# A Framework for Conceptualizing Social Engineering Attacks

Jose J. Gonzalez[1], Jose M. Sarriegi[2], and Alazne Gurrutxaga[2]

[1] Agder University College, Faculty of engineering and science,
Research Cell "Security and Quality and Organizations," Serviceboks 509,
4884 Grimstad, Norway
(and Gjøvik University College, NISlab, 2802 Gjøvik, Norway)
[2] Tecnun (University of Navarra), Manuel de Lardizábal 13,
20018 San Sebastian, Spain
jose.j.gonzalez@hia.no, jmsarriegi@tecnun.es,
A900348@alumni.tecnun.es

**Abstract.** At the highest abstraction level, an attempt by a social engineer to exploit a victim organization either attempts to achieve some specific target (denial of service, steal an asset, tap some particular information) or it wishes to maximize an outcome, such as to disable the organization by a terrorist attack or establish a permanent parasitic relationship (long-term espionage). Seen as dynamic processes, the first kind of exploit is a controlling ("balancing") feedback loop, while the second kind is a reinforcing feedback loop. Each type of exploit meets a first line of defense in control processes or in escalating ("reinforcing") processes of resistance. The possible combinations of the two modes of attack and the two modes of defense yield four archetypes of exploit and natural defense. Predictably, the social engineer would seek to outsmart the first line of defense; it is shown that each archetype implies a particular strategy to do so. Anticipation of these modes of attack must be the starting point for an effective multi-layered defense against social engineering attacks.

**Keywords:** Social engineering, critical infrastructure, pattern recognition, system archetype, system dynamics, information security.

## 1 Introduction

While the technical security of most critical infrastructure is high, it remains vulnerable to attacks from social engineers, whether outsiders or insiders. A report released in October 2004 by the Gartner Research Group concluded: «The greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses.» [Quoted in ref. 1, p. 152]. No exception for the vulnerability of critical infrastructure to social engineering attacks is made in this prediction or in recent assessments by other security expert groups. The recent study by Keeney et al. [2] on computer system sabotage in critical infrastructure sectors mentions examples of social engineering techniques (p. 27, 40).

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 79 – 90, 2006.

In the context of information security, social engineering is «the term that hackers give to acquiring information about computer systems through non-technical means» [3]. The Gartner Research Group defines social engineering as «the manipulation of people, rather than machines, to successfully breach the security systems.» [Quoted in ref. 1, p. 152] Wikipedia [4] defines it as «the practice of obtaining confidential information by manipulation of legitimate users.» It has been claimed that social engineers typically proceed by gathering information about people in the target organization, and then applying "neuro-linguistic programming" techniques (NLP) [5]. Harl in "People Hacking" [6] states succinctly: «social engineering is the art and science of getting people to comply to your wishes.» Social engineering is closely related to what magicians call "psychological forcing": An agent inserts surreptitiously grounds for false belief into the stream of consciousness of people; then they can be lead to make what they experience as free and rational decisions when it is the agent who controls their actions [7, p. 243]. Social engineers take advantage from existing security breaches or vulnerabilities (such as employees' poor training, ineffective segregation of duties or faulty supervision of tasks).

Much is found in the Internet, in magazines and newspapers about social engineering, because deception is central for innumerable phishing attacks, propagation of worms and even for spamming. However, there are comparatively few peer reviewed papers and books dealing with social engineering. Of particular interest is research documenting social engineering attacks from the perspective of the attacker. An early study by Winkler [3] described a social engineering attack against a company with their permission, demonstrating how easily unauthorized access can be obtained. Ten years later, this is still very much the case: A recent paper defining a metric for resistance to social engineering [8] concludes «our experiment shows that it is relatively cheap and easy to mount a large scale social engineering attack (or experiment) with a high success rate.» Are there strong reasons to exclude organizations and companies within the critical infrastructure from this gloomy prediction? From our personal experience as consultants and scientific researchers we would conclude that the danger to critical infrastructure from social engineering attacks is real and increasing.

Given the scarcity of strictly controlled scientific studies of social engineers assaults [3, 5, 8], the next best source are the books by Winkler [9, 10] and by Mitnick & Simon [11], which mostly consist of anecdotal evidence. The books have a plethora of details, but we argue that something is missing: A simple way to conceptualize social engineering attacks. Without a framework that allows to recognize attack patterns, the social engineering cases described in the books [9-11] read mostly like a game of check described in terms of moves of individual figures. While there is no yet general agreement about how chess masters think, it is widely agreed that pattern recognition is one of the crucial elements [12]. Master chess players think in terms of strategic patterns: *openings* (such as Caro-Kann Defense, English Opening, King's Pawn Opening, Sicilian Defense); *middlegame strategies* (such as forking, skewering, pinning, discovered checks, sacrifices); and *endgame studies*. We argue that descriptions of social engineering attacks in terms of system archetypes have qualities as strategic patterns: they conceptualize crucial aspects of the attack and defense process; they are cognitively simple; they are fairly easy to recognize and to interpret; they are modular and can be combined.