esse

# IT Security in Large IT Infrastructures SS18
# Lecture 07: Wrap-Up

Florian Fankhauser
Christian Schanes

**INSO – Industrial Software**
Institute of Information Systems Engineering | Faculty of Informatics | TU Wien

# Agenda

IT Security Topics in Large IT Infrastructures

Literature Examples

Wrap up of the Lectures

Security Tests

# IT Security Topics

- IT security aspects in large IT infrastructures
- Competing stakeholders/requirements: cost vs. usability vs. security vs. performance vs. ability to test vs. ...
- Understanding the impact of security topics, e.g., in order to get the budget for IT security measures
- Think about IT security at all!
- Think laterally :)

# Excerpt of Topics in SS2018

- Communication Networks
- Secure Payment
- CEO Fraud, Comfort vs. Security, Employees Travelling Internationally, APT
- Requirements for an ISMS based on the new ISO 27001:2013 Standard Exemplified by the BRZ Infrastructure
- Lifecycle and IT Security of a Bank Chip-Card from the Issuing to the Expiration
- Cloud Security
- Security Based on Open Specifications, Deutsche Gesundheitstelematik

# Literature: IT Security Aspects in Large IT Infrastructures


- Christian Schanes, Florian Fankhauser, Thomas Grechenig, Michael Schafferer, Kai Behning, and Dieter Hovemeyer. Problem space and special characteristics of security testing in live and operational environments of large systems exemplified by a nationwide it infrastructure. In *The First International Conference on Advances in System Testing and Validation Lifecycle, September 2009, Porto, Portugal*, pages 161–166. IEEE Computer Society Press, September 2009. doi: 10.1109/VALID.2009.24
- Andreas Mauczka, Christian Schanes, Florian Fankhauser, Mario Bernhart, and Thomas Grechenig. Mining security changes in freebsd. In *Mining Software Repositories (MSR), 2010 7th IEEE Working Conference on*, pages 90–93, February/March 2010. doi: 10.1109/MSR.2010.5463289

# Literature: IT Security Aspects in Large IT Infrastructures


- Bruce Schneier. *Schneier on Security*. Wiley Publishing, Inc., Indianapolis, Indiana, 2008. ISBN 978-0-470-39535-6
- Herbert Bunz and Manuel Koch. Privacy in the german health telematic infrastructure. In *Proceedings of IHIC 2008*, 2008
- George L. Wooley. Results of classroom enterprise security assessment of five large enterprise networks. *J. Comput. Sci. Coll.*, 18 (3):185–195, February 2003. ISSN 1937-4771. `http://dl.acm.org/citation.cfm?id=771712.771737`

# Literature: IT Security Aspects in Large IT Infrastructures


- Phillip Porras and Vitaly Shmatikov. Large-scale collection and sanitization of network security data: risks and challenges. In *Proceedings of the 2006 workshop on New security paradigms*, NSPW '06, pages 57–64, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-923-4. doi: 10.1145/1278940.1278949. `http://doi.acm.org/10.1145/1278940.1278949`
- Alexander Marold, Peter Lieven, and Björn Scheuermann. Probabilistic parallel measurement of network traffic at multiple locations. *Network, IEEE*, 26(1):6 –12, January/February 2012. ISSN 0890-8044. doi: 10.1109/MNET.2012.6135850

# Literature: IT Security Aspects in Large IT Infrastructures


- João Porto de Albuquerque, Holger Isenberg, Heiko Krumm, and Paulo Lício de Geus. Improving the configuration management of large network security systems. In *Proceedings of the 16th IFIP/IEEE Ambient Networks international conference on Distributed Systems: operations and Management*, DSOM'05, pages 36–47, Berlin, Heidelberg, 2005. Springer-Verlag. ISBN 3-540-29388-4, 978-3-540-29388-0. doi: 10.1007/11568285_4. `http://dx.doi.org/10.1007/11568285_4`
- Tyler Moore and Ross Anderson. Economics and internet security: a survey of recent analytical, empirical and behavioral research. Technical Report TR-03-11, Harvard Computer Science, 2011. `ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf`

# Literature: IT Security Aspects in Large IT Infrastructures


- Saar Drimer, Steven J. Murdoch, and Ross Anderson. Thinking inside the box: system-level failures of tamper proofing. Technical Report UCAM-CL-TR-711, University of Cambridge, Computer Laboratory, February 2008. `http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf`
- Tyler Moore, Richard Clayton, and Ross Anderson. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009. doi: 10.1257/jep.23.3.3. `http://www.aeaweb.org/articles.php?doi=10.1257/jep.23.3.3`
- Neelu Sinha and Laila Khreisat. Cloud computing security, data, and performance issues. In *2014 23rd Wireless and Optical Communication Conference (WOCC)*, May 2014. doi: 10.1109/WOCC.2014.6839924

# Different Projects – Similar Security Aspects

- Management Attention
- Costs
- Appropriate Level of IT Security
- Security Procedures, ISMS
- People

- Often, politically exposed – mass media

- Risk Estimation
- Attack Scenarios
- Backwards Compatibility/Forward Compatibility
- Processing Speed
- Processing Power, Disk Space (RFID, Deutsche Gesundheitskarte)
- New Technologies

# Different Projects – Similar Security Aspects

- Who is responsible for security problems
- Security vs. usability
- How to secure confidential information
- Where to store secure keys?
- Think larger, how secure are crypto systems? Who listens to your communication?
- What influences the security of the system? E.g., problem with compression and AES encryption, RSA vs. ECC
- Where are your data processed, stored, ...? Do you know where your data will go?
- What problems arise if several data sources are linked? E.g., Linked open data uncovers confidential information?

# Communication Networks

- Different Communication Technologies (POTS, VoIP, GSM, SS7, WhatsApp, Skype, Social Media,...)
- Secure Encryption vs. (Lawful) Interception
- World Wide Communication
- Availability, Ease of use
- Interoperability
- Smartphone as Communication Centre

# Secure Payment

- More and More Electronic Means for Payment
- Online Banking
- Debit Cards, Credit Cards
- NFC, Smartphones
- World Wide Use
- Availability, Ease of use
- Penetration Test of Banking Infrastructure

# Multiple Security Short Stories

- CEO-Fraud
- Comfort vs. Security
- Employees Travelling Internationally
- Advanced Persistent Threat (APT)
- Industry 4.0
- Critical Infrastructures

# ISMS

- Basics of an ISMS
- Example BRZ, Certification Processes
- Different security measures to secure the IT infrastructure
- Awareness, Understanding
- Secure Coding Standards
- Audits

# Lifecycle and IT Security of a Bank Chip-Card from the Issuing to the Expiration

- EMV Specification
- Shift of Liability
- Interoperability
- Structure/Security of Chipcards
- Card Vendor/Card Personaliser
- Card Management System
- Issuer, Acquirer
- Cryptography, HSM

# Cloud Security

- Many systems in the cloud
- Technical requirements (e.g., IP multicast)
- TAP technology, TAP in the cloud
- Aggregation of messages
- Processing applications
- Processing of security data in the cloud

# Deutsche Gesundheitskarte

- Security, transparency, confidence – cornerstones of the telematics infrastrucutre
- Sound security measures, provide a secure platform for services
- Multiple mechanisms to achieve trust (e.g., different smartcards, certifications, Konnektor)
- Multiple layers of security
- X.509 vs. CVC
- Different security mechanisms in order to access medical data
- Backup of medical data
- Common Criteria Certifications
- ISMS, monitoring of devices and news/web

# Security Tests

- Complexity of systems increases test efforts
- Test environments only cover a subset of the features of the production environment
- Problems by testing in production environments
- Backward compatibility vs. new attack patterns leads to regular retests
- Test data vs. production data: certificates/private keys, configurations e.g. IP address, confidentiality of production data, ...

# Further Work – Working with the ESSE team

- Working as a tutor
- Taking part in CTF contests as part of ESSE's CTF team
  Defragmented Brains – `http://www.defbra.at/`
- Researching IT Security in Large IT Infrastructures
- Projects
- Seminar aus Security
- Diploma Thesis
- Thesis
- Sometimes in cooperations with external partners

# Thank you!

https://security.inso.tuwien.ac.at/