Social Engineering Attacks
Lightning Talk

predict
prioritise
prevent
TRESPASS

Sven Übelacker
Security in Distributed Applications
Hamburg University of Technology

2015-02-24
DFN-Konferenz, Hamburg

SEVENTH FRAMEWORK PROGRAMME

European Commission

TUHH
Technische Universität Hamburg-Harburg

What is Social Engineering (SE)?

definition by Mouton et al. [10]

The science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity.

- Kevin Mitnick was the first one widely known to use SE for gaining access to the digital security domain [9]
- Social Engineering in other domains is nothing new
  - cf. Adam Smith's theory of human behaviour in "The Theory of Moral Sentiments", 1759: passions and the impartial spectator (loss aversion, overconfidence, altruism, …) [1]
- e.g. Phishing, Apple Road Trick, Stuxnet, Snowden documents

Social Engineering (SE)

Categorisation of Social Engineering Attacks

- re-use of Cialdini's Six Principles of Influence [2]
  - Authority, Reciprocity, Commitment and Consistency, Social Proof, Liking, Scarcity
- Stajano/Wilson's seven principles for understanding scam victims [13] (cf. "The Real Hustle")
  - Distraction, Social Compliance, Herd, Dishonesty, Deception, Need and Greed, and Time principle
- Gragg's Psychological Triggers of SE [5]

Why Do People Succumb to SE Attacks?

- socio-demographics [3]
- knowledge (awareness) of SE attacks and attacker's intentions [4]
- stressors
- freedom of action
- proficiency towards technology & internet
- cultural background (e.g. uncertainty avoidance) [7]
- evolutionary flaws in risk perception and assessment [12]
- personality traits [11] and impulsiveness
- human information processing
  - peripheral/heuristic vs. central route processing [8]
  - Dual Process Model of Persuasion [6]

↪ **How to measure such factors?**

SE Questionnaire

- questionnaire will be available this summer
- enhanced by influential factors to shed more light on this topic
- gather empiric data to measure intended behaviour via scenario-based questionnaires derived from SE attacks
  - **Have you experienced SE attacks in your organisation?**
  - **Do you have countermeasures or procedures in place to prevent or mitigate SE attacks?**
- **Who wants to participate in the questionnaire and receive updates as well as results?**

Thank you! Suggestions & Questions in the Breaks!

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.

About TRESPASS

- EU funded FP7 integrated project (2012--2016)
- covering the three socio-technical 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

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/21998/2/089533005774357897%5B1%5D.pdf`.

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.

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.

Literature II

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.

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

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

Francois Mouton, Louise Leenen, Mercia M Malan, and HS Venter.

Towards an Ontological Model Defining the Social Engineering Domain.
In *ICT and Society*, pages 266--279. Springer, 2014.

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`.

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.

Literature III

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