Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2011 Proceedings

International Conference on Information Resources Management (CONF-IRM)

6-2011

A Taxonomy for Social Engineering attacks

Koteswara Ivaturi
The University of Auckland, k.ivaturi@auckland.ac.nz

Lech Janczewski
The University of Auckland, lech@auckland.ac.nz

A Taxonomy for Social Engineering attacks

Koteswara Ivaturi, Lech Janczewski
The University of Auckland, New Zealand
k.ivaturi@auckland.ac.nz, lech@auckland.ac.nz

Abstract
As the technology to secure information improves, hackers will employ less technical means to get access to unauthorized data. The use of Social Engineering as a non tech method of hacking has been increasingly used during the past few years. There are different types of social engineering methods reported but what is lacking is a unifying effort to understand these methods in the aggregate. This paper aims to classify these methods through taxonomy so that organizations can gain a better understanding of these attack methods and accordingly be vigilant against them.

Key words
Information security, social engineering attacks, security attack taxonomy

1.0 Introduction
The term 'social engineering' is found to have its roots from the early 20th century political science field where it meant to represent smart methods that solve the social problems. Due to the positive connotations of the word 'engineering' it was appropriated for various social problems of the time. Karl Popper, in his book endorsed the idea as sense of social change based on well established instrumental knowledge (Hansson, 2006). Over the years, especially after the World War II the term gained a more negative flavour and was associated with the stereotyped designs employed by politicians to gain electoral advantage (Duff, 2005). Today the negativity of the term still persists but has gained usage in field of Information Systems Security to describe cases where people are persuaded to furnish critical information that should otherwise remain private (Hansson, 2006). This involves a gamut of things like revealing passwords, providing access to the organization's internal infrastructure etc.; the concept has gained a lot attention over the recent years as a potent attack vector primarily because of the disastrous consequences it can cause.

There has been a considerable increase in the number of research papers that studied this topic which is enough evidence that social engineering has attained academic significance. The literature provides studies on different methods of social engineering attacks through various case studies. Laribee (Laribee, 2006) suggests taxonomy to classify these attacks based on three broad criteria 'close access techniques' 'online social engineering' and intelligence gathering. However, the list of different attack vectors that especially fall under online social engineering is not updated and 'information gathering' as we will have discussed below is not strictly unique to social engineering. In another study David Harley (Harley, 1998) suggests of a taxonomy that lists a few social engineering attacks but we feel it lacks the clarity and comprehensibility required for a good taxonomy. A taxonomy is required when it is necessary to provide a clear and consistent overview of a phenomenon without any obvious overlap (Hansman & Hunt, 2005). A good taxonomy is the one that is mutually exclusive, unambiguous and comprehensive and comprehensible (Lindqvist & Jonsson, 1997) and the aim of this paper is to provide a taxonomy for social engineering attacks in line with these requirements.

The paper starts by introducing the nature and impact of social engineering attacks in Sections 2 & 3. Section 4 lays the groundwork for the taxonomy by describing the anatomy of a social engineering attack, and finally Section 5 discusses the new proposed taxonomy by describing each type of attack vector and the reasons why it falls under a particular category. Section 6 briefly discusses possible countermeasures to mitigate the effect of these attacks and finally we conclude the paper with Section 7 by discussing the potential of this taxonomy and future research directions.

2.0 Nature of social engineering attacks

There are many interpretations and definitions of the term available throughout the literature. Though the exact wording of most of the available definitions varies, the common essence that emanates from each of them is that social engineering involves methods that can control human behaviour to one's objective utility. It is generally accepted that the main chink in the armour of any organization's security architecture is the people of the organization and that is where that attack starts (Barber, 2001; Barrett, 2003; Mitnick & Simon, 2003). A social engineer can control the victim's behaviour usually by evoking strong human emotions. The usual route is that the attacker weaves a plausible story in order to bag the trust of his victim. The story commonly used in such situations is filled with basic human instincts like greed, sympathy or fear (Townsend, 2010). The way in which attackers gain such trust is by persistently persuading the victim to connect to these emotions. Rusch mentions two ways of persuading an individual: (1) through sound analytical reasoning called 'central route to persuasion' or (2) through eliciting emotions called 'peripheral route to persuasion' (Thornburgh, 2004). As a social engineer would usually employ deceptive or manipulative methods the 'central route to persuasion' is not really an option and hence mostly uses the later method. There are people who knowingly reveal personal information in spite of the awareness of the inherent risks involved (Calluzzo & Cante, 2004; Straub & Nance, 1990). This is primarily seen in the cases where the human emotion evoked is that of greed, for example, downloading 'browser-codec' from unknown sources in order to watch a video online, filling in details of personal information in order to receive a free gift etc., There are also many examples that elicit the exploitation of the human fear factor for example, privates (lowest ranking officials) admitting to allowing unauthorized entry of higher ranking professionals (Thornburgh, 2004) due to the fear of reprisals etc.

3.0 Impact of social engineering attacks

Every social engineering attack is usually associated with an end goal. The goal can be anything from critical issues like getting administrative access of the company's network to less critical issues like taking a self-guided tour of the premises etc., and often the attacker has to deploy an attack plan at various nodes of the chain en route to the goal. Every instance of an attacker getting what he or she wants through social engineering means can be considered to be a successful attempt even though the significance of the information obtained might not be immense (Thornburgh, 2004). It is often the cumulative effect of the success of many such attacks that the attacker is ultimately after. Social engineering techniques hence are considered to be a means to an end and not necessarily a one step attack. Over the recent years there has been a lot of focus on building new and improving existing countermeasures for the orthodox technical attacks. Innovations in security technologies such as anti-viruses, intrusion detection systems (IDS), firewalls and patch management systems have all been able to achieve a substantial mitigating effect on the prevalence of technical

attacks (Twitchell, 2006). As a result, more attackers are employing social engineering methods by targeting the human elements and often combine such techniques with their traditional technical methods. A successful social engineering attack can hence simply nullify the effect of the millions of dollars invested in the security architecture of the organization (Manske, 2000).

4.0 Social Engineering Attack Methods

There are many types of Social Engineering attacks and the variety and scope of such attacks are only limited to the imagination and creativity of the attacker (Manske, 2000). Traditionally, social engineering is largely divided into two categories (1) Human-based social engineering and (2) Technology based social engineering (Aiello, 2007; Damle, 2002; Gulati, 2003).

With regards to the field of information systems, the ultimate goal of a social engineer is to gain direct access to a company's information either physically or digitally through access of its information systems (Thornburgh, 2004). Unlike traditional hacking methods, where the attacker needs to be technically equipped to carry out an attack, a social engineer needs to focus on his social skills in order to carry out a successful attack. Bhagyavati mentions that there are usually three major phases of a typical social engineering attack (Bhagyavati, 2007).

1. Preparation phase
2. Attack phase
3. Post attack phase

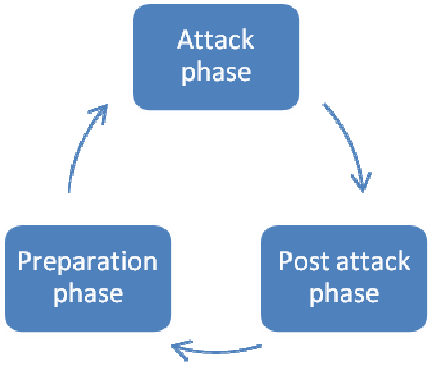

Fig1: The anatomy of a Social Engineering attack.

Kevin Mitnick (Mitnick & Simon, 2003) also describes the 'Social Engineering Cycle' having four distinct stages which are research, developing rapport or trust, exploiting trust and utilizing trust.

The aim of this paper as mentioned before is to provide a taxonomy that gives a good overview of the different types of social engineering attacks and hence we concentrate only on the attack phase as we believe that the other two, preparation and post attack, are generic phases required for any type of attack. There are many sources that quote shoulder surfing, dumpster diving as types social engineering attacks (Granger, 2001; Manske, 2000). Although they help attackers in gathering intelligence in the preparation phase, they do not involve any form social interaction with the victim, which is a basic need to be categorized as

a social engineering attack. Hence we do not classify them as social engineering attack methods as part of our taxonomy.

5.0 Taxonomy for Social Engineering

5.1 Person-Person

The type of attacks that can be categorized as Person-Person social engineering are typically the ones that involve direct or in person interaction of the attacker with the victim where the attacker uses deceptive methods to take advantage of the victim's ignorance or his behavioural weakness and exploits the trust (Kamal & Crews, 2008).

5.1.1 Impersonation

Impersonation is arguably one of the most valued techniques that a social engineer can use as it can be carried out with little preparation and has the advantage of not revealing real identities (Redmon, 2005).

5.1.1.1 Pretexting

One of the popular impersonation techniques is called pretexting, which is the practice of obtaining information under false pretense. It is often more than a simple lie as it involves a lot of research on the victim before carrying out the attack. One of the widely quoted cases of pretexting is the HP scandal case where security experts used this method on the board members of the company to investigate the trail of a data leak of the company's strategy (Baer), 2008). The investigators impersonated as the board members themselves in order to get access to the phone records. This created quite a stir in the media and eventually led way to birth of a new law (Menn, 2010) that prohibits the use of such techniques for obtaining any information under false pretense, including the use of fraudulent statements or impersonation.

5.1.1.2 Reverse Social Engineering

The attacker presents himself as a person in a perceived position of authority which influences the victim to ask more questions instead of the attacker. The orchestration of such an attack usually spans three stages which are sabotage, advertising and assisting (Granger, 2001). For example, the attacker firsts sabotages the network of the organization, then advertises himself as a right person with a solution and with a bit of assistance from the victim fixes the problem. In the last stage he gets what he really needs by requesting the victim to log into the network under the aforementioned pretext. Such attacks are highly effective as it leaves the victim with a sense of satisfaction as the network problem goes away and hence leaves no reason for suspicion. This type of an attack is also termed as Quid pro quo where the attacker provides some incentive that persuades the victim to divulge information that otherwise would not be shared.

5.1.1.3 Tailgating

Tailgating simply means following a person with authorized entry into a secure area, basically riding on coattails (Long, 2008). The act may be considered to be legal or illegal depending on the circumstance but in general this term has a negative connotation and is used to describe an illegal act.

The common denominator for all the above mentioned attacks is that the attacker builds a character and then fabricates a misleading story around this character which is aimed at evoking the victim's basic human emotions of greed, sympathy or fear (Workman, 2008). The attacker must be able to simply anticipate and prepare for questions that might be asked

by the victim. In order to facilitate this and to further project credibility to the story, the attacker usually uses two tools (1) using the company lingo in the story and (2) portrays knowledge personnel and policy (Thompson, 2006). A typical story involves a character and a context which the attacker uses as a vector. The character can either be a fake one originating from a figment of the attacker's imagination or a real character that the attacker wishes to masquerade as. These types of attacks are increasingly becoming easier to orchestrate with the help of public databases such as LinkedIn & XING, which give the attacker organizational structure along with names of individuals and the positions they occupy (Huber, 2009; Roßling & Muller, 2009). To gain a broader understanding of such person-person attacks we categorize them into two broad categories (1) Impersonating by building a fake persona & (2) Impersonating a real persona. These two categories should include all case scenarios discussed above like pretexting, reverse social engineering or quid pro quo. One thing to observe here is that the conceptual aspects of these methods are not necessarily used as attack vectors only for person-person scenarios but could be also be used via other media as well as discussed below.

5.2 Person-Person via media

All attack vectors which do not involve the physical presence of the attacker are categorized as the Person-Person via media attacks. The ubiquitous use of computers and mobile phones has helped the social engineering attackers gain more viable and scalable options for carrying out their attacks. The use of media as an attack vector often has more advantages than the in person attacks as it simultaneously gives the attacker the power of anonymity and scalability. Text, voice and video are the three types of media that are taken into consideration for the taxonomy.

5.2.1 Person-Person via Text

This category includes all types of attacks that use text as a medium for communication. Examples are activities that are involved with the Internet like email, browsing, chatting and social networking to short messaging services (SMS) or even traditional offline media like mail and news papers. The various types of attacks under this category are discussed below.

5.2.1.1 Phishing

Phishing is a fraudulent process of acquiring sensitive and personal information by masquerading as a trustworthy entity and is mostly carried out over email. Over the years this problem has not only grown in size but also in complexity (Lee, Choi, & Kim, 2007). Typically, the attacker generates hundreds of random email addresses and sends a blanket email to all of them hoping that at least a small percentage of the potential victims will take the 'bait'. The nature of the 'bait' involves a realistic looking message with a fraudulent call-to-action and a website that the attacker uses to collect the victim's information. This is a type of attack where the attacker is deceptively influencing the victim and persuading him to divulge sensitive information.

5.2.1.2 SMSishing

This form of attack though not prevalent yet, can be an effective tool for a social engineer especially due to the explosion in the use of cellular phones. The anatomy of this type of an attack is very similar in nature to the concept of phishing but is different in that the fraudulent message, instead of being sent as an email, is sent as a SMS to the victim's cellular device (Binay, 2009).

5.2.1.3 Cross Site Request Forgery (CSRF)

This is a type of attack where the attacker tricks the victim's browser into performing undesired actions on behalf of the victim (OWASP). The vulnerability exploited here is the browser's functionality of not being able to distinguish between user generated requests and malicious requests especially when the victim is already logged into a website. But the instantiation of such attacks is by sending an email to the victim that looks legitimate but carries a malicious code in the form of any common HTML element like an image tag, script tag etc., As soon the victim opens the email, the browser executes the HTML elements without any form of verification as it thinks the user is still logged in. This form of an attack is also called as Session Riding.

5.2.1.4 Malware

This attack is probably the most effective and hence most successful of all types of social engineering attacks due to its pervasive and persistent nature. This attack vector is a combination of both psychological and technical ploys and usually feeds on unsuspecting average users, a number that runs in thousands (Abraham & Chengalur-Smith, 2010). As the technology that thwarts malware has evolved so has the complexity of the malware attacks primarily due to the reason that the psychological tactics of the attackers also evolved. Another reason this attack is so successful is because there are so many forms and platforms that the attacker can use to unleash these attacks. Today the word personal computers has taken a whole new meaning with different form factors available like smart phones and tabloids, all of them having the ability to connect to the web and hence all them being viable avenues for attack.

Whatever device and platform used the reason the problem of malware has been so persistent is because the attacker is using his social skills in trying to persuade the victim in order to perform an action that benefits him. The tactics employed as discussed above can be anything that the victim could connect to like curiosity, fear or greed. The following are examples of such attacks and the tactics involved that make them successful.

Email:

This is the most prevalent form to launch a malware attack primarily due to the ubiquity of the application, it is reported that by 2013 approximately 1.9 billion people will be using emails as their primary form of communication (Reardon, 2009). The tactics used here to persuade the user to perform an action mentioned in the email could be by eliciting the victim's curiosity by using catchy and intriguing lines that make the victim open the email. The 'Lovebug' worm in 2000 is a great example of this, where the attacker's email had the subject line 'ILOVEYOU' and an attachment that looked like a text file which made the unsuspecting and curious open the attachment only to be infected with a script that sent a copy of itself and everyone in the address book on behalf of the victim.

Popups:

Popups are random alerts messages that open in a new window and are usually used as means for online advertising. The attackers use this form of attack to present messages that elicit the victim's fear or greed quotient that will eventually persuade them to perform the intended call for action. The recent examples include the emergence of 'scareware' where popups appear that contain a fake message stating that victim's computer has been detected with a virus and that the user has to download a particular anti-virus to remove it (FBI, 2010). The typical user panics and downloads the software with the intent to fix his computer but in doing so inadvertently infects his computer with malware carried in the software.

Search Engine poisoning:
Search engine poisoning (SEP) occurs when the attacker lures people to his website by employing certain 'black hat' or unethical techniques. When the unsuspecting user clicks on the search engine result, because he deems it to be relevant to his query, he is redirected to another website that tries to persuade the user to download a certain malware.

A typical attack of this form usually kick-starts when there is a significant global event. Tools like Google trends are used to monitor such phenomena and whenever a particular keyword is found to be trending, the attackers build fake websites seeded with malware and expose it to the internet (Townsend, 2010). The social engineering angle for this form of an attack is in the fact that the attacker is exploiting the trust that users have in the search results provided by the search engines to launch the malware attack. SEP is becoming increasingly popular as it doesn't even need to elicit the human emotions required for a typical social engineering attack as it is already created through the occurrence of the global events.

Social networking:
Attack methods using social networking software is also on the rise purely due to the ubiquity of such platforms. Recently Facebook reported to have acquired its 500 millionth user (approximately 8.5% of the world's population) and there many such applications that are growing in popularity providing another juicy avenue for the attackers to exploit. Twitter, a popular social networking site has been a subject of numerous social engineering attacks. A typical attack is where the attacker creates a fake profile that has a message and a link which is a shortened form of a full URL, using services like tinyurl.com. The victims are persuaded to click on the link which downloads the malware without permission (Naraine, 2008).
Again, the Social engineering angle here is in the fact that the victim's trust is exploited when he is asked to click on a disguised and shortened form of a malicious URL containing malware from a trusted source in his social network.

5.2.2 Person-Person via Voice
All types of attacks which do not have the attacker's physical presence but use voice as a medium for communication could be slotted into this category. These include the use of both the cellular network where the attacker carries out the attack over cell phones and also the Internet where the attacker can choose to carry his attack leveraging IP-based voice messaging technologies like VOIP. The various types of attacks under this category are discussed below.

5.2.2.1 Vishing
Vishing is the practice of using the cellular network or VOIP into providing personal, financial and other sensitive information for personal benefit (Ollmann, 2007). The attack is analogous to phishing and SMSishing as discussed before but is different in that it is carried out over the phone using voice as a medium. A typical vishing attack is when a victim gets a phone call with a pre-recorded message asking the victim to call back to verify credibility of bank details. When the victim calls the bank an IVR system is set up giving a number of options for the victim to choose. Regardless of what option the victim chooses, they will hear a message that asks them to authenticate themselves by dialling in their account and pin number. Once the information is provided the call is either terminated or redirected to the real customer service leaving the victim in a state of panic.

5.2.3 Person-Person via Video

These types of attacks are the ones where the attacker may use video as a medium for communication to orchestrate social engineering attacks. The explosive growth in the use of internet and increasing broadband penetration around the world has been responsible for the success of websites like YouTube that allow people to share knowledge and communicate through videos. A typical attack of this kind could involve circulating a video claiming to be a 'tutorial' of sorts with a set of instructions to a pre-created problem created by the attacker. If an unsuspecting victim who is affected by the pre-created problem comes across this video online, he or she will willingly follow the instructions and fall prey to the set trap. This type of an attack is quite similar to the reverse engineering technique discussed earlier where the attacker lures the victim by claiming that he has a solution to a pre-created problem. Though there are no reports of such attacks in the media yet this is a definite viable avenue for the hackers to exploit given the number of people who are watching and sharing videos online today.

6.0 Countermeasures for Social Engineering

The most basic definition of social engineering is hacking the human brain. Regardless of the technological advances in the security field this form of attack will be persistent as it is difficult to upgrade or patch human brains as we can to technology (Townsend, 2010). The best strategy is to engage in activities that raise the awareness levels of such attacks through education. A multi layered strategy that implements training to increase awareness and enforces policies like 'need-to-know' access should be employed by organizations to mitigate the effect of these attacks. Social engineering is a game and hence the goal should be to make things difficult for the attacker and reduce or better remove the fun element so that the attacker moves on to a different target.

7.0 Conclusion:

In this paper we tried to bring some clarity to the different types of social engineering attacks through our taxonomy approach. We hope that this taxonomy will be useful to organizations to understand the attack vectors better and consequently be useful in building robust and effective countermeasures for the threats they impose. There definitely is a conscience that this taxonomy may not be complete yet in its entirety and hence we welcome any suggestions from the academic community to suggest any edits. The social methods employed to get around technological countermeasures is a dynamic process where the motivated attacker will always try to up the ante against the victim. As such, we will be documenting these changes and will constantly iterate our taxonomy to make it current.

Taxonomy of a Social Engineering attacks

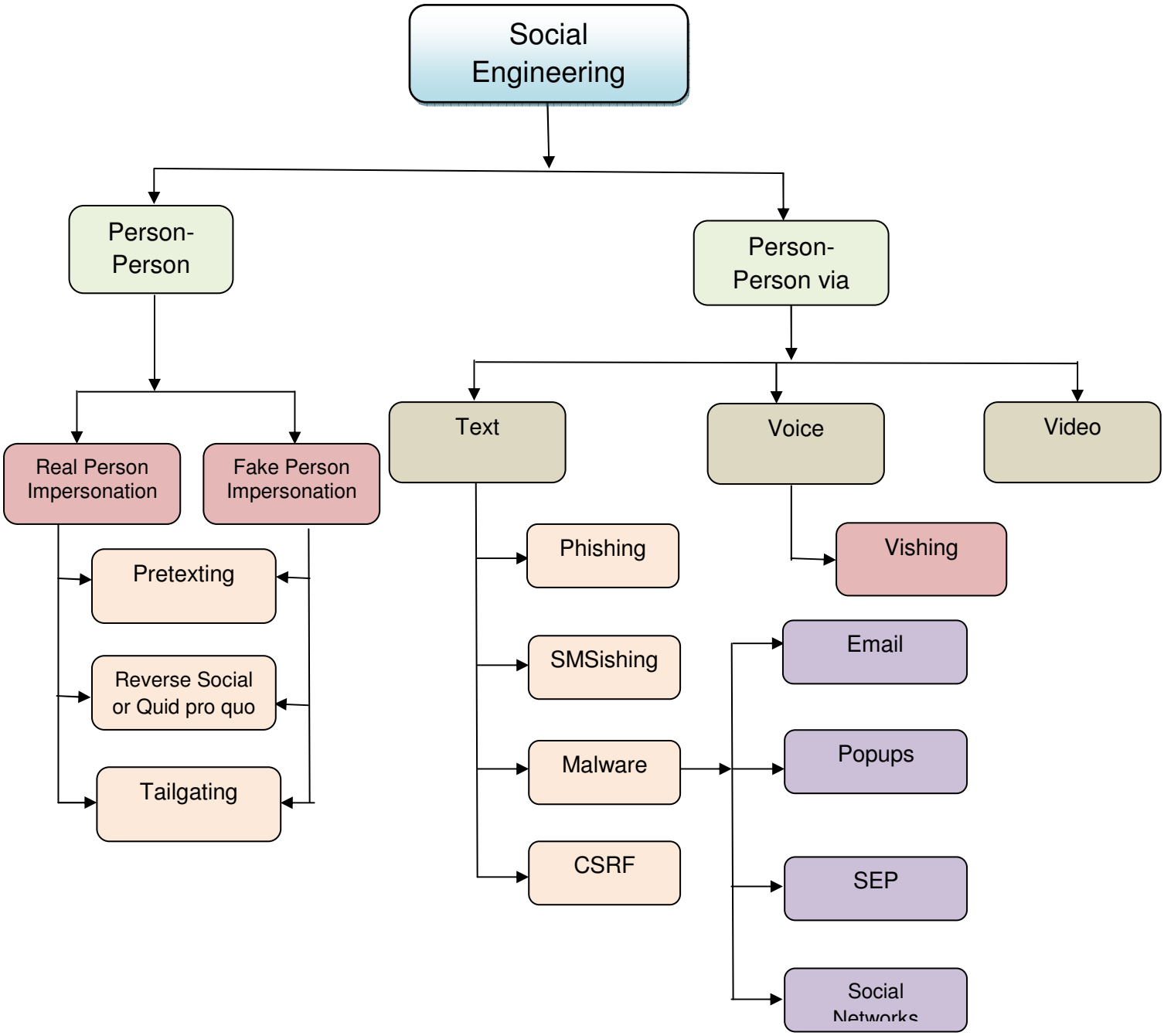

Figure 2: Taxonomy for Social Engineering attacks

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics and implications. Technology in Society, 1-14.

Aiello, M. (2007). "Social Engineering" in: Cyber Warfare and Cyber Terrorism, A.Colarik and L.Janczewski (eds.)Yurchak Printing Inc, New York, 191-198.

Baer, M. H. Corporate Policing and Corporate Governance: What Can We Learn from Hewlett-Packard's Pretexting Scandal? University of Cincinnati Law Review, Corporate Law Symposium, 2008.

Barber, R. (2001). Social engineering: A People Problem? . Network Security(7), 9-11.

Barrett, N. (2003). Penetration testing and social engineering: Hacking the weakest link. Information Security Technical Report, 8(4), 56-64.

Bhagyavati. (2007). "Social Engineering" in: Cyber Warfare and Cyber Terrorism, A. Colarik and L. Janczewski (eds.). Yurchak Printing Inc, New York, 182-190.

Binay, D. (2009). Android anti-SMSishing. Retrieved 20 December, 2010, from http://code.google.com/p/anti-smsishing/

Calluzzo, V., & Cante, C. (2004). Ethics in Information Technology and Software Use. Journal of Business Ethics, 51(3), 301-312.

Damle, P. (2002). Social Engineering: A Tip of the Iceberg. Information Systems Control Journal, 2.

Duff, A. S. (2005). Social Engineering in the Information Age. The Information Society: An International Journal, 21(1), 67 - 71.

FBI. (2010). Protect Your Computer: Don't be Scared by 'Scareware'. Retrieved 20 December, 2010, from http://www.fbi.gov/news/stories/2010/july/scareware/scareware

Granger, S. (2001). Social engineering fundamentals, part I: Hacker tactics.

Gulati, R. (2003). The threat of social engineering and your defense against it. Information Security Reading Room, SANS.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31-43.

Hansson, S. O. (2006). A note on social engineering and the public perception of technology. Technology in Society, 28(3), 389-392.

Harley, D. (1998). Re-floating the Titanic: Dealing with social engineering attacks. Proceedings of the European Institute for Computer Antivirus Research.

Huber, M. K., S.; Nohlberg, M.; Tjoa, S. (2009). Towards Automating Social Engineering

Using Social Networking Sites. 2009 International Conference on Computational Science and Engineering, 3, 117 - 124.

Kamal, M., & Crews, D. (2008). The Psychology of IT Security in Business. The Journal of American Academy of Business, 13(1), 5.

Laribee, L. (2006). Development of Methodical Social Engineering Taxonomy Project. from http://handle.dtic.mil/100.2/ADA457544

Lee, D. H., Choi, K. H., & Kim, K. J. (2007). Intelligence Report and the Analysis Against the PhishingAttack Which Uses a Social Engineering Technique. Proceedings of the 2007 international conference on Computational science and Its applications 2.

Lindqvist, U., & Jonsson, E. (1997). How to systematically classify computer security intrusions. Paper presented at the Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on Security and Privacy.

Long, J. (2008). No Tech Hacking. Syngress publishing, Inc.

Manske, K. (2000). An Introduction to Social Engineering. Information Security Journal: A Global Perspective, 9(5), 1-7.

Menn, J. (2010). How one corporate misstep led to a change in American law. Financial Times(7).

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons.
Naraine, R. (2008). Twitter being used to distribute malware. Retrieved 20 December, 2010, from http://www.zdnet.com/blog/security/twitter-being-used-to-distribute-malware/1640
Ollmann, G. (2007). The Vishing Guide. IBM Global Technology Services Retrieved 20 December, 2010, from http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf
OWASP. Cross-Site Request Forgery (CSRF). Retrieved 20 December, 2010, from http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
Reardon, L. (2009). Email Statistics Report, 2009-2013. Retrieved 20 December, 2010, from http://www.radicati.com/?p=3237
Redmon, K. C. (2005). Mitigation of Social Engineering Attacks in
Corporate America. Retrieved 20 December, 2005, from http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_KRedmon.pdf
Roßling, G., & Muller, M. (2009). Social Engineering: A Serious Underestimated Problem. Proceedings of the 14th annual ACM SIGCSE conference on Innovation and technology in computer science
Straub, D. W., Jr., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly, 14(1), 45-60.
Thompson, S. T. C. (2006). Helping the Hacker? Library Information, Security and Social Engineering. Information Technology & Libraries 25(4), 222-225.
Thornburgh, T. (2004). Social Engineering: The “Dark Art”. Proceedings of the 1st annual conference on Information security curriculum development.
Townsend, K. (2010). The art of social engineering. Infosecurity, 7(4), 32-35.
Twitchell, D. P. (2006). Social engineering in information assurance curricula. Paper presented at the Proceedings of the 3rd annual conference on Information security curriculum development.
Workman, M. (2008). A test of interventions for security threats from social engineering. Information Management & Computer Security, 16(5), 463-483.