employ to achieve the attack objectives and they are used in different parts of the attack cycle. This section describes a number of them, which have been successfully employed in real life scenarios.

A. Information gathering

As the old saying goes, knowledge is power, thus the first and foremost method a skilled social engineer will employ is background checking. When the potential attacker is able to gain extensive information about the target, it is much easier to contact people and fabricate lies. The more detailed information is known, the more sophisticated and convincing lies can be made. Nowadays it is quite easy to get information from the company web site and other Internet resources. Especially small and medium enterprises tend to publish names and contact information of their employees. Larger organizations, on the other hand, may participate in events, like conferences, that leave traces to the Internet. A patient attacker can also monitor the

behaviour of the personnel and even use dedicated surveillance equipment, which is readily available. A bold social engineer can just walk into the premises of the company and try to spot interesting information.

A classical method for acquiring information among the social engineers is dumpster diving. Sometimes companies can be careless when getting rid of papers and manuals. When adequate disposal procedures are not employed, a dumpster can provide a wealth of information, even passwords. Especially at times when departments are moving, the amount of disposable paper can be quite extensive. Even if the company is taking advantage of separate classified material trash bins, it might be that these bins quickly are filled up and the people end up using ordinary trash bins for the rest of the material. It might be also that conventional trash bins are more usable, i.e. do not contain a lock nor a very small hole for inserting wealth of papers. Companies also ought to pay attention to the disposal of old equipment. On several occasions there have been cases, where sensitive information has been retrieved from the hard disks of some recycled computers. It is also worth considering the electronic equivalent of the dumpsters, i.e. the operating system may offer the possibility of a trash folder, which contains the files intended for deletion. This is kind of a usability feature that is intended to help the users to undo their mistakes when deleting files. Equivalently, the format command may be accompanied with a message "all data will be lost" that can give false impressions regarding the recoverability of the data. Another place that can provide interesting information is the swap file, which is used to store information that cannot be kept in memory, i.e. it is an extension of the processing storage. It might be that even if the contents of the data files are encrypted, the same information can be retrieved from the swap file. Of course, if one can steal a powered on device, the information is readily available. The mere physical access to the device can also be enough, depending on the level of protection used in the device. Only now the companies are starting to realise that the mobile terminals, like modern phones, are capable of holding quite a lot of information and even email exchange, thus providing interesting targets for an information gatherer.

Information can also be gathered through a method known as shoulder surfing, which simply means that the attacker tries to see what a person is typing. Typically this is used for retrieving passwords or PIN codes. This naturally requires that the attacker has a physical access to the place where the information is typed. In company setting this, thus, means that there first has been a breach of physical security, although people can also work in places like trains and planes, when it is relatively easy to see what a person is writing without rousing much suspicion. In public places this is much easier to accomplish. For example, it is relatively easy to spy PIN codes, when people are accessing ATMs. There have been cases where an attacker has first spied the PIN and then stolen the bank card, thus enabling him or her to make unauthorised withdrawals from the bank account. It might be that a sophisticated attacker could also take advantage of technology to succeed in retrieving typed information. This could be, for example, the audio recording of the typing [10]. Of course, the physical presence can also be used for eavesdropping, if the persons are not wary about what they discuss. It is likely that within the company the personnel are less careful about what they say, because they expect that no unauthorised people are present. Additionally, if one is able to make people brag, then people may not be as careful about what they reveal. It is also interesting how much personal information people are giving away during cell phone conversations, even in places like busses. Carefully selected bus route and time of day can reveal very specific information regarding certain companies.

Surveys can also be an effective way of gathering information. Even though the questions can be innocuous at a glance, together they could reveal interesting pieces of information about the workings of a company or details of personnel that could be used for building relationships. Naturally surveys can also directly ask for sensitive information, such as passwords, and the success rate can be astonishingly high (like close to 60% in [11]). The answer rate can be further increased by promising a chance to win a prize of a sort.

B. Smooth talking

Persuasion is one of the basic social engineering methods, which relies to the psychological triggers described earlier. It requires a convincing and smooth talking individual, but is very simple and can be very effective. When the target is lulled into trustful state, the information or a favour can be got just by asking. Like Kevin Mitnick has stated: "You try to make an emotional connection with the person on the other side to create a sense of trust. That is the whole idea: to create a sense of trust and then exploiting it." [12]. The social engineer needs to be good in reading people in order to make the right suggestions at the right time. It is easier to get more valuable information, if some information of smaller value has been disclosed earlier, because the people are likely to have more positive attitude towards people they have had some earlier relationship. This can also be efficiently exploited in the case of two different co-workers, who know each others: you do a small favour for the first one, who, if referred to, is likely to vouch for your trustworthiness to the second one. In other words, trust estimation based on transitivity fails.

Persuasion is more effective at times when people have decreased sense of judgement. As previously stated, the high emotional state of the victim is beneficial for the social engineer, but tired people are also more susceptible to the suggestions made to them. Picking a time like the end of a work day or after lunch is likely to produce better results from the point of a view of the attacker. Another good time is summer as there can be summer workers, who are less knowledgeable about the company policies and more easily follow the instructions given by "older workers".

Persuasion can be enhanced with bribery, i.e. giving something of value to the user in exchange of information. For example, BBC reported of a survey, in which over 70% of the people were willing to reveal their password in exchange of a chocolate bar [13]. Of course, it can be

questioned whether all of the given passwords were real, but for an attacker it may be enough to get hold of one correct one.

C. Impersonation

Social engineering usually requires some form of impersonation in order to win the trust of the target. Quite often used tactic is to impersonate an IT support person, who is "checking the network" and asks for a password or asks to install a piece of software. Other support staff, like janitors and repairmen, also does not catch the eye of the unwary and can be quite successful in finding interesting pieces of information. Someone could also pose as a manager and rely on the peoples' trust on authorities. Posing as a fellow colleague in trouble might earn the attacker sympathy enough to gain access to the desired information. Impersonation often is preceded with an identity theft, which can be simple as acquiring an official looking company badge (fake one will usually do), a company t-shirt, or carefully gathered collection of personal information of a person. Identity theft in itself is an increasing cause for worry that has direct economical consequences as many cases have shown (see, for example, [14], [15], and [16]). Nowadays companies are eagerly outsourcing their non core functions, so it is not so surprising to see strange faces at the work facilities.

D. Breaching physical security

Usually a company has some sort of physical security measures, locked doors at least, in place. Even though even more sophisticated techniques might be in place, a social engineer could simply use tailgating, sometimes also called piggybacking, to access the facilities, i.e. go through the locked door at the same time as other persons. Additionally, smoking is gradually getting forbidden in the company premises, which is a good thing in itself, but the result is that a social engineer might attach himself to the group of people smoking outside and tailgate them back inside. Impersonation also makes it easier to breach the physical security. By making a physical appearance the social engineer takes a bigger risk, though.

E. Reversing the roles

Reverse social engineering is a method in which the attacker entices the victim to be the party that initiates the contact. This kind of setting is likely to make the victim less suspicious of an attack. Typically this means that the victim has a problem of some sort and calls for help. The following kind of steps can be observed [17]. First, in order to accomplish the attack the attacker has to first sabotage the system that the victim is using. This could be as simple as injecting some extra scripts through cross site scripting (XSS) vulnerabilities. Also, the attacker needs to do some marketing, which could be a business card, a supposed IT support phone number, or an error message with contact information, in order to lure the victim to contact him. In the final phase the attacker assist the victim in solving the problem. So, a level of trust is established and the victim is happy to help the supposed support person with any questions he might have in order to get the problem solved. The attack can be executed without actually doing any initial sabotage: Just put a flyer on the bulletin board announcing a new helpdesk number [18].

F. Technological means to an end

Even though social engineering can rely solely on psychological triggers and social interaction, it can also take advantage of the technological means. Technological exploits can further ease the job of the social engineer as one level of security is breached and people may not expect an attack, if they have placed their trust on the integrity of technology. Even more important is the ability to communicate with people in various different ways, though. Especially email has been a very successful instrument in the hands of the culprits, even though the phone is the most classical tool for social engineering. A well known example of email based scams are the so called Nigerian letters, which promise a large amount of cash if the receiver is willing to arrange an offshore bank account for money transfer [19]. Usually the victim has to pay some small fee or tax in order to secure the money transfer, but they can also try to lure the victim to come to a country of their choosing with a substantial amount of money. In essence, the scam feeds on the greediness of the people. Note that this type of scam existed also before the era of email, but now the potential victims can be reached much easier and the target group is vastly larger as gathering email addresses is easy. Just like with spam, automation outweighs the problem of minimal response rate.

Another way of using email to deceive people is to use them with fraudulent web sites, i.e. use a technique called phishing, to extract sensitive information, like social security numbers, credit card numbers, and web bank credentials. The email can be said to be arriving from a bank and asks the receiver to access the given site with the user credentials. The email and the web site can look quite legitimate and fool the unwary customer. With HTML based email messages the underlying links and other suspicious content can be easily obfuscated. It is not always enough, if the bank employs one time passwords and extra confirmation passwords for transactions as the attacks against Nordea, a Scandinavian bank, have shown [20]. Usually phishing like this is successful, because mutual authentication does not exist or the customers are not knowledgeable enough to expect authentication. Even though usually banks employ SSL on their web sites, they can fall for bad design choices that can compromise the safety of the customer credentials by not providing the first login page the protection of SSL [21]. In other words, the bank can claim that the credentials are transferred in a secure fashion after the completion of the login procedure, but there is no guarantee what and where the login page actually is, i.e. it could be a phishing site. Even though the aforementioned procedure is likely to reduce the server load due the missing SSL procedures on the first page, it introduces a security vulnerability in a very sensitive context and contradicts with the previous user training ("look for the lock icon"). It should be noted, though, that SSL is not the ultimate solution as it still can present some challenges from the usability point of view. It is very common that the users do not pay much heed to the warning

messages, which imply that the authenticity of the server might be questionable.

Site fraudulence can also be used against the attacker. An attacker is tricked into attacking a fake system instead of the more valuable production system. To the attacker the system looks like the real system, though. This technique, called honeypot, may cause the attacker to spend his effort in breaking the more carefully audited system. This way it is possible to learn from cracker tactics and see what sort of software they have at their disposal, possibly revealing some previously unknown tools and vulnerabilities. The challenge here naturally is how to detect the attack attempt and guide the attacker to the other system. The system can exists on its own, though, with a sole purpose of attracting attackers.

Email and web sites can also be used to send malware to the victim. This can result in the total comprise of the user machine, which can then be used as a zombie to deliver spam or keylogged for sensitive information. Basic approach would be to send the malware by email and entice the receiver to click on the attachment. After all, the sender of the email can be forged to look pretty much anybody. The enticement to open the attachment is up to the imagination of the sender, but typical is a promise of pictures of questionable nature, or one could be chatting with an employer on phone and include in the context of the discussion a sending of an email [22]. A security conscious email gateway will probably filter this kind of content, so the other option is to do the advertising in the email and get the receiver to visit a web site mentioned in the text. A rather imaginative example of this was reported in [23]: A supposed bank customer reported to the security officer of the bank a fake phishing attempt, and when the officer investigated the forwarded message and clicked the link to the alleged phishing site, a compromising malware was downloaded to his workstation. Another tactic of injecting malware is to misuse the autorun option available in some operating systems. This requires that the user is fooled into running the media containing the malware. One way is to use USB sticks for this, because many users are not actually aware that the autorun functionality can apply to them as well. [24] reports of an experiment, in which USB sticks with an autorun programme were distributed to locations near the target office. Many people picked them up and were curious enough to plug them into their computers, which were subsequently compromised. The same kind of "curiosity killed the cat" approach could be employed in simple forum discussions: Pose as a legitimate writer with some reasonable input to the discussion, include a URL in the signature of the writer and wait for the curious forum readers to click the link. As the previous examples show, a social engineer could use quite creative tactics in extracting information with the help of technology and fooling people into doing actions the attacker wants. Of course this kind of approach can leave traces of the attack compared to the purely social means and the attack can be noticed, but at that point it can already be too late anyway. The attacker has better chances of remaining totally anonymous, though.

G. Passing the passwords

An interesting authentication feature that some sites offer is the extra security question. These usually are features that are used to enhance the usability of the service in the case the user has forgotten his or her password. After answering the question the user is granted access or the password is mailed to the address of the user if known. As [25] has noted this can be very bad practise, because the answer to the question can be much easier to guess than the password or the answer can be found out by doing some research ("what is the name of your pet"). The user might be tempted to reuse the question in other sites as well even if they were security conscious enough or told to use different passwords, which can result in the disclosure of it, especially if the other site is controlled by the attacker. The same threat is also evident, if a person uses the same login and password on multiple sites.

Mailing of forgotten passwords can also provide avenues of attacks. In the extreme case the attacker could get access to domain's name registry account and change the routing of email, i.e. reroute all messages via the attacker and snoop interesting information like passwords [26]. Some might think that if this is done with help of SMS (Short Message Service) available in GSM, it is especially secure. However, a clever social engineer posing as an operator technician could request password submission, call the victim, claim some inconsistency in the network, and ask what information was transmitted to the victim. Some claim that this was part of the procedure, along with some technical exploits, that was used to hack Paris Hilton's mobile phone account, but the information is not conclusive. It is would seem more likely, though, that the target of social engineering included operator employees. This does not mean, however, that the attack described would not work against an unwary customer. It just shows how the same context, like a message from the service and contact from the service technician using other channel within a relatively short time period, can be used to make the mental shortcut easier. [26] shows additional examples of exploiting context awareness.

H. Attack chains

The above described methods can be viewed from the perspective of different social engineering categories and the attack chains they form. Table I gives an illustrative example of some of the described methods in terms of the categories and the possible attack chains. Note that there is not just one truth in here: Methods can be varied imaginatively to accomplish varying kinds of consequences.

Table I
Examples of methods and relevant attack chains

Method	**Attack chain**
Shoulder surfing	Extracting
Persuasion	Influencing → Extracting
Tailgating	Bypassing → Extracting
Impersonation	Influencing → Extracting
Nigerian letter (email)	Influencing → Tricking
Phishing email with web site impersonation	Influencing → Tricking → Extracting
Reverse social engineering	Tricking → Influencing → Extracting

V. Outlook for the future

As we walk toward the future of ambient networks we might ask ourselves whether the technological development and ubiquitous computing will help to mitigate the threat of social engineering. Sadly, this is not so. The advent of new means of communication and interaction enables the attacker to put himself farther away from the intended victims. Even though the human factor may decrease due automation and various sensors can make statistical assumptions based on face features or strain of voice, it does not mean that the abuse would become impossible. In fact, some attacks involving trickery may become easier, when the environment is unattended by human observers. As Kevin Mitnick has stated, "The security landscape, the only thing that's changed in regards to vulnerability are technical issues, but with social engineering, it's all remained the same." [27].

A. Virtual presence

Research, an important factor in social engineering, is likely to become easier as more and more information is available through data networks and search engines. This is something that Google CEO, for example, has learnt [28]. People leave more traces of themselves in the Internet and even though they might think they have erased old records, the data might still be lying around in search engine caches or archive services [29]. In a way, this information digging could be called the electronic equivalent of the dumpster diving (e-dumpster diving if you like).

People also engage in different kinds of social networking and chat services, which can prove to be valuable sources of information. The social engineer can simply be a passive observer of discussions or actively engage with discussion with a forged identity, thus being able to extract information of his choosing. In some cases it is possible to coerce the non-technical people to do things they would not normally do by threatening them with viruses, for example [30]. The people themselves can release personal information by posting it on community web sites and keeping a blog. This can also reveal linking between persons, i.e. it is possible to build social relationships maps [29]. Such information can be used for establishing a context of trust or help in identity theft. Note that virtual communities can present opportunities for direct exploits with monetary value. This affects, for instance, some online games with their own side-economies [31], even though the jurisdictional status of this can be bit of a grey area currently. Hence, the designers of virtual communities have more responsibility in taking into consideration the possibilities of social engineering and education of their users, as well.

B. Tokens and devices

In this regard it is worthwhile to consider what sort of identity tokens are used and in what way in the future systems. For example, e-passports can hold sensitive information about their holder that would be quite useful in accomplishing identity theft. Some of the employed security measures can be deemed inadequate to protect the data [32]. Additionally, if such passports are used in other circumstances as an identification tool, such as in e-commerce, the function creep undermines the data protection features even further [32].

If the people have personal tokens, which can be plugged into various reading devices in order to get the same personalised environment regardless of the device, the design of the system needs to take into account the fact that the reader might be compromised and tries to steal user credentials or information. Note that even though there might be smart cards or other tamper resistant token solutions, they still often use passwords or PINs to be typed to allow the security operation on the token. Without a dedicated input device this information can be captured. Additionally, the tokens can be fed with false information to be used in the security calculations, like signing operations.

Ubiquitousness and terminal independency also provide new opportunities for misuse. A people willing to help might be willing to lend his or her terminal for someone for a second or two and end up paying for some extra service or disclosing some sensitive information. This has actually already happened with mobile phones, when someone has borrowed the terminal for a quick call, arranged a conference call with two other parties, and then disconnected the original phone from the conference. The abusers could also lend their terminals in hopes of capturing interesting information or credentials. The possibility to attach the personal terminal to external input and output devices for better usability at some random location also provides a weak point, and the above discussion regarding the tokens applies here as well. If the user has the choice of using unauthorised device versus having no connectivity at all, the most users are likely to take the first option [18]. More generally, if you manage to cause denial of service condition against a secure service, the users might be tempted to use the available insecure equivalent instead.

C. Dynamic data handling

An important fact in any service is the authenticity of the presented information. An interesting factor regarding this is the use of semantic web technologies that are envisaged to help machines in interpreting the information they read, i.e. give semantic meaning to the strings of characters, thus helping, e.g., in searching information. The problem with the authenticity is the same as nowadays: People can make various claims about the semantic meaning of their data, but there may not be any guarantees that this truly is so or that nothing harmful is injected. This could be used, for example, to lure unsuspecting victims to access automated content feeds or web sites that provide malware instead of genuine information. Even today some web pages contain additional non-related keywords to confuse search engines and the people using those engines.

Additionally, if the cognitive radio concepts become widespread, this could give new ways to abuse the devices, when the user or the device is tricked into installing software that could seriously affect the functionality of the device. The similar issues are present with any other reconfigurable device, so the designers should carefully think whether it is feasible to allow total user control when deciding what sort of updates to install, even though to

some this may decrease the flexibility. Even though there are security models, which control the privileges of an application in software platforms of the terminals, the malware could get additional rights by tricking the user. For example, a programme might promise, in addition to some useful functionality, free SMSs for the user, thus requesting privileges to send SMSs. After the user is fooled into doing this, the programme can easily send a number of SMSs to a service number, thus defeating the security model and having direct financial consequences.

It is also important to remember the relationship between authentication and authorisation. Even though some material might be authentic, it does not mean that who ever is providing the material is authorised to provide it. For example, if in the not so distant future people exchange automatically their electronic business cards upon meeting each others, it should not be possible to forward the card onwards and pose as someone else. Currently, this is quite easy to accomplish with the traditional business cards. So, the systems should take care in ensuring that the appropriate bindings with the identity and authorisation are in place. Additional concern comes from the federation concepts of identity management, which allow different identities to be linked together and used to accomplish single sign on to multiple different services. In this setting, the attacker needs to acquire just one set of credentials to enable access to many different places.

D. Context awareness

As mentioned previously, the use of SSL may not be enough to ensure the authenticity of the web site due the usability issues. The user themselves may therefore have hard time estimating what is authentic and what is not. This is especially troublesome, if all the other context information would give indication that the other party is a valid transaction partner [26]. With the future networks there will be plenty of context information available regarding the user context [33] as well as the network context [34]. If the access to this information is not carefully controlled, a more convincing kind of social engineering attacks can be launched. For example, if the location of the user can be discovered, then one might craft attacks, which take advantage of this information in convincing the user that the received information is somehow genuine, like impersonation of a nearby shop special offer (if such functionality was enabled). Alternatively, this kind of information digging could reveal other interesting information like that the person is accessing company internal network through a VPN (Virtual Private Network) at home, which probably has weaker physical security measures. Even though context awareness could be employed to catch things like "this user's behaviour at this hour is not in line with the normal behaviour profile of this particular user", this does not yet guarantee that an attack is in progress, because there can be exceptions to the user normal behaviour much like when trying to analyse "normal" traffic on the company network and detect intrusions. It can be used to signal the need for extra auditing, though.

E. New networking paradigms

An extra complication is the envisaged future network setting, where practically any device can be a network and anyone can act as an operator. False context information could be advertised in order to reroute traffic and extract interesting information. The same thing can happen analogously on service level as well, if the service oriented architecture and service composition ideas are taken to their extremes. Evaluating trustworthiness of such parties can be difficult, if one wishes to promote the ideas of ubiquitousness and flexible usability. If only untrusted communication paths are available, is that incentive enough for people to stop communicating? As often is, the security and usability requirements can be contradictory.

The same problems of trust relationships are evident in using ad hoc paradigm in forming future networks. In some of these the trust may be based on reputation factor, i.e. if you have proved being a trustworthy partner in the past communication, your reputation score will grow. In this setting a malicious party just patiently conducts honest behaviour and waits for the chance to make that one "big coup" and then disappears. Similarly, a group of members, some of which could be zombies controlled by the attacker, could be colluding to affect the quorum decisions, although inconsistent behaviour could be detected.

F. Usability

As already stated usability and security often are contradictory. The challenge is to implement the security methods in such a way that the user does not view them as nuisance and is not tempted to lower them, as this can lead not just to social engineering attacks but to various other attacks as well. In other words, security design should be non-obtrusive and possibly such that user does not even see it. For example, very stringent password chance policies are something that users clearly feel and see and they can easily lead to situations where the passwords are written on notes, although it should be obvious by now that the password, even though often usable and easy to implement, should not be the sole authentication mechanism. UI (user interface) design principles should take better into account the security requirements, so that violating the integrity of information should not be possible. An example of such UI issue is the case where a user can be fooled into believing that a valid S/MIME signature on an email corresponds to a different individual, i.e. allows impersonation, if security and presentation do not support each others [35]. This just proves that security needs holistic design and there should be cooperation with the usability and UI people as well [36]. The interaction should go both ways.

VI. COUNTERMEASURES

The very nature of social engineering suggests that the most effective way of preventing it from happening is through the user training. This should be accompanied with relevant policies that dictate the user actions in potential abuse circumstances. Naturally it is expected that the administrative and physical security is taken care of and the company has meaningful security and data management policies [37]. Examples of such policies can be found, for

instance, from [38]. It must be emphasised, though, that just making policies is not enough. The company has to make sure that the employees understand what the policies actually mean and what can be the consequences, if the policies are not followed or are followed in a lax manner. One additional aspect is that the company ought to also consider negative policies. In other words, they should state that certain kind of activity, like IT-support asking passwords via phone, will never take place. The training should be used to raise the awareness of all the personnel about the possible social engineering methods, but it should be especially targeted to people, who work in positions where people are expected to be friendly and helpful, like helpdesks and receptionists. It is the responsibility of all, though, to make sure that no unauthorised information is leaked nor is any unauthorised physical access allowed. This also includes understanding the importance of identity verification. There is clearly need for this, as a survey shows that 48% estimate the lack of employee awareness and training as a major security challenge to their business [39]. Other organizations, like operators and financial institutes, should also remember their responsibility with regard to customer education.

The user training can be made more effective through audits, which can be conducted by outsider auditors. This could be, for example, simulated attacks that could reveal the weak points and also teach people who fall for them. Personal experience is likely to be more effective learning method than sitting at lectures or reading policy documents. Online auditing itself may not reveal the real culprit as some form of impersonation probably is taking place, but it mitigates the possibility of malicious insiders through deterrence. Of course there might the problem of proving whether the insider was malicious or just a victim of social engineering. But as Bruce Schneier has stated, in the end the organization is at the mercy of its people [18]. This is backed by estimates, which state that around 60-70% of information thefts are conducted by insiders. However, sometimes it is not even known that some information has leaked.

The companies should also pay attention to what sort of information they are revealing about themselves and their employees on public channels like Internet, so the personal information should be kept to minimum and it is better to use role names than the actual names of the persons. It is also important to take care of the proper disposal of the material that is no longer needed. This applies to paper, electronic information, and hardware as well. The advances in feature matching and similar algorithms may require a more complete destruction of paper documents than mere shredding [40]. The hardware, especially hard disks and such, should be destroyed rather than rely on erasing the contents, which still can leave traces of information. There are companies that offer this kind of services, but one needs to be certain that they employ due procedures, otherwise they could be real gold mines for information diggers.

As the previous discussion shows the threat of social engineering cannot be solved with technological means alone, but the effects can be mitigated and the technology assisted attacks, such as those employing malware, can be made harder to accomplish. Extra auditing or the mere possibility of it in itself can function as a deterrent, for example. The passwords are the weak point of security as people can easily give them away or write them down on papers (even though some experts say that this is not always a bad idea [41]). The future systems need to rely on stronger forms of authentication, so that it is not possible to give ones credentials over the phone, for instance. There has to be also means to authenticate the information, so that phishing and similar information collecting techniques are noticed and prevented, even though software can even now make heuristic conclusions regarding the content and issue warnings, although this can easily lead to false warnings. The user cannot be trusted to be able to make the correct decision, if the user interface makes it easy to bypass the warnings. Additionally, the importance of authorisation needs to be taken into consideration as well, i.e. one needs to have authorisation for one's actions as well, so that unauthorised delegation of privileges cannot take place. Similarly, one needs to review the need for privileges for different kind of users, i.e. give only the required privileges. It is good to remember, though, that the software, even the security software, can still have undiscovered (or unpatched) security holes in them, which defeat the intended purpose.

From the design point of view the systems that rely on security by obscurity are clearly very vulnerable to social engineering attacks. As the skilled social engineer has various ways of affecting people and getting them reveal secret information the secrecy of such systems is easily compromised. Thus, the systems should not base their security assumptions solely on the secrecy of some functionality or data. Security needs several layers, i.e. defence in depth, that can mitigate the effectiveness of an attack, if one of the security measure fails, like when people give out too much information or allow unauthorised people to roam the premises. In other words, one needs to have breakpoints, either policy or technology based, in the phases of the attack cycle depicted in Figure 1. Additionally, the security design of any system should not be a separate design activity, but should take an integrated approach right from the start of the whole design process [36]. This should also ensure that security is an embedded feature, not something you turn off in the name of usability when shipping the final products.

VII. Conclusion

In this paper we have investigated the nature of social engineering and methods that can be employed to launch a successful attack against an unwary victim. As we have shown this is not solely a technological issue and is not likely to be rectified even by the new emerging technologies for the future networks as the social engineering by nature circumvents the technical barriers using psychological means. In fact, the technology can lull people into false sense of security, which is a favourable condition for a skilled social engineering. Also, the technology is bringing changes to the way people build their social structures and communicate, hence providing new opportunities to affect people. Therefore, the most effective way to combat social

engineering is by user training. Otherwise, the carefully crafted security policies can seem too distant for the everyday worker, who is mostly interested in getting his or her job done, but can still feel sympathy for the fellow worker in distress. A holistic approach in design processes can help to alleviate the threats, which may result from decisions based on the usability factors alone. In other words, security should not be treated as a separate function of the system but as the sum of all the parts.

ACKNOWLEDGMENT

The author wishes to thank Vesa Huotari and Jukka Koskinen for many interesting discussions and valuable suggestions regarding social engineering and its applicability in the general field of security. Additionally, the author wishes to thank professor Sari Kujala for giving suggestions on the psychological aspects of affecting people.

REFERENCES

[1] Harl. People Hacking: The Psychology of Social Engineering. Talk at Access All Areas III, 1997. Available at http://bak.spc.org/dms/archive/aaatalk.html (accessed 08/2006)

[2] Weirich D., Sasse M. A. Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. Proceedings of the 2001 workshop on New security paradigms, 2001.

[3] Gartner. There Are No Secrets: Social Engineering and Privacy. Gartner's Information Security Strategies Research Note TU-14-5662, 2001. Available at http://www.gartner.com/gc/webletter/security/issue1/index.html (accessed 08/2006)

[4] Cialdini R. B. Influence: The Psychology of Persuation. William Morrow and Company, 1993.

[5] Gragg D. A Multi-Level Defense Against Social Engineering. SANS Institute White Paper, 2002. Available at http://www.sans.org/rr/papers/51/920.pdf (accessed 08/2006)

[6] Milgram S. Behavioral Study of Obedience. Journal of Abnormal and Social Psychology 67, 1963.

[7] Rusch J. The Social Engineering of Internet Fraud. Proceedings of the 9th Annual Conference of the Internet Society (INET'99), 1999.

[8] Farber D. Mitnick on Mitnick: "Why I'm going legit" (part two). Kevin Mitnick interview by CNET Networks, 2001. Available at http://www.silicon.com/a55864 (accessed 08/2006)

[9] Cialdini R. The Science of Persuasion. Scientific American Mind, Jan 2004 issue. Available at http://www.sciammind.com/article.cfm?articleID=0007DC8D-AC4A-116D-A7E783414B7F0000 (accessed 08/2006)

[10] Zhuang L., Zhou F., Tygar J.D. Keyboard Acoustic Emanations Revisited. Proceedings of the 12th ACM conference on Computer and communications security, 2005.

[11] Orgill G.L., Romney G.W., Bailey M.G., Orgill P.M. The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems. Proceedings of the 5th conference on Information technology education, 2004.

[12] Lemos R. Mitnick teaches social engineering. ZDNet News article, 2000. Available at http://news.zdnet.com/2100-9595_22-522261.html?legacy=zdnn (accessed 08/2006)

[13] BBC News. Passwords revealed by sweet deal. BBC News online article, 2004. Available at http://news.bbc.co.uk/1/hi/technology/3639679.stm (accessed 08/2006)

[14] Durham-Vichr D. Online Con Artist Steals Identities of World's Richest. NewsFactor Magazine online article, 2001. Available at http://www.newsfactor.com/perl/story/8326.html (accessed 08/2006)

[15] CBS News. An Identity Theft Nightmare. CBS News online article, 2005. Available at http://www.cbsnews.com/stories/2005/02/25/eveningnews/consumer/main676597.shtml (accessed 08/2006)

[16] Mercuri R.T. Security watch: Scoping identity theft. Communications of the ACM, Volume 49, Issue 5, 2006.

[17] Allen M. Social Engineering, A means to violate computer security. SANS Institute White Paper, 2006. Available at http://www.sans.org/rr/papers/index.php?id=529 (accessed 08/2006)

[18] Schneier B. Secret and Lies. Wiley Computer Publishing, 2000.

[19] Interpol. Advanced Fee Fraud: 4-1-9 letters (Nigerian letters). Interpol online article, 2005. Available at http://www.interpol.int/Public/FinancialCrime/FinancialFraud/NigerianLetter.asp (checked 08/2006)

[20] The Register. Phishing attack targets one-time passwords. The Register online news article, 2005. Available at http://www.theregister.co.uk/2005/10/12/outlaw_phishing/ (accessed 08/2006)

[21] Ou G. Many Banks failing to use SSL authentication. George Ou weblog at ZDNet, 2006. Available at http://blogs.zdnet.com/Ou/?p=201 (accessed 08/2006)

[22] Granger S. Social Engineering Fundamentals, Part I: Hacker Tactics. SecurityFocus online article, 2001. Available at http://www.securityfocus.com/infocus/1527 (accessed 08/2006)

[23] Higging K.J. Social Engineering Gets Smarter. InternetWeek online article, 2006. Available at http://internetweek.cmp.com/trends/189500411 (accessed 08/2006)

[24] Stasiukonis S. Social Engineering, the USB Way. Dark Reading online article, 2006. Available at http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1 (accessed 08/2006)

[25] Schneier B. The curse of the secret question. ComputerWorld online article, 20005. Available at http://www.computerworld.com/securitytopics/security/story/0,,99628,00.html (accessed 08/2006)

[26] Jakobsson, M. Modelling and Preventing Phishing Attacks. 9th International Conference on Financial Cryptography and Data Security, 2005.

[27] CNN. A convicted hacker debunks some myths. CNN.com online article, 2005. Available at http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html (accesses 08/2006)

[28] Mills E. Google balances privacy, reach. CNET online article, 2005. Available at http://news.com.com/Google+balances+privacy%2C+reach/2100-1032_3-5787483.html (accessed 08/2006)

[29] Nolan J., Levesque M. Hacking Human: Data-Archaeology and Surveillance in Social Networks. ACM SIGGROUP Bulletin, Volume 25, Issue 2, 2005.

[30] Ewing A. Swedish girls 'forced into Webcam sex'. The Local news article, 2006. Available at http://www.thelocal.se/article.php?ID=4277&date=20060707 (accessed 08/2006)

[31] Yan J., Randell B. A Systematic Classification of Cheating in Online Games. Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games, 2005.

[32] Juels A., Molnar D., Wagner D. Security and Privacy Issues in E-passports. Proceedings of the IEEE SecureComm '05, 2005.

[33] Kernschen R. et al. Multimodal user interfaces for context-aware mobile applications. IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, 2005.

[34] Ocampo R., Cheng L., Lai Z., Galis A. ContextWare Support for Network and Service Composition and Self-adaptation. Second International Workshop on Mobility Aware Technologies and Applications (MATA), 2005.

[35] Udell J. How to forge an S/MIME signature. Jon Udell's weblog at InfoWorld, 2004. Available at http://weblog.infoworld.com/udell/2004/03/23.html#a952 (accessed 08/2006)

[36] Yee K. Aligning Security and Usability. IEEE Security and Privacy, Volume 2, Issue 5, 2004.

[37] Whitman M.E. Enemy at the gate: Threats to Information Security. Communications of the ACM, Volume 46, Issue 8, 2003.

[38] Mitnick K., Simon W. The art of deception. Wiley Publishing, Inc, 2002.

[39] Deloitte. 2005 Global Security Survey. Survey by Deloitte Touche Tohmatsu, 2005.

[40] Justino E., Oliveira L.S., Freitas C. Reconstructing shredded documents through feature matching. Forensic Science International Volume 160, Issues 2-3, 2006.

[41] Schneier B. Write Down Your Password. Bruce Schneier weblog, 2005. Available at http://www.schneier.com/blog/archives/2005/06/write_down_your.html (accessed 08/2006)