SEPF
The Social Engineering Personality Framework

predict
prioritise
prevent
TRESPASS

Sven Übelacker
Security in Distributed Applications
Hamburg University of Technology

2015-01-12
Usability Colloquium, TU Berlin

SEVENTH FRAMEWORK PROGRAMME

TUHH
Technische Universität Hamburg-Harburg

European Commission

Our background

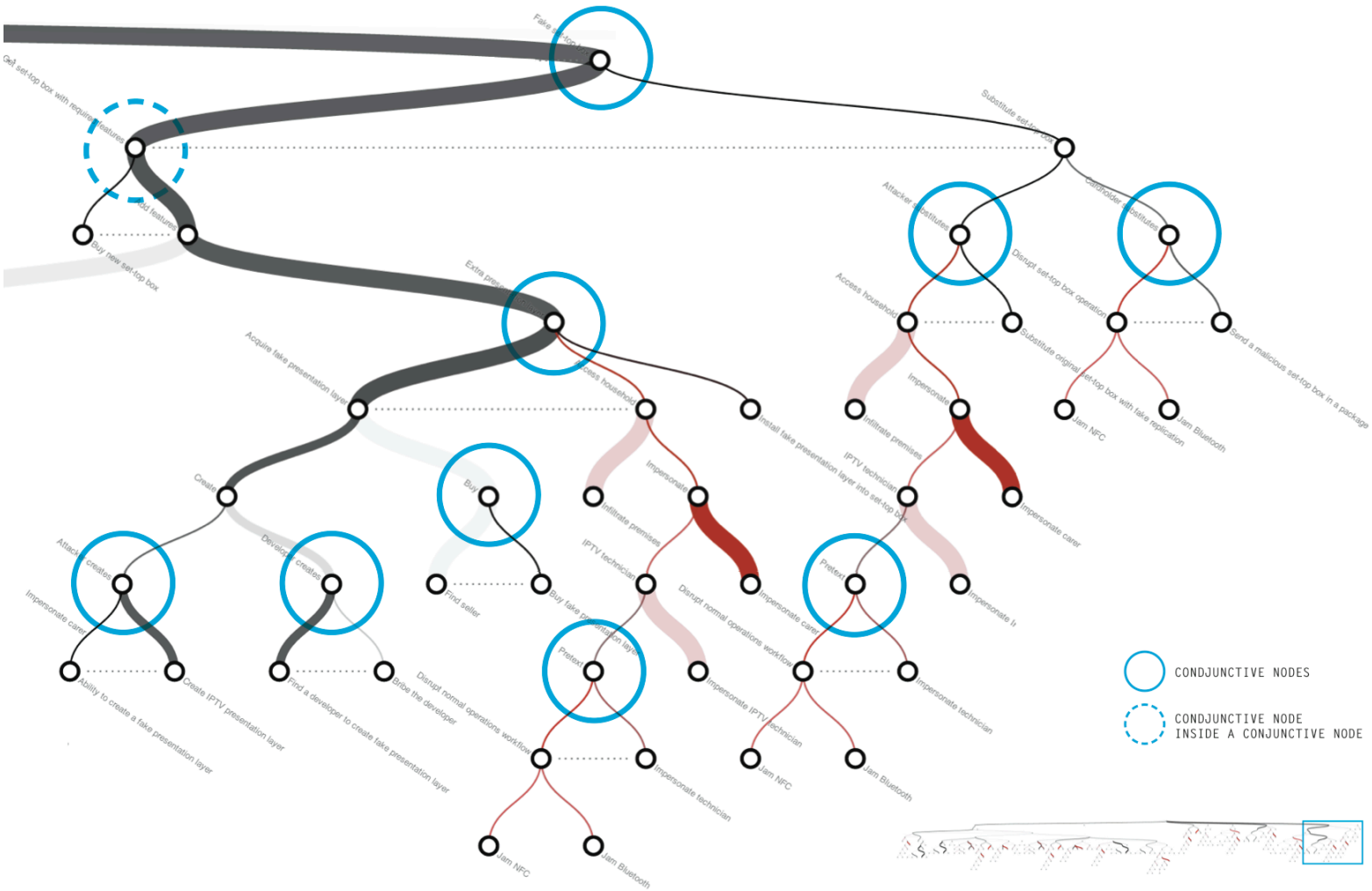
Sven Übelacker

- degree in mathematical economics, focus on actuarial science and information security
- ten years of experience in academic computer centres, focus on information security and data protection; four of them at DFN-CERT (CSIRT and PKI of Germany's national research and education network)
- since March 2013: Security in Distributed Applications (Dieter Gollmann), Hamburg University of Technology, contributing to FP7 funded EU project TRESPASS

about TRESPASS

- EU funded FP7 integrated project (2012--2016)
- covering three security domains
  - technical/physical, digital, and social/organisational
- grounded on three case studies
  - cloud computing, telco, and customer privacy protection
- to develop methods and tools to analyse and visualise information security risks in dynamic organisations, as well as possible countermeasures
- to build "attack navigators" to identify which attack opportunities are possible and most pressing, and which countermeasures are most effective

One of Many Attack Tree Visualisations



LUST's visualisation of an ATree displaying different attribute domains in TRESPASS D4.2.1 [23] (cf. ADTool by University of Luxembourg [14])

Outline

attacker (social engineer) $\leftarrow$ SE $\rightarrow$ "victim" (social target)

- e.g. attacker profiles (via expert knowledge / questionnaires)
- social engineering (SE) techniques
- e.g. "victim" profiling

1st approach: Social Engineering Personality Framework

- susceptibility to specific SE attacks mapped to personality traits of a "victim" (employee)
- with Susanne Quiel

2nd step: find influential factors
3rd step: questionnaire

- incorporating SE scenarios and other factors

What is Social Engineering (SE)?

Hadnagy's definition [10]

"the act of manipulating a person to take an action that may or may not be in the target's best interest. This may include obtaining information, gaining access, or getting the target to take certain action."

- Social Engineering is nothing new
  - Adam Smith's theory of human behaviour in "The Theory of Moral Sentiments", 1759: passions and the impartial spectator (loss aversion, overconfidence, altruism, …) [1]
- Kevin Mitnick was the first widely known to use SE for gaining access to the digital security domain [16]
- HUMINT: "a category of intelligence derived from information collected and provided by human sources." (NATO NSA) [17]

Social Engineering (SE)

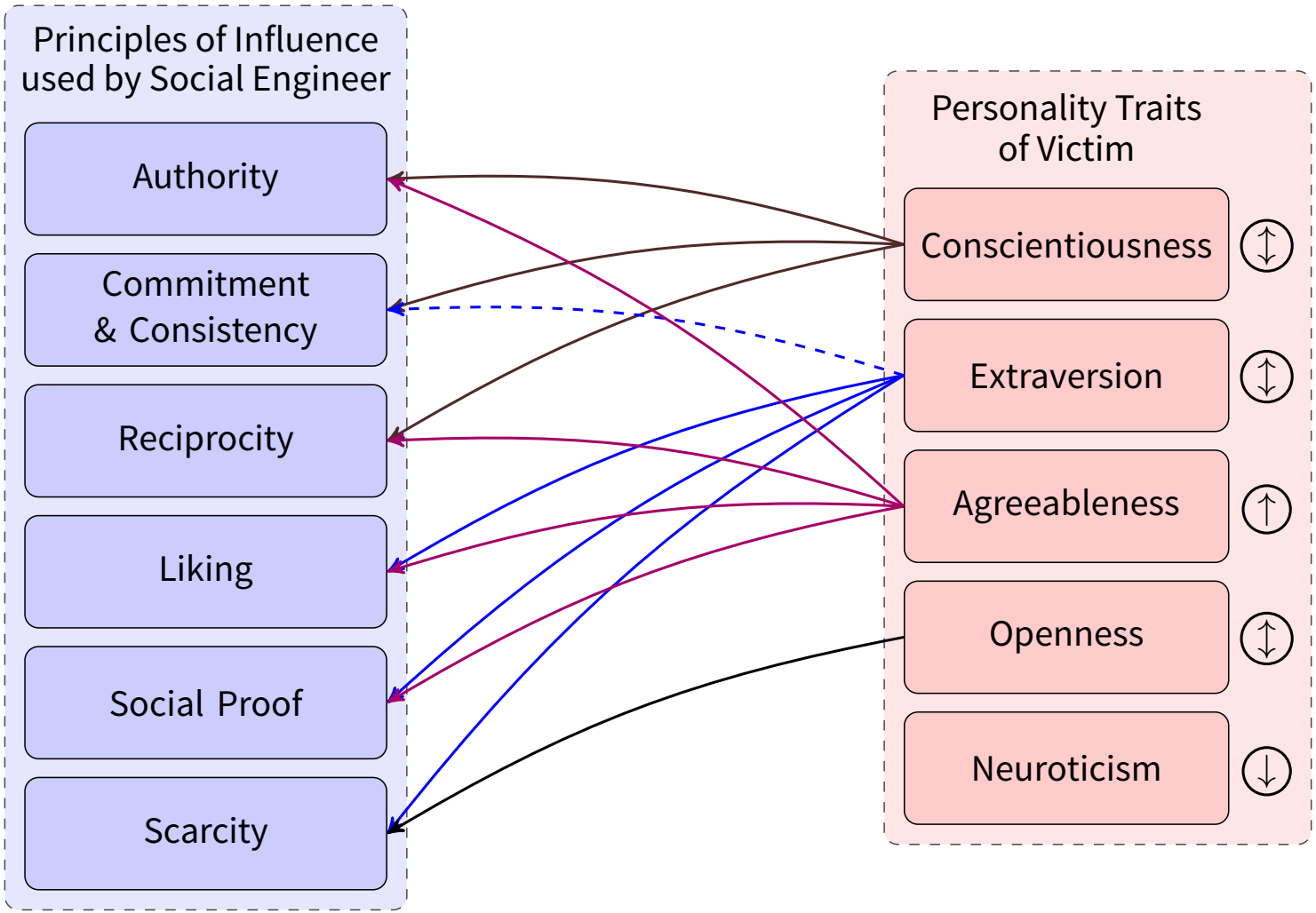
Categorisation of Social Engineering Attacks

- Gragg's Psychological Triggers of SE [8]
- re-use of Cialdini's Six Principles of Influence [4]
  - *Authority*, Reciprocity, Commitment and Consistency, Social Proof, Liking, Scarcity
  - Scheeres [20] mapped Gragg's trigger to these principles
- Stajano/Wilson's seven principles for understanding scam victims [22] (cf. "The Real Hustle")

Why Do People Succumb to SE Attacks?

- socio-demographics [5]
- knowledge (awareness) of SE attacks / attacker's intentions [6]
- personality traits [18]
- stressors
- impulsiveness
- freedom of action
- proficiency/affinity towards technology/internet
- cultural background (e.g. uncertainty avoidance) [12]
- evolutionary flaws in risk perception and assessment [21]
- human information processing
  - peripheral/heuristic vs. central route processing [13]
  - Dual Process Model of Persuasion [9]

Social Engineering Personality Framework



SEPF: Specific personality traits of a "victim" increase (solid line) or decrease (dashed line) the susceptibility to Cialdini's principles of influence which are used for attacks by a social engineer. General personality assumptions about susceptibility (higher, lower, or both) for each trait are depicted by corresponding arrows (↑, ↓, ↕).

Personality Traits

Five-Factor Model (FFM) or the "Big 5" [15]

- five empirically derived personality dimensions **O**penness to Experience, **C**onscientiousness, **E**xtraversion, **A**greeableness, and **N**euroticism
- model widely used in psychology since the 1950's [15]
- consists of subtraits (**s**) which refine each trait further
- questionnaires exist, e.g. NEO-FFI, TIPI [7]
- gathering trait information via user behaviour, e.g. shown with Nokia N95 smartphones [3]

Motivational System (m)

- Hirsh et al. describe what individuals motivate depending on their FFM personality traits [11]

FFM (s)ubtraits & (m)otivational system

Conscientiousness

(s) competence, self-discipline, self-control, persistence, dutifulness, following standards/rules

(m) *achievement, order, efficiency*

Extraversion

(s) positive emotions, sociability, dominance, ambitions, excitement seeking

(m) *reward, social attention*

SEPF Agenda

1. our approach based on comprehensive literature review [19]
2. our more specific suggestions on how to map personality traits to the principles of influence [19]
3. preliminary coping strategies [24]
4. gathering empiric data via online questionnaires incl. feasible SE scenarios [2] per personality trait, SE attack, and domain
5. designing coping strategies against these specific SE scenarios

SEPF: Example Attack Scenarios & Coping Strategies [24]

attack scenario for **extraverted** "victims" **E**

"A social engineer attends a social event on a conference in order to attack an extroverted individual to reveal sensitive information. To receive social attention and become a member of a social group the employee gives in and acts against official company policies."

coping strategy for **extraverted** "victims" **E**

"Rewards for achieved awareness trainings, for instance showing success rate in awareness learning system on company's internal social network (visible to all employees). Establish a system where employees suggest improvements for security policies and procedures -- number of submitted suggestions per employee will be displayed on internal social networking site."

Outlook

- refined SEPF relations need empiric ground
- empiric research is on the way
  - via scenario-based questionnaires derived from SE attacks and not personality traits
  - enhanced by other influential factors to shed light on this topic more holistically

Thank you! Questions?

Contact

Sven Übelacker <uebelacker@tuhh.de>
Security in Distributed Applications
Hamburg University of Technology, Germany
https://www.sva.tuhh.de/

Acknowledgement

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRE$_S$PASS). This publication reflects only the author's view and the European Union is not liable for any use that may be made of the information contained herein.

Literature I

Nava Ashraf, Colin F Camerer, and George Loewenstein.

Adam Smith, Behavioral Economist.
Journal of Economic Perspectives, pages 131--145, 2005.
`http://authors.library.caltech.edu/21998/2/08953300577435789 7%5B1%5D.pdf`.

John M Carroll.

Five Reasons for Scenario-Based Design.
In *HICSS'99: Proceedings of the Thirty-Second Annual Hawaii International Conference on System Sciences, 3*, volume 3051, 1999.

Gokul Chittaranjan, Jan Blom, and Daniel Gatica-Perez.

Mining Large-Scale Smartphone Data for Personality Studies.
Personal and Ubiquitous Computing, 17(3):433--450, 2013.

Robert B. Cialdini.

Influence: The Psychology of Persuasion.
HarperCollins, 2007.

A. Darwish, A.E. Zarka, and F. Aloul.

Towards Understanding Phishing Victims' Profile.
In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on*, page 1–5, 2012.

M. Friestad and P. Wright.

The Persuasion Knowledge Model: How People Cope with Persuasion Attempts.
Journal of consumer research, page 1–31, 1994.

Samuel D Gosling, Peter J Rentfrow, and William B Swann Jr.

A very brief measure of the big-five personality domains.
Journal of Research in personality, 37(6):504--528, 2003.

Literature II

David Gragg.

A Multi-Level Defense against Social Engineering.
SANS Reading Room, 13, 12 2002.
`https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920`.

R. Guadagno and R. B. Cialdini.

Online Persuasion and Compliance: Social Influence on the Internet and Beyond.
The Social Net: Human Behavior in Cyberspace, pages 91--113, 2005.

C. Hadnagy.

Social Engineering: The Art of Human Hacking.
Wiley, 2010.

J. B. Hirsh, S. K. Kang, and G. V. Bodenhausen.

Personalized Persuasion Tailoring Persuasive Appeals to Recipients' Personality Traits.
Psychological Science, 23(6):578--581, 2012.

Hofstede Center.

National Cultural Dimensions.
2014.
`http://geert-hofstede.com/national-culture.html` last visited on April 27th, 2014.

Daniel Kahneman.

Thinking, Fast and Slow.
Penguin Books, 2011.

Literature III

Barbara Kordy, Piotr Kordy, Sjouke Mauw, and Patrick Schweitzer.

ADTool: Security Analysis with Attack-Defense Trees (Extended Version).
arXiv preprint arXiv:1305.6829, 2013.
`http://arxiv.org/pdf/1305.6829.pdf`.

R. R. McCrae and O. P. John.

An Introduction to the Five-Factor Model and Its Applications.
Journal of Personality, 60(2):175–215, 1992.

K. D. Mitnick and W. L. Simon.

The Art of Deception: Controlling the Human Element of Security.
Wiley, 2002.

NATO Standardization Agency.

AAP-06 -- NATO Glossary of terms and definitions (Edition 2014), 2014.
Accessed: 2014-10-22, `http://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf`.

James L Parrish Jr, Janet L Bailey, and James F Courtney.

A personality based model for determining susceptibility to phishing attacks.
Little Rock: University of Arkansas, 2009.
`http://www.swdsi.org/swdsi2009/Papers/9J05.pdf`.

Susanne Quiel.

Social Engineering in the Context of Cialdini's Psychology of Persuasion and Personality Traits.
2013.

J. W. Scheeres.

Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks.
Technical report, DTIC Document, 2008.

Literature IV

Bruce Schneier.

The Psychology of Security.
In S. Vaudenay, editor, *Progress in Cryptology -- AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, page 50–79. Springer Berlin Heidelberg, 2008.

Frank Stajano and Paul Wilson.

Understanding Scam Victims: Seven Principles for Systems Security.
Communications of the ACM, 54(3):70--75, 2011.

The TRE$_S$PASSProject, D4.2.1.

Initial report on visualizations of information security risks, 2014.
Deliverable D4.2.1.

Sven Uebelacker and Susanne Quiel.

The Social Engineering Personality Framework.
In *2014 Workshop on Socio-Technical Aspects in Security and Trust, STAST 2014, Vienna, Austria, July 18, 2014*, pages 24--30. IEEE, 2014.