Technological Con-Artistry

PIs: Kevin F. Steinmetz and Richard Goe

Kansas State University

Overview

Social engineering is often lauded as one of the most significant threats to information security yet little academic attention has been given to the phenomenon. The objective of this project is to develop a deeper understanding of (1) the motivations and characteristics of social engineers; (2) the process by which social engineering is accomplished; and (3) the nature of the threat and strategies used to combat it by personnel involved in IT security.

Scientific Impact:

This study will:

- Be one of the first criminological studies of social engineering;
- Provide an understanding of the role of group dynamics in the creation and implementation of social engineering strategies;
- Develop a criminological theory of social engineering.

Broader Impact:

- Social engineering potentially poses a threat to anyone requiring IT security;
- Will provide a clearer picture of the real threat social engineering poses to IT security;
- Can inform the policies of government and business organizations regarding information security;
- Will produce findings that will be used to educate and inform students of criminology.

Figure 1: Snowball Sampling – Social Engineers and Security Auditors

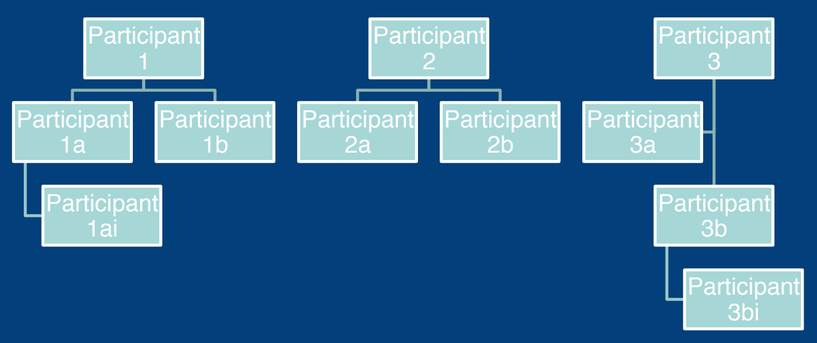
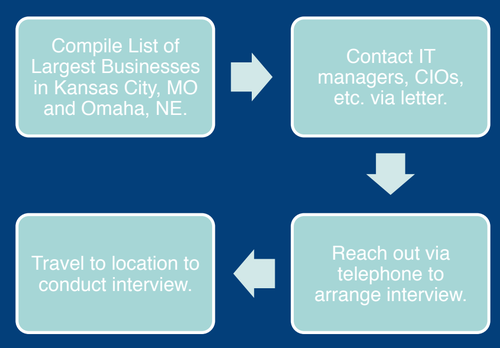


Figure 2: Sampling – IT Professionals



Approach

- A non-experimental, cross sectional research design will be used that employs a multi-methodological approach for data collection.
- Personal interviews will be used to collect both qualitative and quantitative data.
- Qualitative data will be analyzed using a grounded theory-based approach. Quantitative data will be analyzed through univariate, bivariate, and multivariate statistical methods.
- Interviews will be conducted with subjects drawn from three populations involved in the perpetration and prevention of social engineering: social engineers "in the wild," information security auditors, and IT professionals in charge of managing organizational data security.
- Figures 1 and 2 illustrate the sampling approach for the three populations under examination.

Table 1: Demographic Characteristics to Date (n = 10)

Age	$\bar{x}$ = 37.4		**Education**	High School Diploma/GED	10%
				Some College	20%
Race	White	80%		Associate's Degree	20%
	Asian	10%		Bachelor's Degree	30%
	Biracial	10%		Master's Degree	20%
Gender	Male	6%	**Self-Described SES**	Lower/Working	20%
	Female	4%		Lower-Middle	10%
				Middle	60%
Occupation	Information Technology	10%		Upper-Middle	10%
	Information Security	80%			
	Security Auditors*	87.5%	**Marital Status**	Married	70%
	Customer Relations	10%		Not Married	20%
				Quasi-Married	10%

*% of participants working in information security who work specifically as security auditors/penetration testers.

Defining Social Engineering

- Initial results indicate that multiple definitions for social engineering exist. Most orient around influencing or manipulating the behavior of others. Definitions indicate that social engineering, however, is a phenomenon that may not warrant being sensationalized and can be thought of as a form of con-artistry applied to the context of information security.

Social Engineering Pathways

- Tentative findings suggest multiple pathways into social engineering and information security.
- Examples:
  - Begins as interest and evolves into hobby.
  - Transition from (recreational) criminal enterprise to licit profession.
  - Initial interest stemmed from training in social/behavioral sciences.

Gathering Further Interviews

- Recruit participants at hacker/security conventions (ex: DEF CON, DerbyCon, Shmoocon).
- Use prior participants to connect to other possible interviewees.
- Contact heads of IT and CIOs for major companies in two large Midwestern cities. These organizations will be from information-intensive industries.

Putting the "Social" in "Social Engineering

- Despite the stereotype of hackers and other technologists being socially incompetent or averse, the interviews so far indicate that social engineers fail to conform to this stereotype.
  - Participants indicated that social skills were central to the enterprise. Beyond a perhaps obvious attunement to psychological biases, some participants indicated that the most successful social engineers articulated that a genuine sensitivity to the expectations and emotions of others was necessary. In other words, the best social engineers do more than go through rote procedures to influence or manipulate others; they are capable empathizing and relating to others.
  - Interviewees, particularly security auditors, indicated that they have participated in social engineering projects as members of a team. These projects involve a division of labor and a degree of trust in their compatriots.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

University #1 Logo
University #2 Logo