Social Engineering: A Serious Underestimated Problem

Guido Rößling
roessling@acm.org

Marius Müller
mueller.marius@mac.com

Department of Computer Science
Technische Universität Darmstadt
64289 Darmstadt, Germany

ABSTRACT

We describe two experiments to get security-relevant data using Social Engineering. The success of the experiments is disturbing.

Categories and Subject Descriptors

K.4.2 [**Computers and Society**]: Social Issues—*Abuse and crime involving computers*

General Terms

Security, Human Factors

Keywords

Social Engineering

1. SOCIAL ENGINEERING

Wikipedia defines *Social Engineering* as "the act of manipulating people into performing actions or divulging confidential information." We examined the use of Social Engineering to access critical data within the firm of the second author. The security manager and a supervisor were informed about the study and approved it, provided that no actual details were publicized. The "targets" of the Social Engineering were unaware about the experiment, to better allow judging the chances of receiving access to criticial data.

We conducted two experiments. In the first experiment, we tried to get the login information for randomly chosen members of the firm. The second experiment tried to get access to the firm's mail server from one of the administrators. Both experiments were conducted by phone calls from an office inside the firm, but with a suppressed phone number. The supervisor and the security officer were present and listening in to the phone calls. In this way, they received a better impression of how difficult—or not—it was to get the relevant information, and could ensure that the information could not leave the room.

In the first experiment, a random selection of workers was called. The caller claimed to be from the firm's help desk. Only one person noticed that no phone number was transmitted. We used different pretexts, such as necessary patches or the need to verify that the user did not have installed games. 3 of our 6 phone calls were successful, yielding the computer name with user login and password over the phone. Only one of the workers was concerned enough that he wanted to mention the call to other colleagues.

ITiCSE'09, July 6–8, 2009, Paris, France.
ACM 978-1-60558-381-5/09/07.

We then tried to get access to the firm's mail server by calling two administrators. Such access can have wide-reaching consequences, for example in the area of industrial espionage. In the first experiment, the caller acted as a fictitious member of the firm. In this second experiment, the caller assumed the identity of an actual member of the firm, complete with name and affiliation, that he assumed the administrators would know by name but not personally. The attacks were also far more precisely directed: we used XING to locate the target persons (listed as "administrators" inside XING). We then used XING to research the network of persons that the target persons was connected to and thus knew. This approach provided a plethora of information within a short amount of time; other services such as Facebook provided additional information including family photos. This information can usually be researched anonymously or with a fake ID, thus leaving no trace of the real attacker. Free WLAN hotspots can further muddle the trace of the intruder, making it almost impossible to pinpoint the culprit.

The caller presented himself as a member of the IT services. He mentioned several colleagues and supervisors in an appropriate position. He also incorporated some of the researched additional information, such as the "conincidence" of having studied at the same university. This information was interwoven in the phone call and only mentioned in passing, but eagerly taken up by the administrator. At the end of the call, the first person was very close to providing the password, but did not want to do so over a phone line. The second phone call to another administrator was successful.

It is very disturbing that it was so easy to get the requested information. In both cases, 50% of our attempts succeeded, including a login to a manager's computer and access to the firm's mail server. The second "targeted" attack required only a few hours of preparation—all necessary information for acting plausibly and with a solid background in the institution is freely available on XING and other social networks.

We believe that is highly important that students, educators and end users in firms know about Social Engineering. Only two things really help against Social Engineering: *awareness* and *vigilance*. Users need to know about Social Engineering, how it works, and be on alert when "strange" phone calls or emails occur. Only one of our eight "targets" noticed that no phone number was transmitted, although the caller claimed to call from inside the firm. Such information should be passed along to CS students repeatedly.

Educators should also stress the risks of publishing too much personal or professional information and links to colleagues in XING and related platforms. Our experiments have shown how easy it is to act as a concrete person and get the requested information. Due to possible legal consequences, we did not try to get password information and other relevant information from other firms, but assume that would have found it similarly easy to reach our goals.