Making Security Awareness Measurable

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
Magdeburger Institut für Sicherheitsforschung

DeepSec 2017

About Me

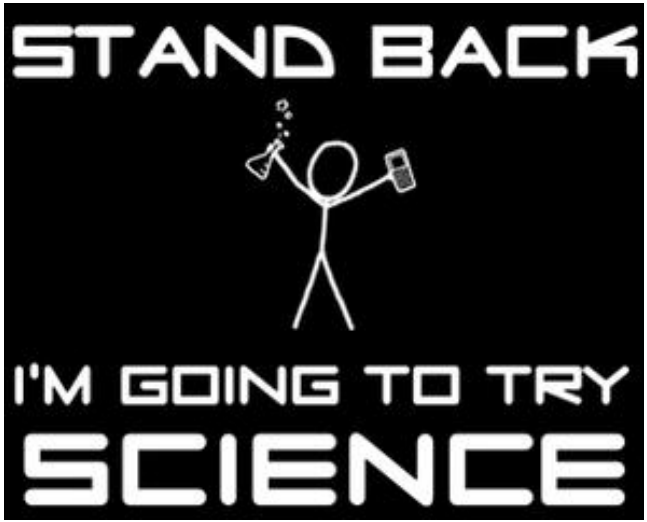
About me

- President of the Magdeburg Institute for Security Research
- Editor of the Magdeburg 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
- memory falsification: DeepIntel 2017: Manipulating the Human Memory for Fun and Profit

Definition (Outrage as a Svc @OaaSvc)

Science is awesome. You aren't doing science in infosec. Why not? Seems to be the overriding message of @0xKaishakunin #AusCERT2014

Stand Back!



Why?

- Security Awareness is a huge buzz word
- money can be made
- scientific foundation lacks
- fundamental research has to be done
- Awareness is not enough
- Evaluation lacks or is to simple
- measuring things is complicated

Why measuring Security Awareness?

- to evaluate security awareness campaigns (What the Heck is Mr. Schumacher doing there?)
- evaluation in a psychological/pedagogical/didactical way, not financial
- to assess the capabilities of an individual
- to assess the capabilities of an organisation
- to identify weak spots
- to make security awareness training professional – no professionalisation without evaluation!
- where diving into the field of psychology and pedagogy
- measuring things there is fundamentally different from measuring things in natural and engineering sciences

Psychology

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

Psychology and IT-Security?

Measurement is the assignment of scores to individuals so that the scores represent some characteristic of the individuals.

- How can we measure security?
- Can we mesure it directly?
- WTF is security?

Psychology and IT-Security?

Security is a latent social construct and has to be treated as such.

Psychological and sociological methods and tools are required.

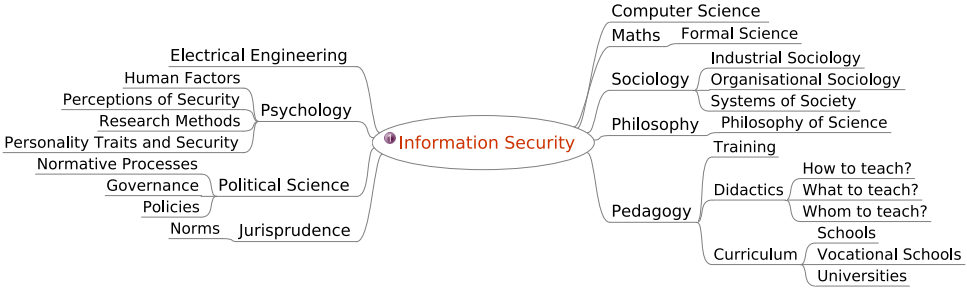
If the security of a system should be enhanced, a diagnosis, prognosis and intervention is required.

Latent Social Construct

- Construct: cannot be directly measured
- can only be measured by using manifest variables to estimate the latent variables
- examples: Intelligence: IQ-Tests
- security cannot be measured directly
- operationalisation of security required

Security and Psychology

- Security is concluded by making Decisions
- Individuals make decisions based on their Biography, the Situation and how they perceive their Environment
  see: von Foerster, Luhmann, Spencer Brown, Baecker et.al.
- Psychology is the Science which researches these Topics.
- Therefore, Psychology is *required* to research Security.
- Psychology is the only Science able to research the basic fundamentals of Security.


Information Security
Computer Science
Maths
Formal Science
Sociology
Industrial Sociology
Organisational Sociology
Systems of Society
Philosophy
Philosophy of Science
Pedagogy
Training
Didactics
How to teach?
What to teach?
Whom to teach?
Curriculum
Schools
Vocational Schools
Universities
Electrical Engineering
Psychology
Human Factors
Perceptions of Security
Research Methods
Personality Traits and Security
Political Science
Normative Processes
Governance
Policies
Jurisprudence
Norms

1996: Ariane 5 Flight 501

64 Bit Float $\rightsquigarrow$ 16 Bit signed Int $\rightsquigarrow$ 320 000 000 Euro

Awareness is not enough

- Awareness is not enough
- being aware of something does not mean you act accordingly
  most smokers know that smoking is bad for your health
- action is required
- theory of action
- cf: Soviet Psychology: Galperin, Wygotski, Leontjew, Leontiew; East German Psychology: Hacker, Volpert (psychological regulation of action)
- English language literature is scarce

What is Security?

- *Security is a latent social construct*
- Operationalisation
- Security is what you define it to be
- *Test test tests*
- If you only have a hammer ...
- The whole measurements depends on the operationalisation!

Operationalisation

The Scientific Way

Qualitiy criteria for tests/measurements:

- Realiability: do multiple test yield the same results?
- Objectivity: how dependent is the measurement upon the examiner?
- Validity: do we measure what we are supposed to measure?


PHRENOLOGY
BY
L.N. FOWLER.

Operationalisation

The Scientific Way

- identify a useful suitable measuring instrument (questionnaire, narrative interview, participant observation)
- identify the measurement parameter
- find a suitable survey methodology
- experiment: identify the dependent and independent variable

Operationalisation

The Practical Way

- WTF is Security for us?
- Identify roles for your organisation (sysadmin, developer, office clerks, management, trainee)
- Identify the decisions they have to make with regards to securityWhat freedom do they have?
- define capabilities to develop, learning outcomes etc.
- Identify way to measure their behaviour/actions and apply them

Example

Storing passwords in a DB

lots of hacks and leaks, from Stratfor to Linkedin; Required Knowledge:

- don't store Passwords in plain text
- encrypt or hash passwords
- which algorithm to use?
  - your own implementation: very bad
  - MD5: bad
  - SHA1: bad
  - SHA1 (MD5 + Salt): bad
  - pkcs5 pbkdf2: better

let the developers create a design or specific implementation and check it

Example
Passwords

define rules for secure passwords

- min length of 12 characters
- min 1 special character, number, lower case, upper case
- no word from a dictionary
- no former password
- no patterns (secret1; secret2; secret3)

check the passwords with PAM etc.

Example
Passwords

- offer a training
- explain how passwords work
- that all computers are connected in your company (everyone is important!)
- how hashes work $\rightsquigarrow$ live hacking
- offer a way to create a strong password in an easy way (eg. Initials):
  I shall create a strong password with at least 12 letters! $\rightsquigarrow$ Iscaspwal12l!

Example
Passwords

- compare the used passwords before and after the training
- congratulations, you made a scientific pre/post testing :-)

Example

Social Engineering

- Oh dear
- How do I prevent Social Engineering?
- break it down to eg. phishing mails
- send out fake phishing mails and measure how many of your coworkers click on the included link
- you have a nice number and even a percentage
- can be presented in colourful Powerpoints
- but only measures one very specific form of Social Engineering
- test design for human based SE is very, very complicated

Know your bias

Why we need Psychology pt. 31337

- Often ignored problem: Person - Organisation - Situation
- Motivation is *fundamental* for human actions
- the same person behaves different in the same situations (humans are no Turing machines!)
- Motivation is very volatile (ever tried to diet or quit smoking?)
- if you have a hammer ...
- statistical bias: selection bias, reporting bias, attrition bias ...
- Hawthorne effect: people change their behaviour when they (assume they) are watched
- Teaching to the Test
- cultural differences (error management culture)

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html

- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- LinkedIn / Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co
- GnuPG: 9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF