Why IT Security is fucked up ...

... and what we can do about it

Stefan Schumacher
www.sicherheitsforschung-magdeburg.de

DeepSec 2014
Vienna, Austria
2014-11-20

$ Id: ItSec-Input.tex,v 1.4 2014/11/20 16:22:14 stefan Exp $

ToC

ToC

About me

About me

- Head 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, Security Awareness, Organizational Security
- psychological profiling for social engineering
- my PoV is more a psychological PoV

Psychology of Security

- Fundamental Research about the Perception of Security
- Fundamental Research about Personality/Attitudes and Security
- Organizational Development and Security
- Cultural Differences
- Didactics (Teaching Methodology) of Security
- What to teach?

ToC

Security in a Post NSA age?

- Talk at AusCERT (Australia) 2014
- Can there be »security« in a Post NSA age?
- Are the 5 eyes an almighty adversary?
- Panopticon $\rightsquigarrow$ Panspectron
- If so, why and how?
- If not, shouldn't we just surrender?

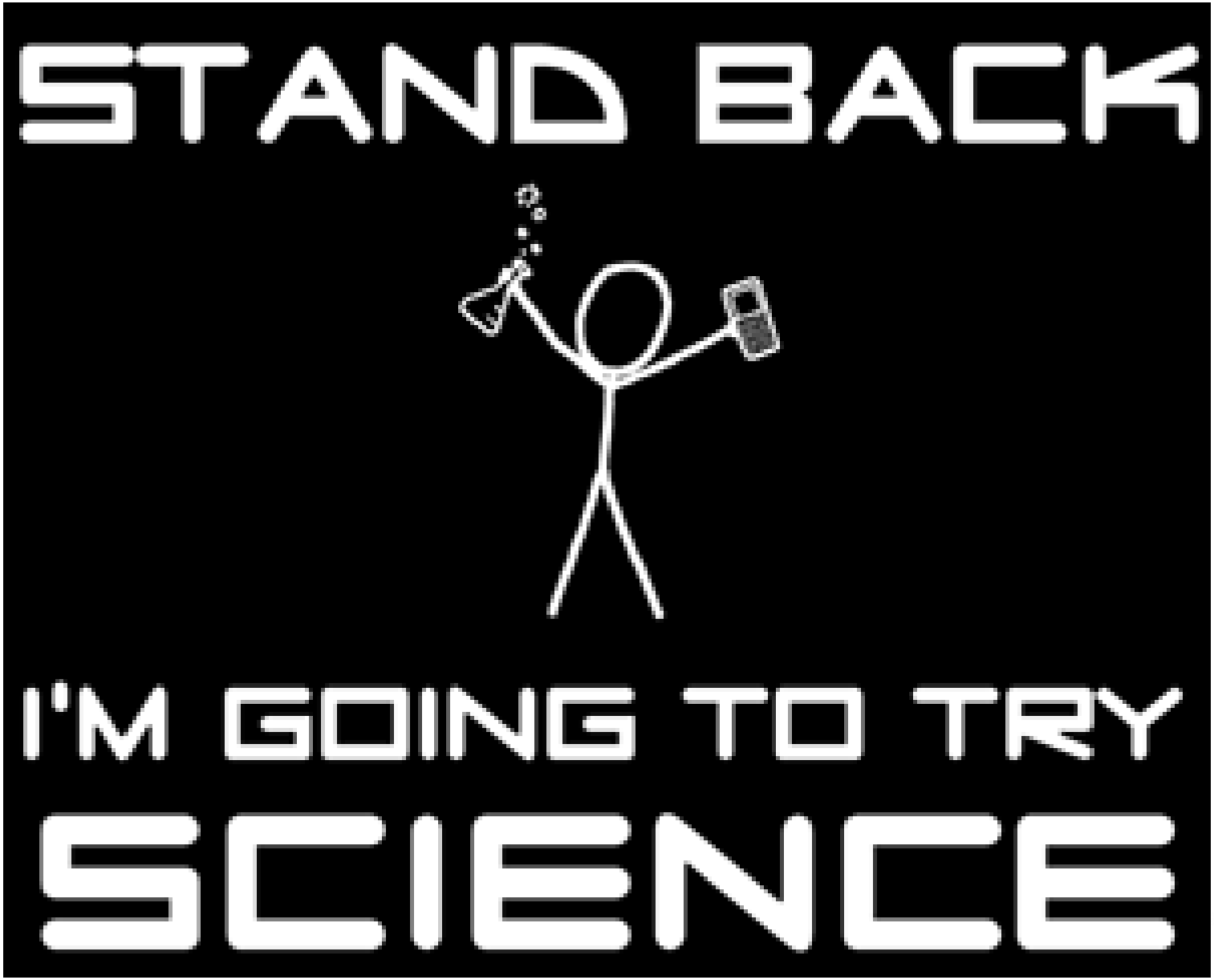
Security in a Post NSA age?

- Of course there can and will be security post NSA.
- Let's discuss some problems and ideas.
- And have a holistic view (read: not just technical)
- use sociological system theory and 2nd order cybernetics
- use psychology to discuss human behaviour and experience
- reflect on the foundation of science
- and how useful are the methods we use?

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!



Consequences for us?

- What do the Snowden Leaks mean for us as security researchers?
- Let's assume there is an adversary with almost unlimited resources.
- How do we have to change how security works?
- What research has to be done?

2nd Order Cybernetics

break the circlejerk

- Cybernetics: transdisciplinary approach for exploring regulatory systems, their structures, constraints, and possibilities.
- Anything said, is said by an observer (Maturana/Varela)
- add the observer to the regulatory system: 2nd order cybernetics
- An observer acting in his field: 1st order cybernetics
- An observer discussing how he constructs his perception of the field he works in: 2nd order cybernetics (What the hell are we doing here?)

Trust

- Trust is one of the buzzwords here
- needs to be defined or explicated
- and operationalized (make it measurable)
- Niklas Luhmann explicated Trust in his 1968 Book *Vertrauen*
- as a »mechanism to reduce social complexity«
- social complexity is reduced with functional specialised subsystems
- Lawyers a experts for Laws, Hackers for IT-Sec, Physicians for Medicine etc. pp.

Consequences

- IT Security needs to professionalize beyond technical problems
- discussing the 31337th Buffer Overflow of the week won't fix fundamental problems
- human factors have to be analysed
- extend IT Security to Information Security
- create a new scientific field of Information Security
- include Psychology, Sociology, Educational Science, Didactics and others
- operationalize Information Security to make it measurable
- create a new vocational field of Information Security
- backed by science

ToC

Why 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.

What is security?

Germany, Informatics

- *VIVA-Kriterien*
- confidentiality
- integrity
- availability
- authenticity

Paradigm Shift

- see Thomas S. Kuhn *The Structure of Scientific Revolution*
- Paradigm: a distinct concept or thought patterns and basic assumptions
- Paradigm Shift: change of these assumption
- let's change it

Psychology and IT-Security?

My Operationalisation of InfoSec

Security is a latent social construct.

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.

Washing your Hands

- two maternity clinics in Vienna, the 1st with MDs the second with midwifes only
- more pregnant Women died in the 1st one
- pregnant women would rather give birth in the streets than be sent to the 1st clinic
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents (cadaverous poisoning)
- He proposed that Physicians should wash their Hands
- the death rate dropped 90%
- His Idea was rejected and he was considered to be crazy
- psychiatrised by force in Vienna

Washing your Hands

- two maternity clinics in Vienna, the 1st with MDs the second with midwifes only
- more pregnant Women died in the 1st one
- pregnant women would rather give birth in the streets than be sent to the 1st clinic
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents (cadaverous poisoning)
- He proposed that Physicians should wash their Hands
- the death rate dropped 90%
- His Idea was rejected and he was considered to be crazy
- psychiatrised by force in Vienna
- This can only be explained by Psychology

Washing your Hands

- two maternity clinics in Vienna, the 1st with MDs the second with midwifes only
- more pregnant Women died in the 1st one
- pregnant women would rather give birth in the streets than be sent to the 1st clinic
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents (cadaverous poisoning)
- He proposed that Physicians should wash their Hands
- the death rate dropped 90%
- His Idea was rejected and he was considered to be crazy
- psychiatrised by force in Vienna
- This can only be explained by Psychology

1996: Ariane 5 Flight 501

320 000 000 Euro

ToC

Societal Problems

- digital divide
- economy and IT
- checks and balances?
- How do politicians decide about things they don't understand? (Max Weber again ...)
- and scientists?
- Why and How did Rijndael become AES? NSA? NIST? Illuminati?

Societal Problems

- digital divide
- economy and IT
- checks and balances?
- How do politicians decide about things they don't understand? (Max Weber again ...)
- and scientists?
- Why and How did Rijndael become AES? NSA? NIST? Illuminati?

Political Problems

- Cyber-War? Cyber-Terror?
- discussed by political scientists – who often don't understand technology
- discussed by IT sec – who often don't understand social implications
- discussed by the military – who often don't understand anything
- discussed by legal experts – who often don't understand technology and social implications
- How to discuss Anonymous? Hacktivism? Neutral?

Political Problems

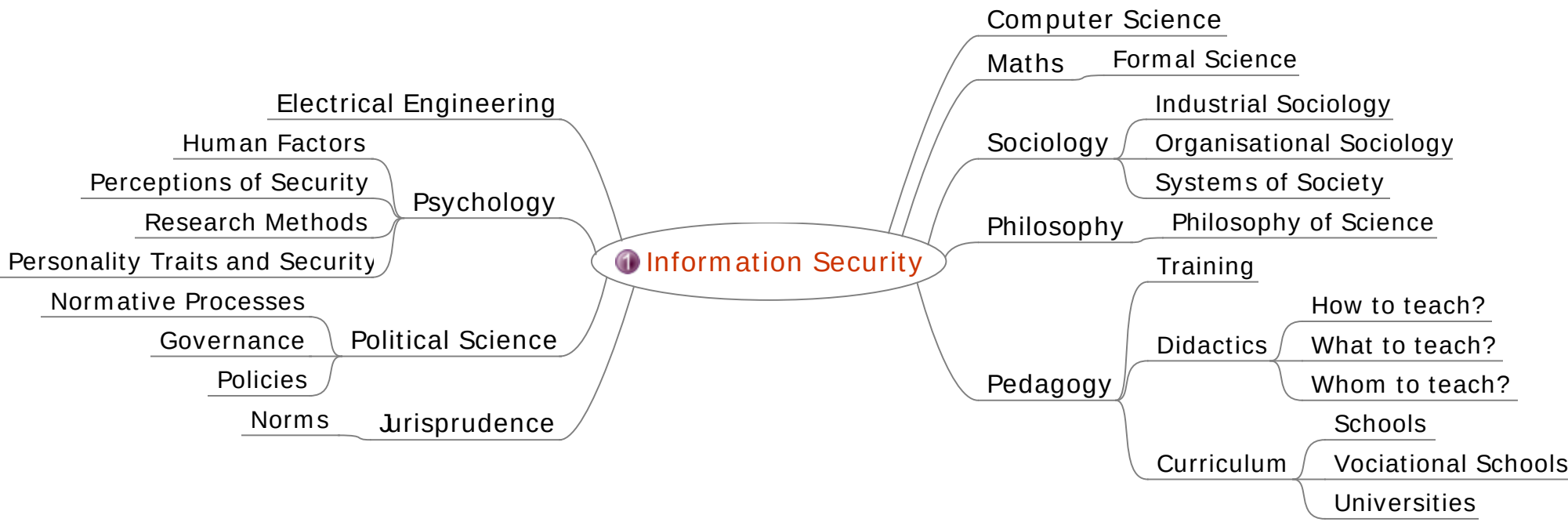
- Cyber-War? Cyber-Terror?
- discussed by political scientists – who often don't understand technology
- discussed by IT sec – who often don't understand social implications
- discussed by the military – who often don't understand anything
- discussed by legal experts – who often don't understand technology and social implications
- How to discuss Anonymous? Hacktivism? Neutral?

Reflection

- The information technology of society?
- The hackers of society?
- The intelligence services of society?

Conclusion

- IT-Security needs it's own research field: security research
- with it's own foundation, methods and tools
- rooted in:
  - Maths as formal science
  - CS/EE as engineering science
  - Sociology, Political Science as social science
  - Jurisprudence as normative science
  - Philosophy as mother of all sciences
  - Psychology as **hub science**


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
Vociational Schools
Universities
Electrical Engineering
Psychology
Human Factors
Perceptions of Security
Research Methods
Personality Traits and Security
Political Science
Normative Processes
Governance
Policies
Jurisprudence
Norms

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

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