December 2006

Social Network Theoretic Framework for Organizational Social Engineering Susceptibility Index

Manish Gupta
M&T Bank Corporation

Raj Sharman
School of Management SUNY

Social Network Theoretic Framework for Organizational Social Engineering Susceptibility Index

Manish Gupta
Executive, Information Security
M&T Bank Corporation
Buffalo NY, USA
mgupta@mandtbank.com

Raj Sharman
Assistant Professor
School of Management SUNY
Buffalo, NY, USA
rsharman@buffalo.edu

ABSTRACT
Social Engineering is an undeniable and pervasive threat to the security of information systems of an organization due to its reliance on social nature of human beings. Social engineering uses dynamic art of manipulating social behavior of human relationships to obtain unauthorized and privileged information. Corporations have pressing need to design and implement reasonable countermeasures and controls to effectively mitigate social engineering attacks. In this paper, we propose a framework for development of social engineering susceptibility index (SESI) that reveals real risks from social engineering attack that an organization's employees are exposed to. Risk managers can compute the SESI index, which is based on social network theory propositions, to understand risk exposure of a critical group of individuals or organizational departments to proactively engage in elevating security measures. The framework equips risk managers with an understanding to design better security decisions and proper policies and measures to reduce risk.

Keywords
Social engineering, social network theory, insider attacks, organizational security, social networks, susceptibility index.

INTRODUCTION

Social Engineering is an ongoing threat to the computer security paradigm, against which it is difficult to protect using conventional or state-of-art technological security mechanisms. At the same time, while information systems deal with human interactions and communications through use of technology, it is impossible to separate the human elements from the technological ones. There is no fine boundary of measurable variables that can be established to draw the line along which we can look at clear-cut cause and effect relationships in either direction between technology and human elements (Turoff, 1986). Because of this, organizations and individuals alike must arm themselves with the knowledge of what information can be used, how information divulged could precipitate further attacks or actual compromise of their systems, how the attacker develops the attack, and in what forms the attack may appear (Thornburgh, 2004).

Successful social engineering attacks give the attacker the means to bypass millions of dollars invested in technical and non-technical protection mechanisms (Manske, 2000). The social engineer uses human emotion and manipulation to trick the victim into giving out privileged information (Orgill et al., 2004). In an organizational setting, support and utilization of information systems usually requires the coordination and collaboration of many individuals spread among numerous divisions of an organization. This poses interesting challenges in understanding the socio-organizational structures and interactions to understand and thwart social engineering attacks. While it may be impossible to completely protect from social engineering attacks, the risks can be mitigated (Mitnick and Smith, 2002).

The social engineering susceptibility index presented in the paper aims to provide insights into social behaviors that unravels the risk exposure of an organization to social engineering attacks from insiders. The framework utilizes propositions and postulates of social network theory in combination with organizational dynamics to develop a social engineering susceptibility index (SESI). The contribution of the paper is two-fold. First, it elaborates socio-organizational components

and characteristics that role-play in social engineering attacks initiated by insiders. Second, it presents a risk-based framework to determine a social engineering susceptibility index (SESI) for individuals or departments, leveraging propositions and constructs of social network theory.

The organization of paper is as follows: Section 2 discusses existing work in social engineering and use of social network theory for risk assessments and analyses. This section also presents overlapping research amongst the areas. Section 3 presents preliminaries and introductions on concepts and operational definitions for SESI framework. Our main contribution lies in Section 4, where we present discussions on propositions of social network theory as they are employed in illustrating methodologies for risk assessment of social engineering attacks in an organizational context. This section develops SESI that represents susceptibility of individuals/departments in an organization to social engineering attacks. Section 5 concludes the paper with conclusion of the discussions in paper and brief discourse on future work.

EXISTING WORK: LITERATURE SURVEY

Social Engineering is an ever-present threat to the security of computer systems due to the illogical, social nature of human beings. Mitigation measures include educating users regarding the threat, and the means social engineers use to obtain privileged information (Hitchings, 1995). This narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be (Hitchings, 1995; Davis and Price, 1987). The hacker will work hard to maintain an apparently innocent relationship, while learning company lingo, names of key personnel, names of important servers and applications, and a host of other valuable information (Granger). Social engineering is generally successful because people are naturally helpful. Having to deal with a lot of information quickly affects logical functioning and can produce "sensory overload" (Burtner, 1991). Since security mechanisms are designed, implemented, breached by people, human factors should be considered in their design. The framework presented in Section 4 considers human relationships and attributes to uncover patterns of insider initiated social engineering attacks.

Many social engineering attacks are made possible with help from the inside of an organization. These threats are commonly referred to as "The Insider Threat" (Littman, 1998). Insider threats are the greatest threat to individual and corporate privacy (Littman, 1998). Studies have been conducted to explore the challenges in coordinating work across organizational and geographical boundaries (Carstensen and Sorensen, 1996; Olson and Teasley, 1996), which can be used to understand social engineering attack channels and mechanisms. Insecure work practices and low security motivation have been identified by research on information security as major problems that must be addressed (DeAlvare, 1990; Ford, 1994; Gordon, 1995). Existing literature survey does not reveal any focused research on understanding social engineering attacks from a social network theory perspective.

Researchers have used social network theory (Granovetter, 1973 and 1983; Milgram, 1997) to discuss issues surrounding privacy and trust in online social circles. Primarily discussions have been on trust and intimacy issues in online networking (Boyd, 2004; Donath and Boyd, 2004). Our contextual relevance in this paper is offline social networks. Social network theorists have discussed the relevance of relations of different depth and strength in a person's social network (Granovetter, 1973 and 1983) and the importance of so-called weak ties in the flow of information across different nodes in a network. Network theory has also been used to explore how distant nodes can get interconnected through relatively few random ties (Granovetter, 1973 and 1983). While an offline social network may include up to a dozen of intimate or significant ties and 1000 to 1700 "acquaintances" or "interactions" (Donath, 2004; Strahilevitz, 2004). It is critical that an individual must realize that a social engineer is trying to manipulate them and that they are personally vulnerable to such manipulation (Sagarin et al., 2002).

PRELIMINARIES

Social Engineering

Social Engineering is a technique used by hackers or other attackers to gain unauthorized access to secure systems through obtaining the privileged information by manipulating human behavior. Mitnick identifies 4 distinct stages of "The Social Engineering Cycle:" research, developing rapport and trust, exploiting trust, and utilizing information (Mitnick and Smith, 2002). Social engineering, by any name, has existed in many forms throughout history and will continue to exist because it relies on human nature (Thornburgh, 2004). Because of this, organizations and individuals alike must equip themselves with the knowledge on social engineering attacks such as what information can be used, how information divulged could precipitate attacks, how the attacker develops the attack, and in what forms the attack may appear. The risk assessment

framework in Section 4 develops a susceptibility index to determine the most attractive targets for social engineering in an organization.

Social Network theory

Social network theory views social relationships in terms of nodes and ties. Nodes are the individual actors within the networks, and ties are the relationships between the actors. There can be many kinds of ties between the nodes. In its most simple form, a social network is a map of all of the relevant ties between the nodes being studied. This approach has turned out to be useful for explaining many real-world phenomena, but leaves less room for individual agency, the ability for individuals to influence their success, so much of it rests within the structure of their network. Social networks have also been used to examine how companies interact with each other, characterizing the many informal connections that link executives together, as well as associations and connections between individual employees at different companies (Isworld.org, 2006).

SOCIAL NETWORK THEORETIC SOCIAL ENGINEERING SUSCEPTIBILITY INDEX

FRAMEWORK BACKGROUND

This paper discusses propositions of social network theory in light of their significance in risk assessment of social engineering attacks initiated by insiders in an organization and to develop social engineering susceptibility index. The discussion presented in this section attempts to identify attributes and social patterns in an organization that are most likely to be targets of social engineering attacks. A risk manager can use the SESI to evaluate 1) an individual, 2) a functional group (organizational department) or 3) a social group. The computed SESI can provide a quantitative

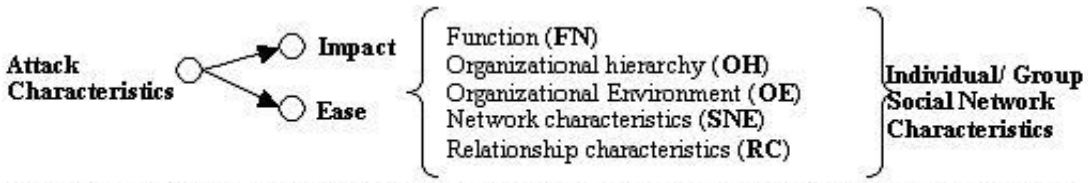

Figure 1: Organizational characteristics and components involved in a social engineering attack

assessment of risk exposure to social engineering attack, for the evaluated entity. This understanding can help them design targeted security polices and programs to mitigate risks from social engineering. Figure 1 presents organizational characteristics and components that inter-play in a social engineering attack. The social network characteristics are explained in detail in the framework presented in following sections. Each characteristic is designed as an index (Table 1) and is composed of social network theory based propositions (ratings). The SESI is composed of characteristic based indices, which in turn have ratings as their constituents. Figure 2 presents a graphical view of the framework illustrates the steps involved SESI computation.

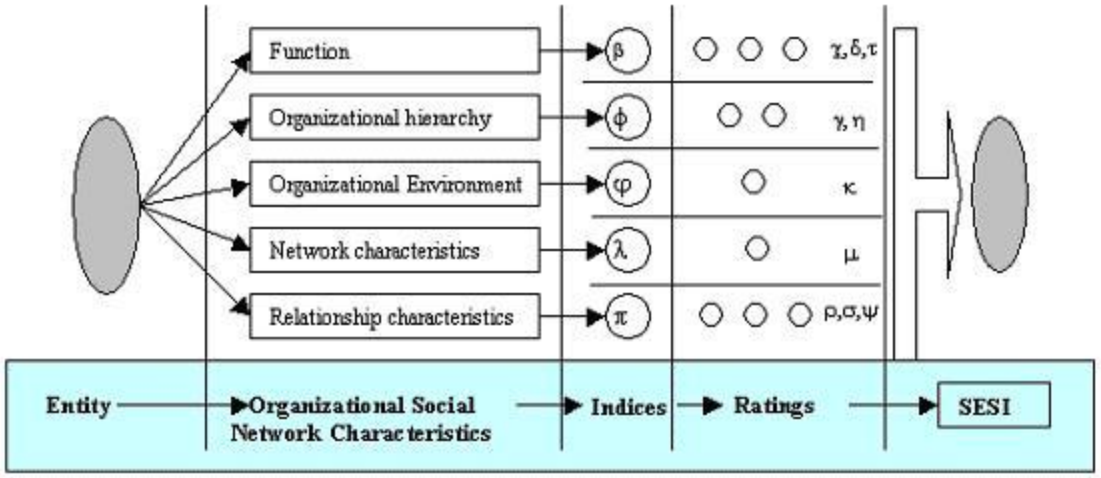

FIGURE 2: SOCIAL ENGINEERING SUSCEPTIBILITY INDEX (SESI) FRAMEWORK

The targets of the social engineering have common social attributes that relate to their attractiveness to a social engineer. This attractiveness varies in degrees of *impact* and *ease*. Degree of impact implies the magnitude of results obtained by such attack. Ease corresponds to convenience with which the attack can carried out that can be expressed in terms of gullibility of victim and knowledge of the perpetrator about the victim's characteristics or environment.

We discuss the characteristics from victim's perspective in the following subsections. Table 1 shows the notations, ratings and indices used in the framework development and discussion in following sections. We have presented risk assessments and propositions of social network theory side-by-side along the discussions below for their associations and

NOTATION	DESCRIPTION / CONSTRUCT	SECTION	SOCIAL NETWORK CHARACTERISTIC
Π	Social Engineering Susceptibility Index	4	
β	Social Function Index	4.1	(FN)
χ	Core Attribute Attractiveness Rating	4.1.1	(FN)
δ	Primary group membership rating	4.1.2	(FN)
τ	Social Centrality Rating	4.1.3	(FN)
ϕ	Organizational Hierarchy Index	4.2	(OH)
γ	Homophilous Rating	4.2.1	(OH)
η	Effective Distance Rating	4.2.2	(OH)
φ	Organizational Environment Index	4.3	(OE)
κ	Social Interpersonal Rating	4.3.1	(OE)
λ	Network characteristics Index	4.4	(SNE)
μ	Social Capital Rating	4.4.1	(SNE)
π	Relationship Characteristics Index	4.5	(RC)
ρ	Weak Ties Rating	4.5.1	(RC)
σ	Impersonation Rating	4.5.2	(RC)
ψ	Named Relations and Positions Rating	4.5.3	(RC)

Table 1: Notations Used in Social Engineering Susceptibility Index Framework

The framework indices' and ratings' discussion presented in the following sections have following conventions and assumptions:

1) The social network theory proposition is mentioned after the sub-heading in italics
2) All the equations are labeled based on section number they are discussed.
3) All the indices ($\beta,\phi,\varphi,\lambda,\pi$) and all ratings ($\chi,\delta,\tau,\gamma,\eta,\kappa,\mu,\rho,\sigma,\psi$) can be evaluated in an *ordinal variable rating scale* of 1 to 10. Exact calculations and validations are beyond the coverage of the paper.
4) Throughout the framework, higher rating or index implies higher overall SESI, other factors kept equal.
5) All the ratings and indices depict *associative behavior* with the SESI (Π). For example, a higher χ (rating) implies a higher β(index), which in turn means higher SESI (Π), given other variables constant.

Overall, the susceptibility index is a direct function, f (), of 5 indices as follows (refer Table 1 for notational explanations):

$$\Pi = f(\beta,\phi,\varphi,\lambda,\pi)$$

Indices and its compositional ratings are discussed in next subsections.

Function (Social Function Index - β)

The more critical function a person does, the more attractive target he will serve for attackers. Attackers would expect to gain more from exploiting people of such social network. For example, typically the *access administrators* in an organization tend to be a ripe target for social engineering attacks as they hold the very high privileges, such as administrative access, in information systems that hold valuable personal and identity information of employees, customers, partners, etc.

Core Attribute Attractiveness Rating (χ)

Cores possess whatever attributes are most valued by the network.

This proposition says that in core/periphery structures the valuation of the attributes is related to the structure. The nodes that have the most of what is valued come to be the core, or the nodes that already have the most of what is valued impose their values on others who have less and confine them to the periphery (Kadushin, 1972). We develop a specific map to proposition in Figure 3 that demonstrates that *system administrators* usually have more attractive attributes and hence are more exposed to social engineering threats.

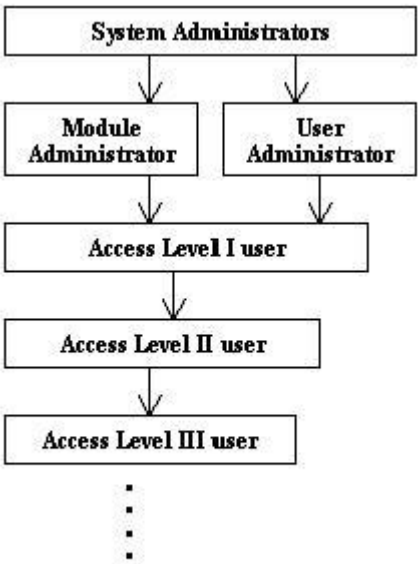

Figure 3: Attribute hierarchy structure

The peripheral circle to system administrators is formed of *module and user administrators* that have access rights to administrative tasks within the system. An attacker can dupe such roles to get him access to systems and breach security requirements of the system. Here the roles and functions of people as mandated by the attribute hierarchy clearly present the structure of information processing network of an organization. Hence, we have social function index (β) varies directly with core attribute attractiveness rating (χ) or,

$$\beta \alpha \chi \text{ ……[R11]}$$

Primary group membership rating (δ)

Members of social circles, especially core members, enjoy some characteristics of primary groups: social support and enforceable trust.

This proposition suggests that social circles can substitute for some of the attributes of primary groups, notably, the kind of social support that they offer. Importantly, social circles not only create the conditions for trust, but for enforceable trust. If trust is violated, there are sanctions that are expected and can be applied (Kadushin, 1972). In Figure 2, we observe that in information systems context, some of the desirable attributes in order of attractiveness are ranked in an order of attribute strengths or levels of privileges. This is where an individual complies because they feel it is their moral duty to. Part of this is guilt. People prefer to avoid guilt feelings and so if there is a chance that they will feel guilty they will if possible avoid this outcome (Harl, 1997). Again, here social function index (β) is directly proportional to primary group membership rating (δ), represented as follows:

$$\beta \alpha \delta \text{ ……[R12]}$$

Social Centrality Rating (τ)

Centrality proposition.

This proposition postulates that where centrality and independence are evenly distributed, there will be no leader, but many errors and high activity (Leavitt, 1951). The effects of positions of centrality have significant implications on functions that administrators of information systems provide. If there are fewer connections and more independence in their job roles, they are more vulnerable to social engineering attacks, their capabilities to verify the tactical frauds employed by an attacker. Besides, in such scenarios the detection of a fraud or attack becomes less visible and hence, takes unusually longer to detect in normal schedule of operations. We can follow from the proposition and arguments that social function index (β) is directly proportional to centrality:

$$\beta \alpha \tau \text{ ……[R13]}$$

Overall, from relations [R11], [R12] and [R13], we observe that social function index (β) is a function g1 (), represented as:

$$\beta = g1 (\chi,\delta,\tau) \text{ ……[R1]}$$

where χ,δ,τ are core attribute attractiveness rating, primary group membership rating and social centrality rating respectively.

Organizational Hierarchy (Organizational Hierarchy Index - ϕ)

Homophilous Rating (γ)

Homophily Vs: Connections, individuals and collectivities.

Homophily is defined as having one or more common social attributes, like the same social class. Two of more people can be said to be homophilous if their characteristics match in a proportion greater than expected in the population from which they are drawn or the network of which they are a part (Verbrugge, 1977). For the purpose of risk analysis and social engineering susceptibility index development, we regard homophily at different levels, one arising from the fact that our analysis is at organizational level and so all employees of a company are homophilous to one degree. Other level comes from the functional departments they work for. The proposition states that the greater the homophily the more likely two nodes will be connected, which is clearly evident from the structure or an organization chart.

At organizational level, whether homophily leads to a greater likelihood of a tie depends on the kind of a connection, i.e., within department or between-departments (Figure 4).

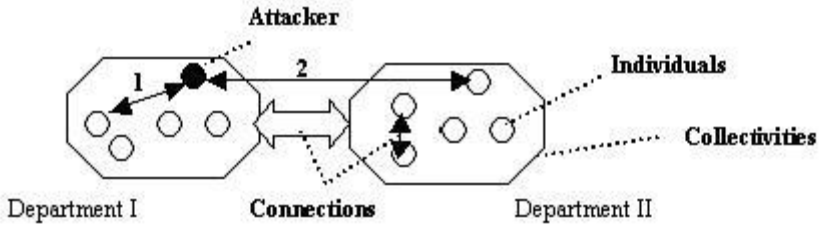

Figure 4 : Within and between department Connections, individuals and collectivities

Here risks come from the analysis of hierarchy that the more homophilous 2 people are the more knowledge they will know about each other that they can use as weapons for launching a social engineering attack. The collectivities that are inherent in a functional department in an organization should be more compartmentalized through separation of duties or segregation of data to mitigate the risks. In Figure 4, above, the attack path 2 is with less ease than the path 1. The homophilous nature of interaction makes attack 1 more likely to succeed. We can follow from the proposition and arguments that Organizational Hierarchy Index (ϕ) is directly proportional to degree of homophilous-ness:

$$\phi \alpha \gamma \quad \text{.....[R21]}$$

Effective Distance Rating (η)

(Effective) Distance between any two nodes

The distance between two nodes in a network is determined by four parameters: (1) the size of the first order zone of nodes in the network; (2) the extent to which nodes in the network have overlapping members in their first order zones; (3) barriers between nodes; (4) agency exercised by the nodes. The risks that arise here in social engineering attacks are from the interpersonal dynamics of an individual and visibility of the departmental role in an organization. Typically, probability of success in same functional group, say 1 or 2 in Figure 5, is higher than across groups. Also higher the position in hierarchy that the attacker impersonates, the authority of the impersonated person makes the attack more plausible.

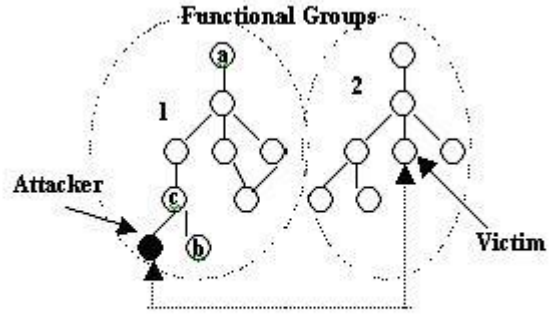

Figure 5: Organization hierarchy view of attack path and distance

For example, *prob*(a à b) > *prob*(a à c) *prob* (c à b) > *prob* (b à c) > *prob* (b à a) from the relative positions of a, b, and c in the organization hierarchy. Here, prob(x à y) is a function representing likelihood of success and higher frequency of attack paths and x is attacker and y is victim. Here, we can rationalize that Organizational Hierarchy Index (ϕ) varies directly with the distance between the nodes:

$$\phi \alpha \eta \quad \text{.....[R22]}$$

Overall, from relations [R21] and [R22], we observe that Organizational Hierarchy Index – (ϕ) is a function g2 (), represented as:

$$\phi = g2\ (\gamma,\eta) \ldots\ldots [R2]$$

where γ,η are Homophilous Rating (γ), and Effective Distance Rating respectively.

Organizational Environment (Organizational Environment Index - φ)

Social Interpersonal Rating (κ)

The Size of the Interpersonal Environment and The "Small World" phenomenon

The proposition states that the number of individuals in the interpersonal environment varies from about 300 to 5,000 persons, depending on how this is measured and the type of society in which the focal person is embedded (Simmel, 1950). The small world proposition states that if there were no overlap in people's personal networks, then one could reach the entire population of the United States in two or three steps (Pool and Kochen, 1978). The source of risks is the size the interpersonal environment. For the purpose of risk analysis, it can stated that greater the environment size the more likelihood of social engineering attacks. The rationale is that the greater size brings a complex pattern of interactions that cannot be isolated for analysis and is more vulnerable to attacks. The impact of social circles of individuals exhibiting such behavior has been analyzed by Simmel (Kadushin, 1969).

Here, we can rationalize that Organizational Environment Index – (φ) varies directly with the social interpersonal rating and can be represented as:

$$\varphi\ \alpha\ \kappa \ldots\ldots [R31]$$

This relation, [R31], can be alternatively represented as function g3 () :

$$\varphi = g3\ (\kappa) \ldots\ldots [R3]$$

where κ is social interpersonal rating.

Network Characteristics (Network characteristics Index - λ)

Social Capital Rating (μ)

The greater the number of intersecting social circles of which a node is a member, the greater that node's social capital.

From risk analysis standpoint, the greater the number of social circles, the higher would the chances of a successful social engineering attack. The individuals with higher access to other disparate circles would tend to be more informative of the attacks behaviors and would be able to recognize a pattern before the revealing confidential information. Further, an important aspect of networks, as in Section 4.1, is that persons who have access to many disparate circles are more likely to be brokers, a of social capital that lends an intuitive relationship with others. This nature of relationship keeps the victim wary of unusual patterns. It is corroborated by the research that they do not have a formal leadership structure and is largely non-hierarchical, and has much space between the nodes (Kadushin, 1969).

Here, we can rationalize, based on proposition and arguments that Network characteristics Index (λ) varies directly with the social capital rating and can be represented as:

$$\lambda\ \alpha\ \mu \ldots\ldots [R41]$$

This relation, [R41], can be alternatively represented as function g4 () :

$$\lambda = g4\ (\mu) \ldots\ldots [R4]$$

where μ is social capital rating.

Relationship Characteristics (Relationship Characteristics Index - π)

Weak Ties Rating (ρ)

Weak ties facilitate the flow of information from otherwise distant parts of a network; and weak ties help to integrate social systems.

The propositions suggest that individuals with few weak ties will be deprived of information from distant parts of the social system and will be confined to the provincial news and views of their close friends. New ideas will spread slowly, and subgroups that are separated by race, ethnicity, geography or other characteristics will have difficulty reaching a *modus vivendi* (Granovetter, 1982). Separation of geography, ethnicity, etc produces gaps that the attackers cannot easily bridge to launch an attack in an organization setting. For example, an attacker in one location of an organization would have less information about the environment and characteristics of other location making attack ineffective. Also, in the same context, the impersonation of ethnical characteristics of a possible victim makes such targets less attractive. This shows that higher the weak ties, lower the overall susceptibility to social engineering attacks, represented as:

$$\pi \alpha^{-1} \rho \quad \text{.....[R51]}$$

Impersonation Rating (σ)

Taking the role of the other.

Social network theory provides excellent insights into social phenomenon and interactions that are operational during a social engineering attack. Most common method of obtaining unauthorized information is impersonating the user whose information is being solicited. Prepositions state that recognizing the other as having separate subjectivity and agency is a vital requirement in social networks. Besides the attacker requires self-knowledge and the ability to be reflexive about the self as well as knowing the desires/characteristics of the other. These are the forces that promote these social "impersonation" processes that might apply across various system levels from the person to the organization and even to larger entities (Simmel, 1950). The social attributes to impersonate effectively is inversely proportional to be duped directly, an inverse relationship:

$$\pi \alpha^{-1} \sigma \quad \text{.....[R52]}$$

Named Relations and Positions Rating - ψ

Informal and named relations and; Stability of named positions

"Informal" or non-prescribed or non-instituted relations tend to be correlated with the formal or prescribed relationships. Network relations can be prescribed by values, organization and institutions. Prescribed relations are given a name. The more formal structure an organizational unit possess the more information is available formally about the individuals and connections that an attacker can use to launch social engineering attacks. A common tactic of "*names dropping*" becomes even more feasible in named positions. Kevin Mitnick, a well known hacker, describes the reactions he has seen, "In the corporate environment, people are unlikely to evaluate a request thoroughly, so they take a mental shortcut" (Farber, 2002). Here, we can follow from the rationales and discussions that named and higher relations and positions attract more attention and hence bear increased susceptibility to social engineering attacks:

$$\pi \alpha \psi \quad \text{.....[R53]}$$

Overall, for Relationship Characteristics Index(π), from relations [R51], [R52] and [R53], we observe that π is a function g5 (), represented as:

$$\pi = g5\ (\rho,\sigma,\psi) \quad \text{.....[R5]}$$

where χ,δ,τ are weak ties rating, impersonation rating and named relations and positions rating respectively.

For the framework we deduce that social engineering susceptibility index to be:

$$\Pi = f\ (\beta,\phi,\varphi,\lambda,\pi)$$

$$\boxed{\Pi = f(\ g1\ (\chi,\delta,\tau),\ g2\ (\gamma,\eta),\ g3\ (\kappa),\ g4\ (\mu),\ g5\ (\rho,\sigma,\psi)}$$

The SESI index is calculated in an ordinal scale of 1 to 10, same scale as used by other indices and ratings. Risk and information systems managers, to evaluate exposure of critical individuals or groups in an organization, can use the SESI

index. This index will help them make informed and better security departments for elevated level of protection for identified group.

CONCLUSION

Social engineering is a very real threat and one that currently has fairly free reign. Businesses have to start taking social engineering seriously by applying the social sciences to protect against the threat. With an understanding of risks and multi-layered defense, social engineering will become a much more difficult attack to carry out. SESI index, which is based on social network theory propositions, can be employed to understand risk exposure of a critical group of individuals or organizational departments to proactively engage in elevating security measures. SESI can serve as a vital security strategy development tool for risk and systems managers. As future works on the framework presented in this paper, more rigorous analytical and mathematical tools can be used to refine the discussed analyses.

REFERENCES

1. Turoff, Murray. (1986) The rational, the pragmatic and the inquiry process: The social study of information-communication systems, Feb-1986, *ACM SIGCAS Computers and Society*, Vol-15-Issue-4.
2. Thornburgh, Tim (2004) Social engineering: the "Dark Art", *Proceedings of 1st Annual Conference on Information security curriculum development.*
3. Manske, K. (2000) An introduction to social engineering, *Information Systems, Security* 9,53-59.
4. Orgill, Gregory L., Romney, Gordon W., Bailey Michael G., Orgill, Paul M. (2004) Security III: 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.*
5. Mitnick, K. and Smith, W. (2002) *The Art of Deception*, Indianapolis : Wiley Publishing Inc.
6. Littman, J. (1998). Inside jobs: Is there a hacker in the next, cubicle? Retrieved on 2/22/2006 http://www.cnn.com/TECH/computing/9808/13/hacker.idg/.
7. Carstensen, P. H. and C. Sorensen. (1996) From the Social to the Systematic: Mechanisms Supporting Coordinating in Design. Computer Supported Cooperative Work, *The Journal of Collaborative Computing*. 5, 4 (1996), 387-413.
8. Olson, J. S. and S. Teasley. (1996) Groupware in the Wild: Lessons Learned from a Year of Virtual Collocation, *Proceedings of ACM Conference on Computer Supported Cooperative Work CSCW '96*.
9. Hitchings, J. (1995) Deficiencies of the traditional approach to information security and the requirements for a new methodology. Computers and Security, 14, 377–383.
10. Davis, D. and Price, W. (1987) Security for Computer Networks. Wiley, Chichester.
11. DeAlvare, A.M. (1990) How crackers crack passwords or what passwords to avoid, *Proceedings of Unix Security Workshop II*, Portland.
12. Ford, W. (1994) *Computer Communications Security: Principles, Standard Protocols and Techniques*, Prentice Hall, NJ,.
13. Gordon, S. (1995) *Social Engineering: Techniques and Prevention. Computer Security*.
14. Boyd, D. (2004) Friendster and publicly articulated social networking, *Conference on Human Factors and Computing Systems (CHI 2004)*, April 24-29, Vienna, Austria.
15. Donath, J. and Boyd, D. (2004) Public displays of connection, *BT Technology Journal*, 22:71–82.
16. Granovetter, M. (1973) The strength of weak ties. *American Journal of Sociology*, 78:1360–1380.
17. Granovetter, M. (1983) The strength of weak ties: *A network theory revisited. Sociological Theory*, 1:201–233.
18. Milgram. S. (1997) The familiar stranger: An aspect of urban anonymity. In S. Milgram, J. Sabini, and M. Silver, eds, *The Individual in a Social World: Essays and Experiments*. Addison-Wesley, Reading, MA.
19. Strahilevitz, L. J. (2004) A social networks theory of privacy. The Law School, University of Chicago, John M. Olin, *Law & Economics Working Paper* No. 230 (2D Series).

20. Sagarin, Brad J.; Cialdini, Robert B.; Rice, William E.; Serna, Sherman B. (2002) "Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion." *The Journal of Personality & SocialPsychology*: Vol. 83(3), Sept-2002, 526-541.
21. Isworld.org, "Social Network Theory", retrieved on 2/2/2006 from http://www.istheory.yorku.ca/socialnetworktheory.htm
22. Burtner, William Kent. (1991) "Hidden Pressures." *Notre Dame Magazine*, Winter 1991- 92 p29-32.
23. Granger, Sarah. "Social Engineering Fundamental, Part I: Hacker Tactics." Security Focus Online. URL: http://online.securityfocus.com/infocus/1527.
24. Kadushin, Charles. (1972) Chapter 2. Some Basic Network Concepts and Propositions, *Introduction to Social Network Theory*, Retrieved from home.earthlink.net/~ckadushin/Texts/Basic Network Concepts.pdf
25. Harl. (1997) "People Hacking: The Psychology of Social Engineering" Text of Harl's Talk at Access All Areas III, March 7, 1997. http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html
26. Granovetter, M. (1982) "The Strength of Weak Ties: a Network Theory Revisited." Pp. 105-30 in *Social Structure and Network Analysis*, eds. Marsden and Linn. Beverly Hills, Ca: Sage.
27. Farber, Dan. (2002) "Mitnick on Mitnick: ' Why I'm going legit' (Part Two) Interview with Dan Farber." ZDNet, Oct-2002.
28. Leavitt, Harold J. (1951) "Some Effects of Certain Communication Patterns on Group Performance." *Journal of Abnormal and Social Psychology* XLVI:38-50.
29. Verbrugge, Lois M. (1977) "The Structure of Adult Friendship Choices." *Social Forces* 56576-97.
30. Pool, Ithiel S. and Manfred Kochen. (1978)"Contacts and Influence." *Social Networks* 1(1):5-51.
31. Simmel, Georg. (1950) The Sociology of Georg Simmel, ed. KH Wolff, NY: Free Press.
32. Kadushin, Charles. (1969). *Why People Go to Psychiatrists*. NY: Atherton Press.