

Topic Title: Social Engineering: Where's the Research?

Introduction

The problem of social engineering currently stands as one of the most under-researched problems in our field. The question as to why there is so little work in solving this problem seems to be that it is viewed as outside the domain of computer security. In other words, there is no viable technical solution to this problem. However, since both the hacker and security practitioner communities acknowledge that social engineering is often highly successful, we believe it is time we considered this problem within our research agendas.

Objectives

The main objective of this work is to conduct research in the area of social engineering. To date, most existing studies are anecdotal in nature with very little in the way of documented, repeatable work. Our research will begin the process of building a body of work that is documented, repeatable and practical in that the outcomes will lead to solutions for existing security problems.

Questions we will address include: Does training and education really work to counteract social engineering? If so, how much, what kind and how often does it need to be repeated? Are there other methods that work? Do computer policy and other enforcement mechanisms help with this problem? Is there an optimal combination of policy and training that works?

Research Plan

One of the authors actively conducts security assessments, which often contains a social engineering component. Clients will be recruited from this pool and with their permission allow us to gather data from real world examples. This will allow us to build a database of known techniques that do or do not work in a fashion similar to exploit databases.

Solutions will be researched in order to counteract the vulnerability of people responding to social engineering exploits. Currently, methods involving training and policy enforcement are being emphasized, but other more creative approaches will also be considered.

Accomplishments

Social engineering case studies are currently being documented and a database of these cases has been started. The case studies are being analyzed for common trends and distinguishing characteristics which will help inform solutions.

Future Plans

Future research will include a continued effort to document and study social engineering cases. Noting what worked or didn't work and determining the factors involved will yield valuable insight into the problem. Solutions in the form of training, policy or other means will be formulated. These strategies will then be tested both in the field with clients in actual work environments and in a series of experiments in a controlled environment. The exact nature of the solution implementation is still being determined.

The ultimate goal of this research will be to gain a better understanding of this minimally researched topic so that workable solutions can be developed and the risk from social engineering can be reduced in a more systematic manner.