HATCH: Hack And Trick Capricious Humans
A Serious Game on Social Engineering

Kristian Beckers and Sebastian Pape and Veronika Fries

Technische Universität München
Goethe University Frankfurt

Technische Universität München

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

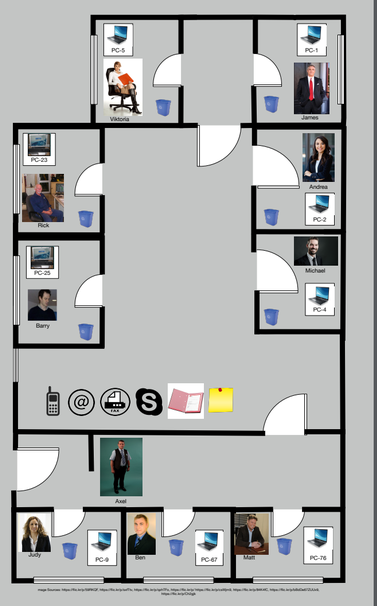
Objectives

A serious game on social engineering which aims to:

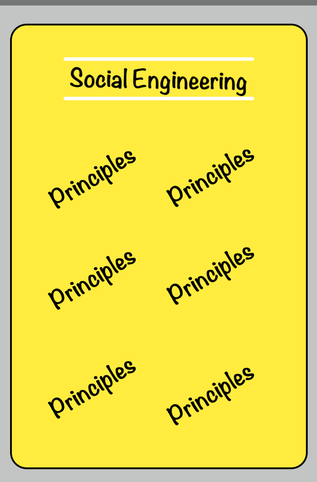
- Train the players on social engineering techniques
- Identify possible weaknesses to social engineering

Preparation

1. Present an *overview diagram* of the company that shall play the game. This diagram has to include the physical architecture of the company, the people working in that company and their locations, as well as communication channels e.g. VoIP, Email, etc. Finally the diagram has to show vital assets of the company, e.g., valuable information on a computer system. All players check the diagram for completeness and as a natural consequence should be familiar with it at the beginning of the game.

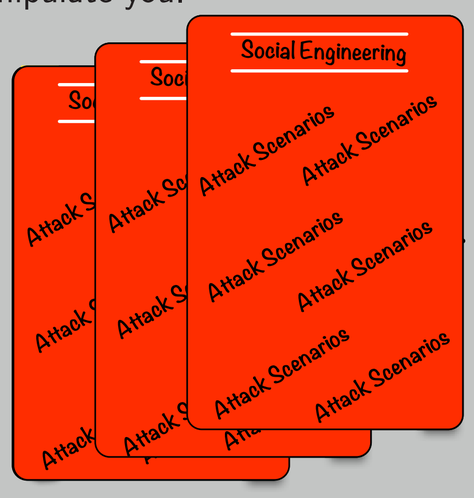


Draw Cards



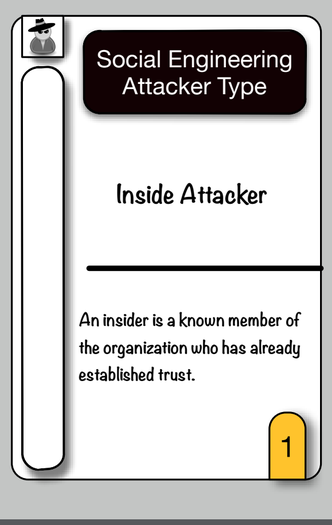
2. Each player draws 1 card from the set of *human behavioural patterns*.

   The card deck contains the human behavioural patterns, e.g. the so-called *Need and Greed principle* that states "Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you."



3. Each player draws 3 cards from the set of *attack techniques*.

   The card deck contains attack techniques, e.g. the technique of reverse social engineering that comprises creating a problem for the selected person and solving it. The gained trust is used to ask the victim for a favour.



4. Each player gets 1 *attacker type* card.

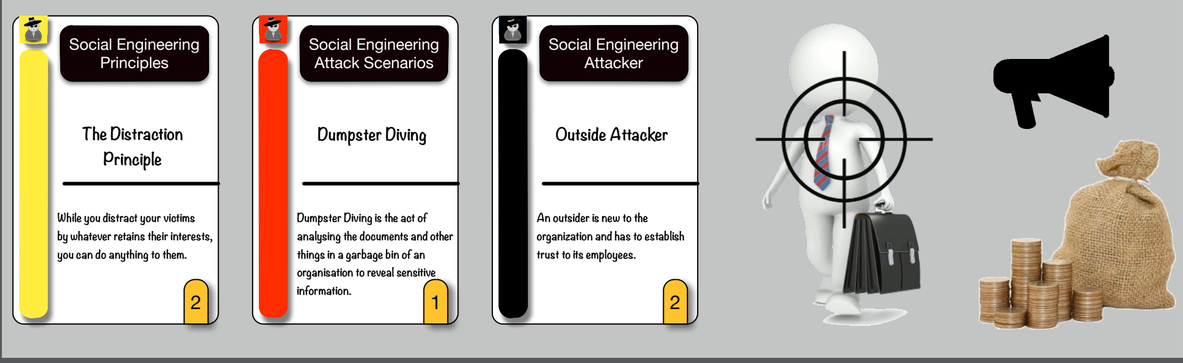
   The card has two sides. One for an inside attacker that is a well known member of the organisation and has established trust. Another one for an outside attacker that is unknown to the members of the organisation and that has to establish trust.

Brainstorming Phase

5. The players take the role of the attacker. Each player thinks of how to apply the exploit of the behavioural pattern in combination with one of the three attacks on one of the persons in the overview diagram to attack an asset. Moreover, the player has to choose if she is an insider or outsider of the organisation.
   The players get **5 minutes** to think about their attacks.

Attack Phase

6. The active player presents his attack to the group. Each attack consists of a principle, an attack scenario, an attacker, a victim, a communication channel and a targeted asset. Note that after a player has proposed an attack it is finalised and cannot be changed anymore by the player.



Discussion

7. In this round the other players discuss if the proposed attack is feasible and bring arguments why this could be unrealistic. All attacks have to be documented. If the proposed attack is not plausible the turn ends immediately. Finally, the other players have to make the choice on how many points are granted. In addition, the other players can also propose improved versions of an attack and gain points.

Points

The following points can be gained per round:

Attack **2 P.** feasible | **1 P.** feasible with help
1 P. plausible but infeasible | **0 P.** non plausible → end turn
Attacker **2 P.** outside attacker | **1 P.** inside attacker
Principle **2 P.** perfect match | **1 P.** somewhat match | **0 P.** no match
Scenario **1 P.** match | **0 P.** no match
Attack Improvement by other Players
2 P. major improvement | **1 P.** minor improvement

Iterate (Phases 2 – 7)

8. The next player proposes an attack in the same fashion explained above. This iterates until all persons iterated at least twice. After each round, the players restock their cards. The Brainstorming Phase may be shortened by the players.

Debriefing

9. We propose the following steps for a structured threat elicitation:
   - ▷ Identify the most relevant targets of social engineers in your organisation
   - ▷ Try to figure out why some people were attacked more often and others not at all
   - ▷ Analyse why some communication channels were used more often than others
   - ▷ Determine which assets were attacked more often than others

Supported by:

Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie

Federal Ministry of Education and Research

{kristian.beckers,veronika.fries}@tum.de

sebastian.pape@m-chair.de