About

- These slides are a part of a summer school on IT security and hacking I taught at university in summer 2019
- Some sensitive parts have been redacted
- The parts about Security, Crypto and Blockchain have been included



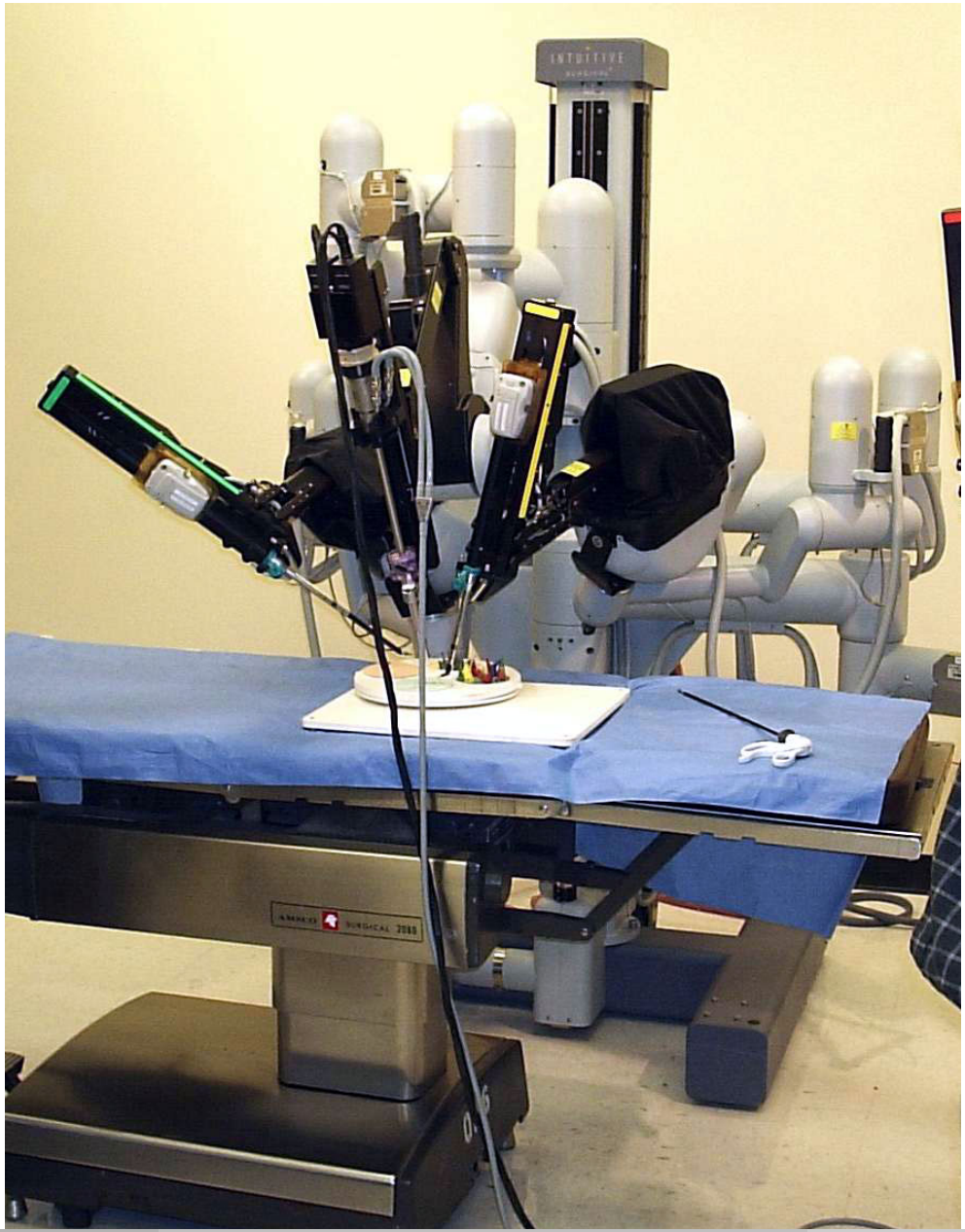
Part I

Intro:

So why so sad?



Laproscopic Surgery Robot



Where are we going to?

- more and more IT
- almost no one knows how to do IT security right
- lack of training
- lack fundamental research
- no psychology of security

Risks I

- White collar crime and industrial espionage can hit everyone!
- targeted attacks against industry and science
- foreign powers support their own industry with their own intelligence services
- Cyberwar: attacks on critical infrastructure (including health care)

Risks II

- non-targeted attacks by organised cyber-crime syndicates e.g. from Russia
- well established mafia structures, set up by former military intelligence and LEOs
- well trained computer scientists and hackers
- almost complete analysis of communication data by the NSA (Echelon/Prism/Tempora)
- economic warfare against Germany
  NSA vs. Enercon https://www.focus.de/finanzen/news/enercon-spione-im-wind_aid_162267.html
- Protect your assets!

Attack Vectors

some examples

- underground market for exploits, vulnerabilities and malware exists
- phishing tools, trojans etc. can be bought premade or customised
- IRC chat rooms or underground forums
- simple standard attacks can be done easily
- Who is going to attack me? I am not that interesting!
  Wrong! A »dragnet« is cheap!

Attack Vectors

some examples

- underground market for exploits, vulnerabilities and malware exists
- phishing tools, trojans etc. can be bought premade or customised
- IRC chat rooms or underground forums
- simple standard attacks can be done easily
- Who is going to attack me? I am not that interesting!
  Wrong! A »dragnet« is cheap!

Attack tools

- fully automatised attack tools scan through large parts of the internet
- try to identify version of the operating system and find known vulnerabilities
- break into targets and install trojans and root kits $\rightsquigarrow$ botnets
- BredoLab: 30.000.000; Mariposa 13.000.00; Conficker 9.000.000 Zombies; Rustock 1.700.000 Zombies and 44 billion spam mails/d


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/20/2013
12:37 PM
Time left
72 : 34 : 50
Next >>

CRYPTOLOCKER

- attacks Windows and trojanises it
- encrypts f.e. Office, OpenDocument, Text, AutoCAD, Bilder
- 2048 bit RSA encryption, private key on CnC Server
- pay 400 € or the private key gets deleted
- CryptoDefense: ca. 38000 $ per month
- untargeted mass attacks, now we see targeted attacks
- with much higher ransom
- German jeweller chain paid 1 mio €

Cryptolocker

- 10 FEB 2016: Lukas Hospital Neuss (537 beds, 90 000 out-patients, 29 500 in-patients p.a.), champion of digitalisation
  shut down by a ransomware attack (crypto trojaner)
- 08 FEB 2016: Dettelbach (Bavaria) municipality shut down by TeslaCrypt 2.0, paid the ransom (ca. 600 EUR)
- 30 APR 2019: CityComp, cloud hoster for VW, Porsche, AirBus, NH Hotels et.al. hacked, ransom of 450 000 EUR wanted
- nice operation theater you got there
  would be a shame if something happened to it
- JUN 2017: 16 Hospitals across the UK shut down, 450€ demanded
- MAY 2019: Lake City, USA paid ca. 460 000 US$ ransom



- ABC News Video

Attack Tools

- February 2000: eBay.com, Amazon.com, Buy.com, ETrade.com, CNN.com shut down with dDoS attack; FBI claimed damages to be 1,7 Mrd US$
- Offender : 15 years old high school pupil going by the name *Mafiaboy*, used a script called *Stacheldraht*, to shut down websites because he was bored
- Operation Payback: dDoS attack on Visa, Mastercard and Paypal in the Netherlands, 15 and 16 year old pupils arrested

Attack Tools

- February 2000: eBay.com, Amazon.com, Buy.com, ETrade.com, CNN.com shut down with dDoS attack; FBI claimed damages to be 1,7 Mrd US$
- Offender : 15 years old high school pupil going by the name *Mafiaboy*, used a script called *Stacheldraht*, to shut down websites because he was bored
- Operation Payback: dDoS attack on Visa, Mastercard and Paypal in the Netherlands, 15 and 16 year old pupils arrested

- A Theory from Social Science / Mass Psychology
- influencing masses to a predictable, predetermined behavior
- sth. totalitarian regimes want
- Think of *We* (Jewgenij Samjatin), *1984*, *Brave New World*

- in IT Security/Hacking:
- a technique to circumvent security mechanisms by misusing human behavior
- »Hacking People«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?

- in IT Security/Hacking:
- a technique to circumvent security mechanisms by misusing human behavior
- »Hacking People«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?

Spear Phishing I

- targeted attack against a C-Level executive
- information on friends, coworkers, hobbies etc. gathered from OSINT
- social networks like Facebook, LinkedIn, Stayfriends
- favourite vacation places, favourite musice, former class mates
- attacker create multiple fake social media profiles
- gather and cross check information
- created a website about the favourite football club

Spear Phishing II

- managed by a former class mate
- contact and invite victim to join the website
- it's about his favourite football club, of course he joins
- uses one of his standard passwords
- his private email account uses the same password
- malware sent to his children, their accounts taken over
- captured accounts used to attack his work accounts
- **You have lost ...**

LEFT-PAD/INDEX.JS

```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch && ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```



Buffer Overflow

- buffer to small for to big data
- buffer overflow, memory integrity is violated
- consequences: return address of a sub routine overwritten with arbitrary data $\rightsquigarrow$ root exploit
- code monkey just has to use the correct code...

Buffer Overflow in C

Das Problem

```
1 void input_line()
2 {    char line[1000];
3      if (gets(line))
4          parse_line(line);
5 }
```

`line` with length 1000 declared
`gets` points to an array *without length*
wenn `line` greater than 1000 = Problem
Thou shalt not follow the pointer



Buffer Overflow in C

Die Lösung

```
1 void input_line()
2 {    char line[1000];
3      if (fgets(line, sizeof(line), stdin))
4          parse_line(line);
5 }
```

`gets` points to an array *with length*
avoid low level languages, PaX, `w^x` ...
It's a human decision



Buffer Overflows

- 02.11.1988: Morris-Worm exploited a Buffer-Overflow via `gets()` in finger(1)
- 1996: Aleph One *Smashing the Stack for Fun and Profit* in Phrack 49
- 2001: Code Red
- 2008: SQL Slammer
- CORE-2007-0219: OpenBSD's IPv6 mbufs remote kernel buffer overflow
- 2007: Buffer Overflow in Snort
- VU#987308: HP LoadRunner buffer overflow vulnerability



1996: Ariane 5 Flight 501



Ariane 5 Flight 501

- 1996 Ariane 5 501: self destroyed after 36,7 Sekunden
- Software ported from Ariane 4 to Ariane 5
- 64 Bit Float casted in 16 Bit signed Int
- Acceleration of Ariane 5 is much higher $\rightsquigarrow$ Overflow
- test simulation did not find the error
- Firework worth 320 000 000,– Euro

Part II

Problems of IT Security:

Research Proposal



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

1 Social Science

2 Psychology

3 What to do?

4 Fundamental Research

Security in a Post NSA age?

- Talk at AusCERT (Australia) 2014
- Talk at PhDays Moscow 2015
- 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?

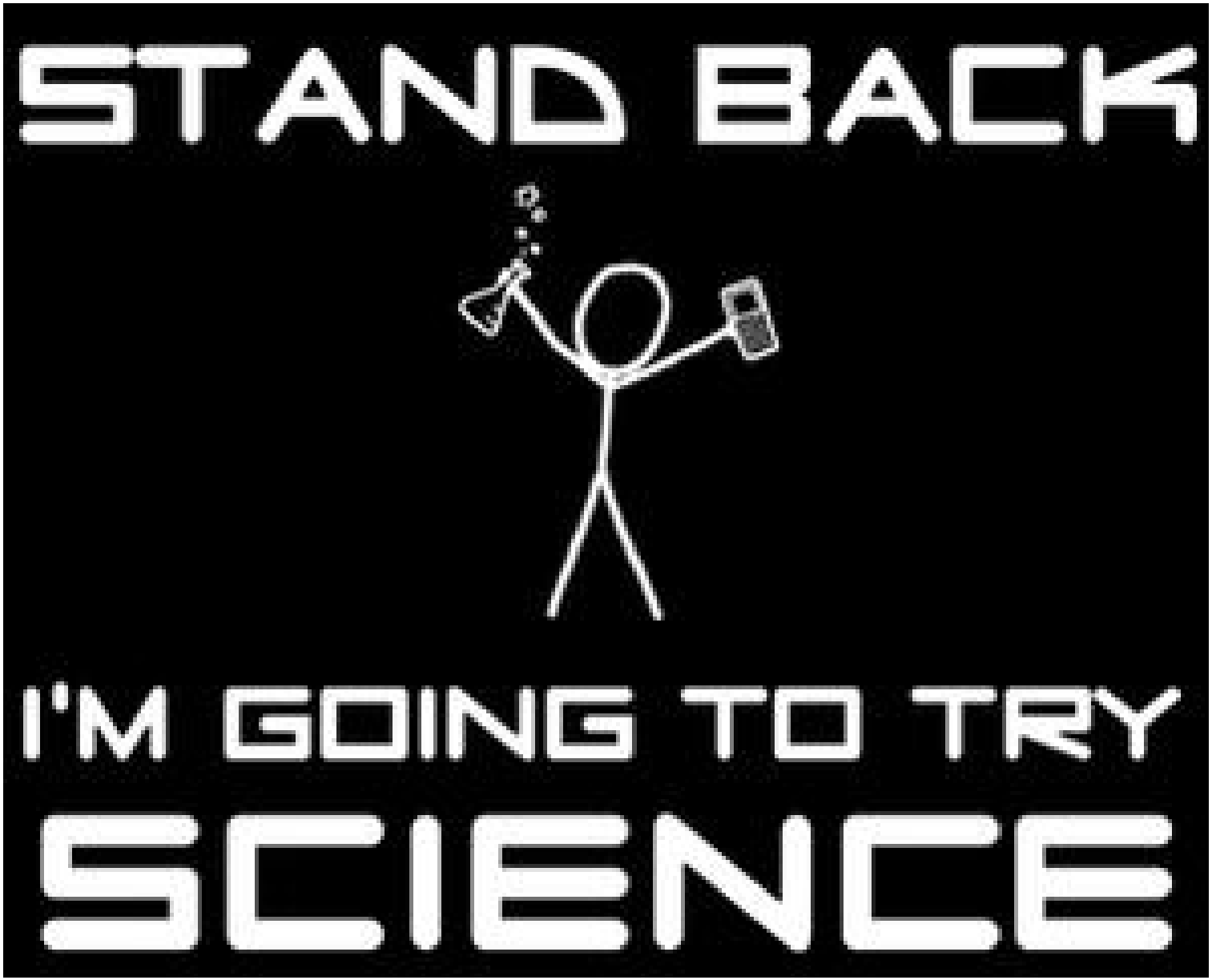


Definition (Outrage as a Svc @OaaSvc)

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



Stand Back!



After Snowden

- NSA leaks had differents effects on society
- sociological system theory (Niklas Luhmann et.al.): societies differentiate into functional specialised subsystems
- each subsystem focuses on different aspects of it's environment/society
- Legal System vs. Religious Systems vs. Political System
- Science: Philosophy vs. Humanities vs. Engineering vs. Natural Science

After Snowden

- Hacker: those conspiracy theorists with their tin foil hats were right ...
- IT-Sec: Paranoids: we expected the worst case scenario and prepared for it
- IT-Sec: not so paranoid: well, they have a lot to do
- Business: often helpless against industrial espionage, resigned
- Politicians: follow the party programme ..., Piratenpartei failed
- End User: either uninterested or resigned, Twitter activism does not really help
- Media: circlejerking according to their agenda

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.

Trust

- every user has to trust the sysadmin
- every sysadmin has to trust the OS developers
- every os developer has to trust the compiler
- every compiler has to trust the OS it's running on
- there is no way to have an ontological access to the surrounding world
- you have to trust your own perception
- can you?



Trust

- every user has to trust the sysadmin
- every sysadmin has to trust the OS developers
- every os developer has to trust the compiler
- every compiler has to trust the OS it's running on
- there is no way to have an ontological access to the surrounding world
- you have to trust your own perception
- can you?



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

1 Social Science

2 Psychology

3 What to do?

4 Fundamental Research

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

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.

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

1 Social Science

2 Psychology

3 What to do?

4 Fundamental Research

ToC

1 Social Science

2 Psychology

3 What to do?

4 Fundamental Research

Perception of Security

- radical constructivistic approach
- each Individual perceives the World in one's own Way
- shaped by one's former experiences
- We have to explore this Worldview in depth
- by qualitative Research

Perception of Security

- different Tools and Methods exist
- several qualitative/semi-structured Interviews are lead with different interviewes
- eg. autobiographic-narrative Interviews with Hackers and Users
- Expertinterviews with Hackers and Researchers
- What shapes a Hacker's mind?
- How do Users perceive IT-Security?
- How can this Perception be changed?
- Are there science based Security Awareness Tools?

RISKHOMEOSTASIS

- Risk behaviour is controlled by different Variables
- Self-perception, subjective Skills, objective Skills, Perception of Risk, Risk acceptance
- Researched in Industrial Psychology: Air Traffic Controller/Pilots, Workers in Nuclear Power Plants, Motor Vehicle Operator ...
- Study: East German Taxi Drivers switched from Wolga to Mercedes and had more accidents

RISKHOMEOSTASIS

- Risk behaviour is controlled by different Variables
- Self-perception, subjective Skills, objective Skills, Perception of Risk, Risk acceptance
- Researched in Industrial Psychology: Air Traffic Controller/Pilots, Workers in Nuclear Power Plants, Motor Vehicle Operator ...
- Study: East German Taxi Drivers switched from Wolga to Mercedes and had more accidents

Personality and Security

- Different Theories of Personality exist
- We use empirical sound Tools to examine Personality Traits and security relevant Behaviour
- Personality Traits are very stable over Lifetime
- quantitative research
- Big5: Neuroticism, Extraversion, Openness, Conscientiousness, Agreeableness
- Motives: Power, Achievement Orientation and others
- How do they correlate with security relevant behaviour?

Organizational Development

- Security is a huge and hot Topic in Companies
- lots of Money is spend on Security Awareness and Training
- lots of different Methods exist eg. in Knowledge Management, Leadership, Organizational Development
- Which of them are useful for security relevant Behaviour?
- Strict Hierarchies can be easily attacked with Social Engineering ...

Cultural Differences

- Culture influences Organisations and Individuals
- What are the differences? How can they influence Security?
- Death by Fan?
- The Protestant Ethic and the Spirit of Capitalism by Max Weber
- eg: How is the TVET system organized? Is there a TVET System? On the job training? Only colleges?
- Lots of Tools and Methods exist, Research Results also
- Can they be transfered to our Problems?

Didactics

- Didactics is the Science of Learning and Teaching
- Teaching Methodology
- very well researched in Germany due to the dual TVET System and in company training
- well funded and empirical sound
- several curriculums for IT skilled labour exist
- how can they be enhanced with IT security?

How?

- How can we teach Security?
- Which Methods work best under which Circumstances?
- E-Learning? Blended Learning? Only Facts? Theory? Practical Approach?
- Culture is relevant
- well researched Model of Competencies/Capabilites is used in Germany
- not only facts are taught, but also studying and research methods
- independent learning is emphasized
- trainees learn *how* to keep their knowledge up to date
- trainees have to be able to know *what* to learn

How?

- How can we use this Model of Competencies/Capabilites?
- What are the best Methods to develop those Competencies?
- action oriented teaching? project work? masterpieces?

Who?

- Who has to learn about IT Security?
- Sysadmins, Developers, End Users
- create different roles
- determine what each role has to learn

What

- What to teach and learn?
- Who needs to understand Elliptic Curve Cryptography? Webmaster? Sysadmins? End Users?
- Who needs to understand what?
- How do we test that?
- When and How do those Curriculums and Tests need to be revised?

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

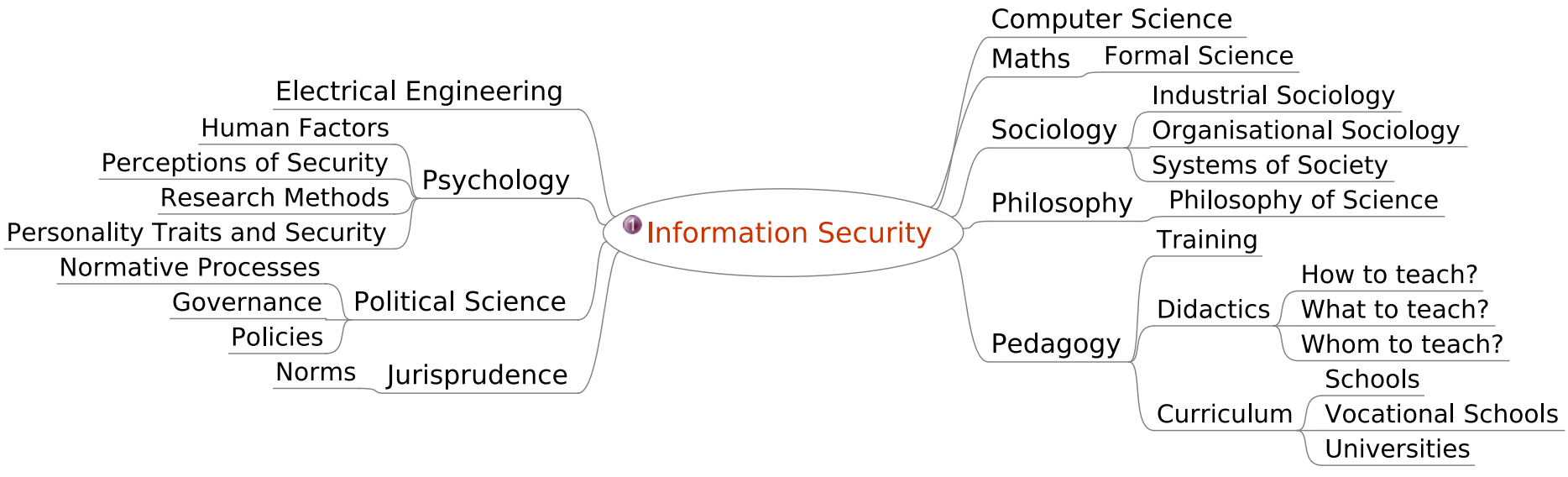
- Cyber-War? Cyber-Terror?
- discussed by political scientists – who often don't understand technology
- discussed by IT sec – who often don't understand social implications
- discussed by the military – who often don't understand anything
- discussed by legal experts – who often don't understand technology 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
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

Part III

Threats, Actors and Vulnerabilities

Threat Modeling

- a process by which potential threats can be identified, enumerated, and prioritized
- from a hypothetical attacker's point of view
- systematic analysis of the probable attacker's profile
- the most likely attack vectors
- and the assets most desired by an attacker

Threat Modeling

- Where are the high-value assets?
- Where am I most vulnerable to attack?
- What are the most relevant threats?
- Is there an attack vector that might go unnoticed?

1. Who is threatening us?
2. What are their motivations and goals?
3. How dangerous are they?

1. Who is threatening us?
2. What are their motivations and goals?
3. How dangerous are they?

1. Who is threatening us?
2. What are their motivations and goals?
3. How dangerous are they?

WHO IS THREATENING US?

- Script Kiddies: unskilled, uses scripts made by others
  80% of all attacks, but only simple ones, easy to defend against
- Hacker: skilled computer expert that uses their technical knowledge to overcome a problem
  small number of attacks, but sophisticated - highly sophisticated attacks
- competitors: industrial espionage attack sophistication varies, might hire black hat hackers, APTs
- organised crime: ransomware campaigns, industrial espionage, APTs
- state actors: highly sophisticated attacks, APTs
- insider threat: oh dear



Why are they threatening us?

- Just for fun
- To gain street credibility
- Denial of Service
- steal data
- advanced persistent threat
- industrial espionage
- revenge / destruction

Attack Vectors

- Passwords
- Known Vulnerabilities
- Vulnerabilities in PDF viewers
- Vulnerabilities in Webbrowsers
- Zero Day Exploits

PLASTIC ROUTERS

- cheap devices in the internet (cameras)
- Router, NAS, smart TV, Smartphones, Smartmeter, Industry 4.0, Cars, IoT
- millions of FritzBoxen hacked
- Synology NAS exploited as Bitcoin Miner
- Vulnerabilities in Smart TVs
- SCADA! (Siemens Simatic STEP7? Stuxnet?)
- Pressure on the manufacturers? Dream on!

Myagmar, S., Lee, A. J., & Yurcik, W. (2005).Threat modeling as a basis for security requirements. *Symposium on requirements engineering for information security (SREIS), 2005*, 1–8

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.703.8462&rep=rep1&type=pdf



Part IV

Crypto

Cryptography

- no security without cryptography
- cryptography is hard to implement
- harder to check for security

Group Work

- What is a Man in the Middle Attack?
- Describe the von-Neumann-Architecture
- Describe protection rings (in Computer Science)
- confidentiality
- integrity
- availability
- authenticity
- non repudiation
- accountability

Group Work

- What is symmetric and asymmetric cryptography?
- What are the public and private key used for?
- What is a Hash? What is a cryptographic hash? A digital signature?
- What is key escrow?
- Name 10 programs/standards that utilise cryptography and explain their use.
- Name 5 crypto algorithms and cipher modes and explain their use.

Part V

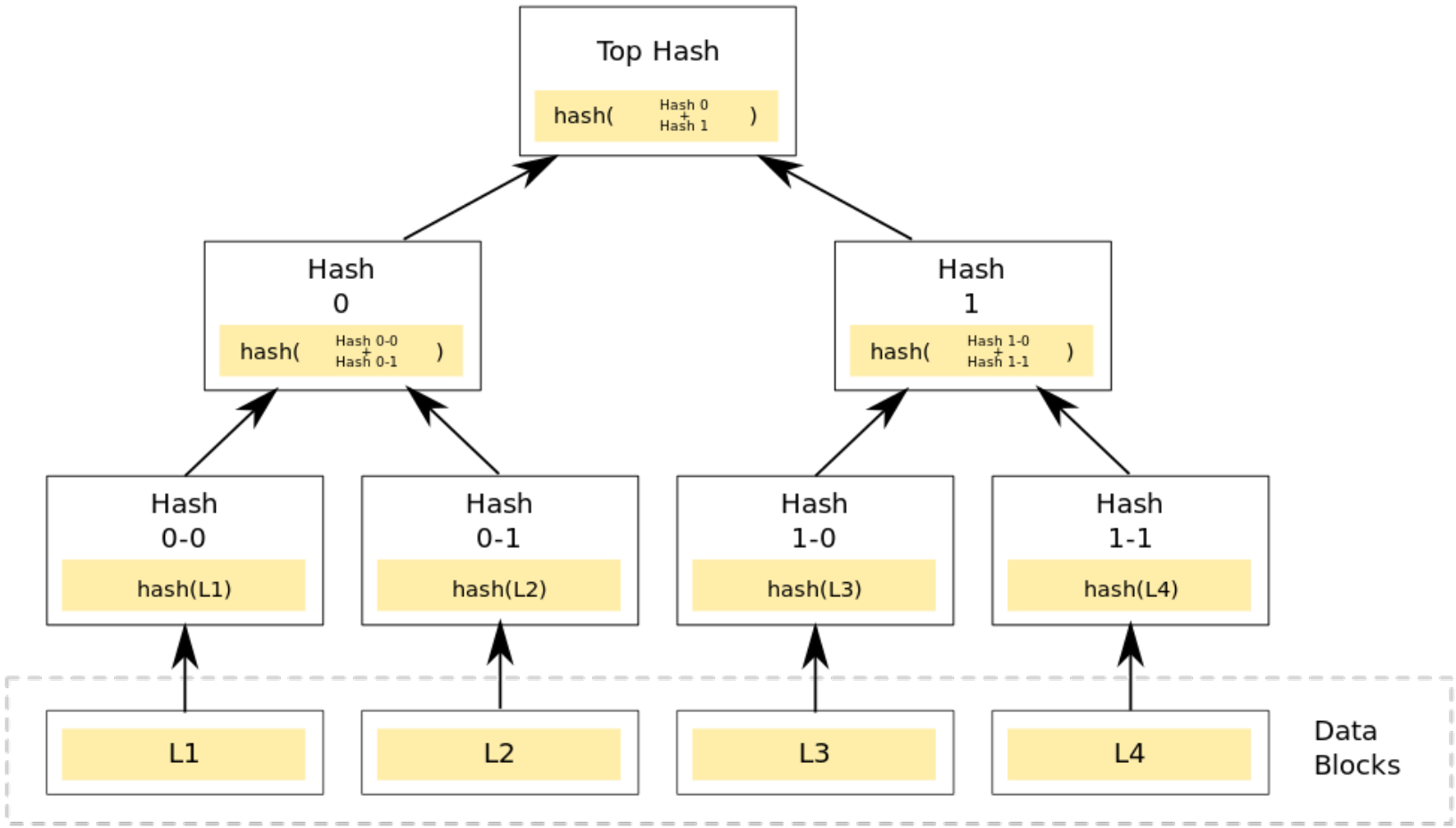
Blockchain

Blockchain

- growing list of records (blocks) linked together using cryptography
- each block contains a cryptographic hash of the previous block, a timestamp, and transaction data
- works as a distributed ledger
- by design: resistant to modification of the data
- can be managed by a peer-to-peer network
- does not require a central server or trusted authority
- once recorded, data in any given block cannot be altered retroactively without alteration of all subsequent blocks
- which requires consensus of the network majority

- decentralized, distributed and public digital ledger that
- used to record transactions across many computers
- so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks
- transaction can be easily and independently verified and audited
- blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server
- authenticated by mass collaboration
- removes the characteristic of infinite reproducibility from a digital asset
- confirms that each unit of value was transferred only once
- value-exchange protocol

- designed by Ralph Merkle (Merkle Tree)
- tree of hashes
- leaves are hashes of data blocks
- nodes further up in the tree are the hashes of their respective children
- root hash: hash of the complete data (eg. file or database)
- checking if a leaf is part of any given binary hash tree: $log(n)$ hashes have to be calculated
- hash list: n hashes
- a branch of the tree can be checked even if the whole tree is not available


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

- batches of valid transactions
- hashed and encoded into a Merkle tree
- includes the cryptographic hash of the prior block $\rightsquigarrow$ block chain
- blocks can be produced concurrently leading to a fork
- blockchain needs an algorithm for scoring different versions
- block time: average time it takes for the network to generate one extra block
- Ethereum: 15 sec, Bitcoin: 600 sec
- hard fork: change of rules, old rules will see new blocks as invalid



- no central points of vulnerability
- no central point of failure
- massive database replication: every node has a copy of the blockchain
- no user is trusted more than any other
- use of public key cryptography
- risk of centralisation as mining becomes expensive

- public blockchain: no access control needed, guards against bad actors not required
- private blockchain: use access control
- problem: single computer (network) controls the access $\rightsquigarrow$ SPoF

- computer protocol
- digitally facilitate, verify, or enforce the negotiation or performance of a contract
- performance of credible transactions without third parties
- transactions are trackable and irreversible
- self-executing and/or self-enforcing contractual clauses
- Bitcoin provides a scripting language to create custom smart contracts, eg: escrows, time locks, multi-party lottery with no operator

- asymmetric cryptography
- each user has a key pair
- address of user is a hash derived from the public key
- users can view all past transactions