Psychological Profiling for Social Engineering

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

DeepIntel 2013
Oberaichwald, AT



About me

- President of the Magdeburg Institute for Security Research
- Editor of the Magdeburger Journal of Security Research
- Freelance Security Consultant
- Hacker for 20 years, ex-NetBSD developer
- Educational Science and Psychology, Research on Social Engineering
- Focus on Social Engineering, Security Awareness, Organizational Security



Inhaltsverzeichnis

1 Intro

2 Profiling

3 Communication

4 Personnel Psychology (IO)



Social Engineering

- use/abuse human behaviour to reach goals
- hacking people
- Why should I crack `/etc/master.passwd` if I only have to ask a user for his password?
- social engineering is based on human behaviour $\rightsquigarrow$ psychology, sociology, educational science
- Profile enhances success of Social Engineering



Example for Social Engineering

- sophisticated attack on high ranking manager
- identify former class mates including the former class representative
- create fake IDs of former class representative in social networks
- set up fake website about favourite football club owned by former class representative
- contact victim via social network (do you remember me? former class representative, X is now living in Y, fans of the same club, set up a website, photos from the last training ...)
- manager creates account on website using his standard password ...



Psychology

- empirical and theoretical science
- describes and explains human behaviour and experiences
- human development and the internal and external causes and conditions
- Differential and Personality P., Social P., Industrial P., Organisational P.
- also: Industrial and Organisational Sociology, Organisational Development



Inhaltsverzeichnis

1 Intro

2 Profiling

3 Communication

4 Personnel Psychology (IO)



History of Profiling

- scientific, empirical, forget TV series
- Galen of Pergamon: bodily fluids - blood, yellow bile, black bile, and phlegm
- Temperaments: sanguine (pleasure-seeking and sociable), choleric (ambitious and leader-like), melancholic (analytical and thoughtful), and phlegmatic (relaxed and quiet)



History of Profiling

- C.G. Jung: archetypes-as-such and archetypal images figures like Mother, Father, Child, Wise Old Man, Hero
- Alfred Adler: inferiority complex
- Erik H. Erikson: stages of psychosocial development
- they are not empirical sound!
- tests have to be reliable, objective and valid
- personality traits do not predict how someone behaves in every situation
- rather stable, useful on strategic level



Big 5

- empirical lexical analysis in the 1930s by Thurstone, Allport and Odbert
- counting adjectives describing personality in dictionaries (cf. corpus linguistics)
- factor analysis in the 1960s found 5 stable factors
- Neuroticism, Extraversion, Openness, Conscientiousness, Agreeableness



Big 5

- Neuroticism – (sensitive/nervous vs. secure/confident). The tendency to experience unpleasant emotions easily, such as anger, anxiety, depression, or vulnerability. Neuroticism also refers to the degree of emotional stability and impulse control, and is sometimes referred by its low pole – »emotional stability«.
- Extraversion – (outgoing/energetic vs. solitary/reserved). Energy, positive emotions, surgency, assertiveness, sociability and the tendency to seek stimulation in the company of others, and talkativeness.
- Conscientiousness – (efficient/organized vs. easy-going/careless) A tendency to show self-discipline, act dutifully, and aim for achievement; planned rather than spontaneous behavior; organized, and dependable.



Big 5

- Openness to experience – (inventive/curious vs. consistent/cautious) Appreciation for art, emotion, adventure, unusual ideas, curiosity, and variety of experience, intellectual curiosity, creativity and a preference for novelty and variety a person has; imaginative or independent, personal preference for a variety of activities over a strict routine
- Agreeableness – (friendly/compassionate vs. cold/unkind) compassionate, cooperative rather than suspicious, antagonistic, measure of ones' trusting and helpful nature, and whether a person is generally well tempered or not.



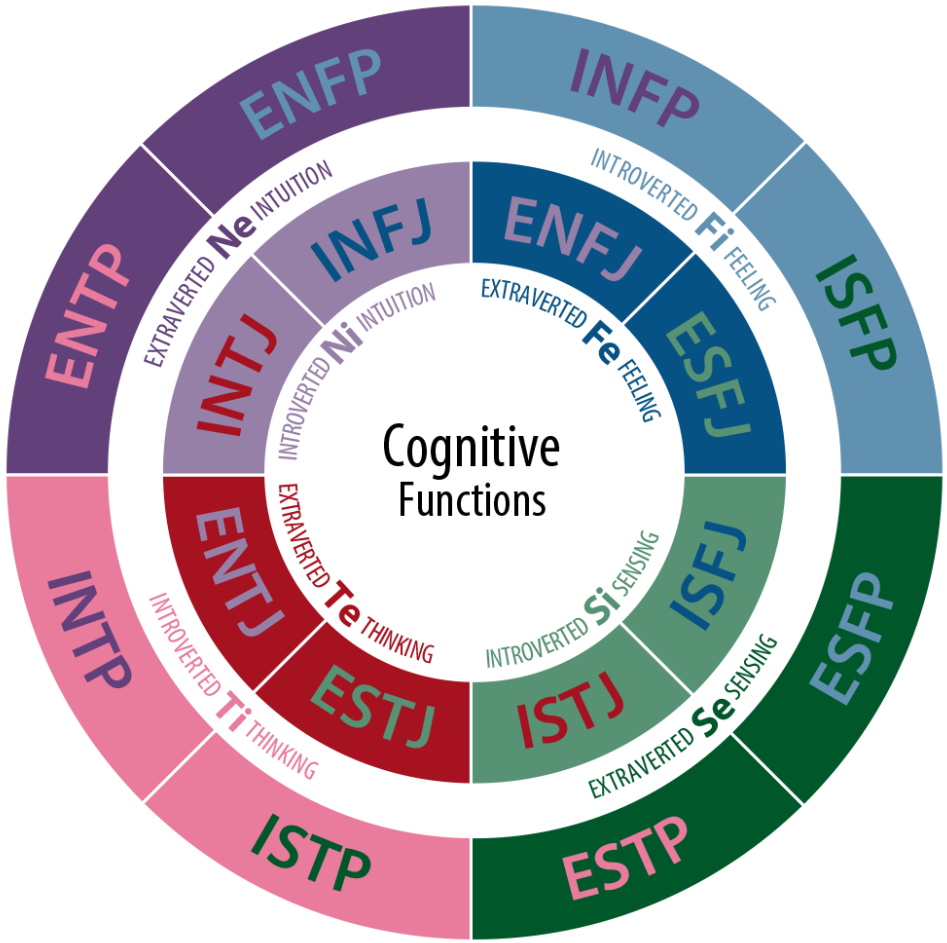
Myers-Briggs Type Indicator

- measure psychological preferences in how people perceive the world and make decisions
- based on C.G. Jung: Psychologische Typen (1921)
- judging function (thinking or feeling) or their perceiving function (sensing or intuition)
- 4 dichotomies:

Extraversion (E)	(I) Introversion
Sensing (S)	(N) Intuition
Thinking (T)	(F) Feeling
Judging (J)	(P) Perception



Myers-Briggs Type Indicator



Jungian Type Index

- introduced by Optimas in 2001, developed in the 1990s in Norway
- enhancement of MBTI, better translatable
- replaced MBTI in the nordic countries



Attachment theory

- John Bowlby, James Robertson, Mary Ainsworth (1940-1970s)
- describes the dynamics of long-term relationships between humans
- developmental psychology, research done on babies/infants
- 4 types identified
- can also describe attachment in adult relations
- used by Romeo-Agents of the MfS



Attachment theory

- Secure attachment
  easy to become emotionally close to others, comfortable depending on others and having others depend on me, don't worry about being alone or having others not accept me



Attachment theory

- Anxious–preoccupied attachment
  I want to be completely emotionally intimate with others, but I often find that others are reluctant to get as close as I would like. I am uncomfortable being without close relationships, but I sometimes worry that others don't value me as much as I value them.
  Seek high levels of intimacy, approval, and responsiveness from their partners, value intimacy to such an extent that they become overly dependent on their partners



Attachment theory

- Fearful–avoidant attachment
  I am somewhat uncomfortable getting close to others. I want emotionally close relationships, but I find it difficult to trust others completely, or to depend on them. I sometimes worry that I will be hurt if I allow myself to become too close to others.
  People with this attachment style have mixed feelings about close relationships. On the one hand, they desire to have emotionally close relationships. On the other hand, they tend to feel uncomfortable with emotional closeness



Attachment theory

- Dismissive–avoidant attachment
  I am comfortable without close emotional relationships, It is very important to me to feel independent and self-sufficient, I prefer not to depend on others or have others depend on me.
  desire a high level of independence, attempt to avoid attachment altogether, view themselves as self-sufficient and invulnerable to feelings associated with being closely attached to others



Inhaltsverzeichnis

1 Intro

2 Profiling

3 Communication

4 Personnel Psychology (IO)



Paul Watzlawick

- *1921 in Villach/Carinthia
- 5 axioms of communciation
  - One Cannot Not Communicate
  - Every communication has a content and relationship aspect such that the latter classifies the former and is therefore a metacommunication
- Pragmatics of Human Communication Hardcover (1969) by Watzlawick/Beavin/Jackson

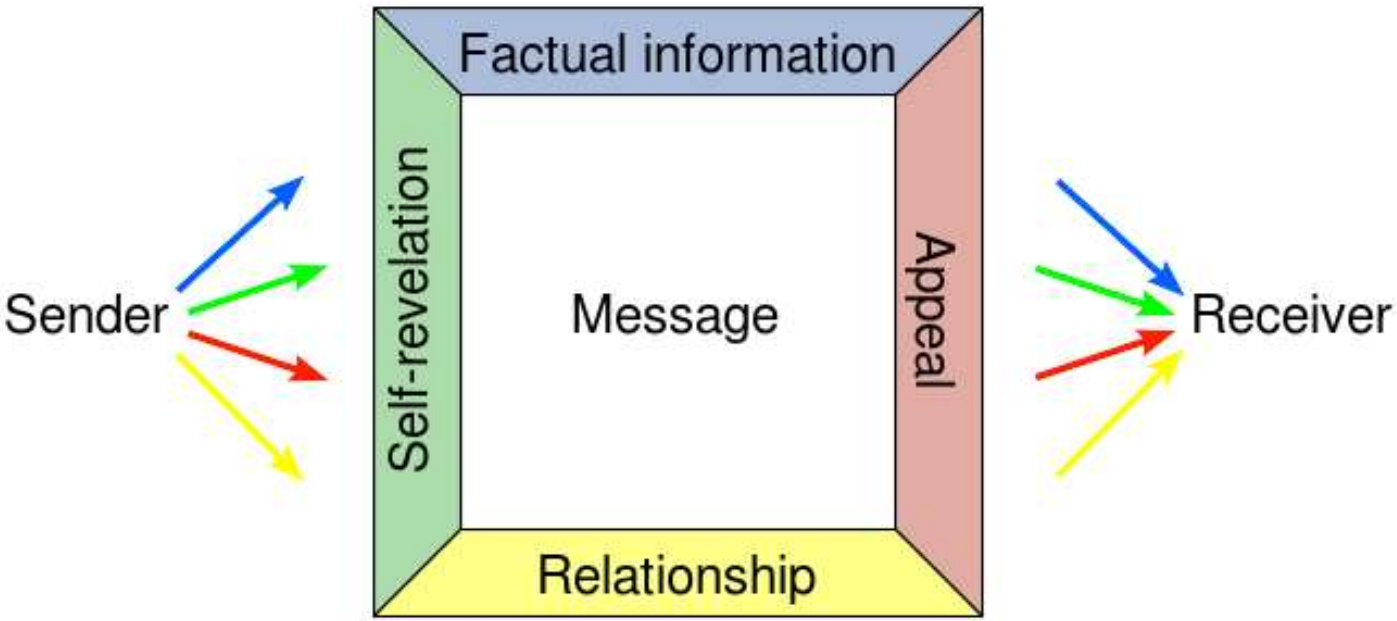


Friedemann Schulz von Thun

- Prof. em. of Psychology in Hamburg
- developed the 4-sides-model (»4 ears and 4 beaks«)
- bunch of books (Miteinander reden etc.)
- every message has four facets



Friedemann Schulz von Thun



Friedemann Schulz von Thun

facts matter of fact like data and facts, which are part of the news

self-revealing conscious or not intended - tells something about himself, his motives, values, emotions etc.

relationship how the sender gets along with the receiver and what he thinks of him.

appeal contains the desire, advice, instruction and effects that the speaker is seeking for



Friedemann Schulz von Thun

A man (first sender of the news) and a woman (first receiver of the message) are eating a homecooked meal together.
The man says: »There is something green in the soup.«

- Factual layer: There is something green.
- Self-revealing layer: I don't know what it is.
- Relationship layer: You should know what it is.
- Appeal layer: Tell me what it is!



Friedemann Schulz von Thun

The man says: »There is something green in the soup.«
The woman hears:

- Factual layer: There is something green.
- Self-revealing layer: You do not know what the green item is, and that makes you feel uncomfortable.
- Relationship layer: You think my cooking is questionable.
- Appeal layer: I should only cook what you know in the future!

The woman answers: »If you don't like the taste, you can cook it yourself.«



Friedemann Schulz von Thun

The man says: »There is something green in the soup.«
The woman hears:

- Factual layer: There is something green.
- Self-revealing layer: You do not know what the green item is, and that makes you feel uncomfortable.
- Relationship layer: You think my cooking is questionable.
- Appeal layer: I should only cook what you know in the future!

The woman answers: »If you don't like the taste, you can cook it yourself.«



Transactional Analysis (ta)

- Eric Berne: Games People Play: The Psychology of Human Relationships
- theory of personality AND of communication
- post-Freudian, ex-Freudian, focus on Transactions



Transactional Analysis (ta)

key ideas

Structural analysis analysis of the individual psyche

Transactional analysis proper analysis of interpersonal transactions based on structural analysis of the individual's involved in the transaction

Game analysis repeating sequences of transactions that lead to a predetermined outcome subconsciously agreed to by the parties involved in the game

Script analysis a lifeplan that may involve long term involvement in particular games in order to reach the life pay-off of the individual



Transactional Analysis (ta)

ego states

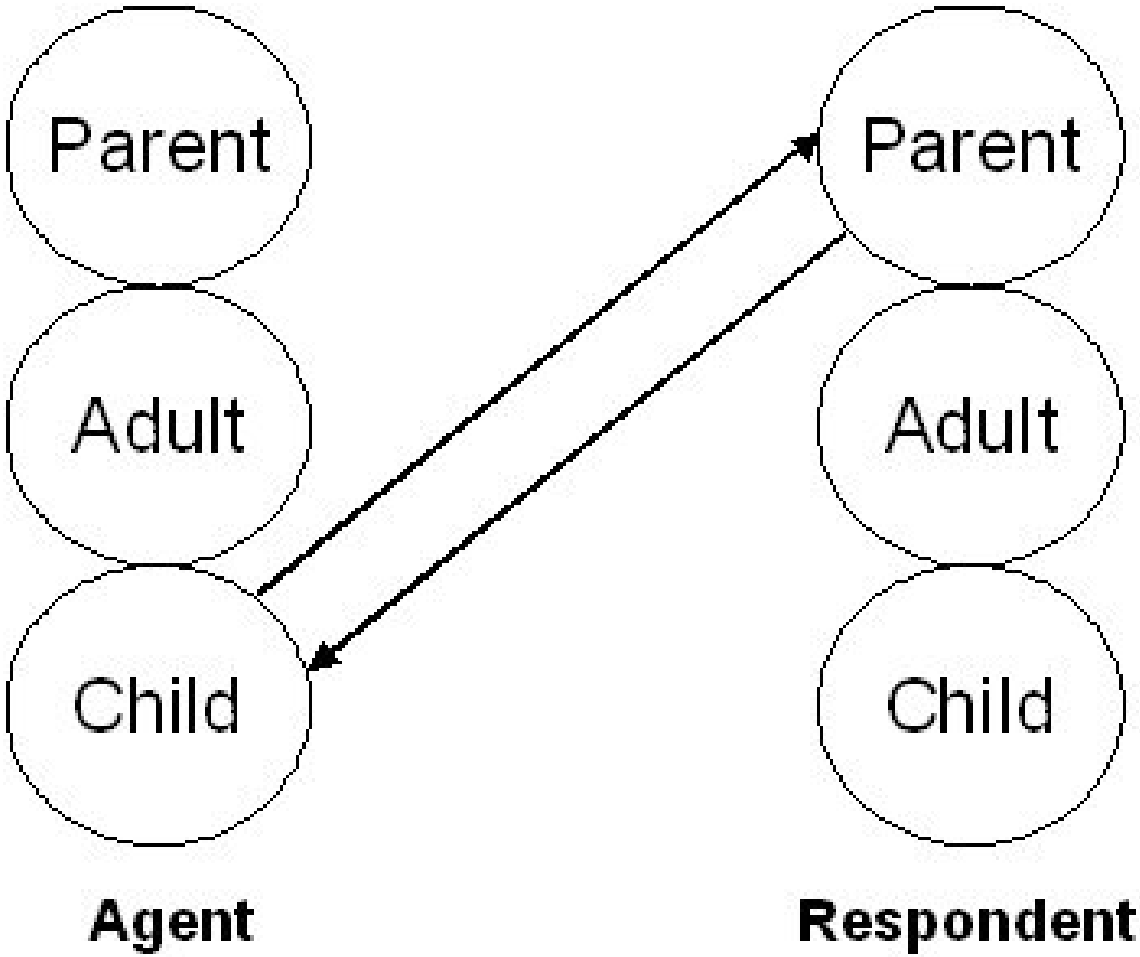
Parent (exteropsyche) behave, feel and think in response to an unconscious mimicking of how their parents acted, or how they interpreted their parent's actions.

Adult (neopsyche) like a computer processing information and making predictions absent of major emotions that could affect its operation, directed towards an objective appraisal of reality.

Child (archaeopsyche) behave, feel and think similarly to how they did in childhood, source of emotions, creation, recreation, spontaneity and intimacy.



Transactional Analysis (ta)



Inhaltsverzeichnis

1 Intro

2 Profiling

3 Communication

4 Personnel Psychology (IO)



Organisations

- Organisations have a culture
- personnel is selected to fit into that culture
- job advertisement describe how the organisation *sees* itself
- which is not necessarily true (flat hierachy?)
- assessment center select potential employees based on their personality
- attend an AC?



Personnel Psychology

- Industrial Psychology offers a lot of methods for diagnostics
- Assessment Center, IQ tests, personnality tests
- Organisational Psychology and Sociology analyse Organisations
- esp. their culture of hierarchy and learning
- What happens when employees make mistakes? Are they punished? Are they afraid of being punished?



Coda

- profiling can enhance social engineering attacks
- expensive and time consuming
- should be done by psychologist with scientific methods
- needs training and practice
- cannot be learnt from a book
- ethical? can seriously fuck up people!



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- youtube.de/Sicherheitsforschung
- http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

