12TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND
TECHNOLOGY SYMPOSIUM

ADAPTING C2 TO THE 21ST CENTURY

SOCIAL ENGINEERING:
A study on the weakest link in information systems security – the human factor.

<u>(student abstract)</u>

Cognitive and Social Issues

Carlos Alexandre [student]
Paulo Viegas Nunes

Information Warfare / Competitive Intelligence Post-Graduation student
at the Military Academy in Lisbon

Military Academy

Rua Gomes Freire, 1169-203 Lisboa

Telephone: 351217953492 / Fax: 351217905271

carlos.alexandre@cgd.pt

Abstract

Social Engineering: A study on the weakest link in information systems security – the human factor.

In this article we'll analyze the state of art of social engineering, describing possible attack typologies and psychological associated factors.
"Social engineering refers to lying, cheating, tricking, seducing, extorting, intimidating and even threatening employees into revealing confidential information that can then be used to break into systems. Social engineering is based on deception and on violation of social norms of fairness and honesty." is the definition made by M.E.Kabay to describe social engineering.

As these forms of attack use mainly human vulnerabilities, although technical skills my also be used, there are no software or hardware to prevent, or even mitigate, this kind of risk.

The solution – also referred as "human firewall", which is not achievable in the short term, implies that behaviours need to change, and, in order to obtain this behavioural change, one must also look to disciplines not directly correlated to information security, such as social and cognitive psychology. Some high level concepts – personality issues, stressful conditions, collaboration and cooperation with someone pretending to be a working partner - from psychology are incorporated in this article.

In a fast speed change environment where technology have compelled us to analyse risk and vulnerabilities through a technological prism, let us take a moment to synthesize an old but ever present concept – deception, that now is called "Social Engineering".

"Loose lips sink ships", a famous WWII slogan, represents an actual, both military and civilian concern as it is impossible to program a human being.

Awareness, formation and education, three distinct concepts, are one of the keys, also brought to the present article, to architect the referred "human firewall".

Key Words

Social Engineering; Security; Human Factor; Awareness; Security Policies