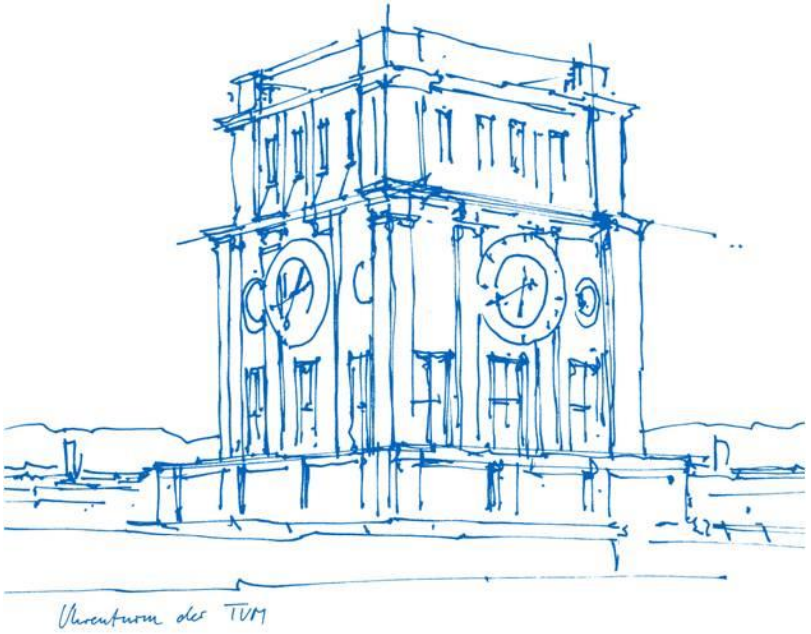
Accountability: A Cross-disciplinary View

Preliminary Meeting

Amjad Ibrahim

Ehsan Zibaei

Prof. Dr. Alexander Pretschner



Technische Universität München

Fakultät für Informatik

Lehrstuhl XXII für Software Engineering

Who we are

Prof. Dr. Alexander Pretschner
Since May 1st, 2012 heading Chair XXII (Software Engineering) @TUM
Room: MI – 01.11.058
Email: pretschn@in.tum.de

Amjad Ibrahim, M.Sc.
Room: MI - 01.11.059
Email: **ibrhaim@in.tum.de**

Ehsan Zibaei, M.Sc.
Room: MI - 01.11.055
Email: z**ibaei@in.tum.de**

http://www22.in.tum.de/teaching/accountabilityseminar/

Agenda for today

- Seminar theme
  - Goals
  - Possible Topics
- Road map
- Rules
- Dates

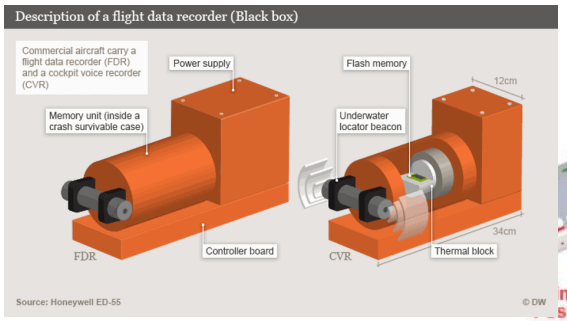
Introduction

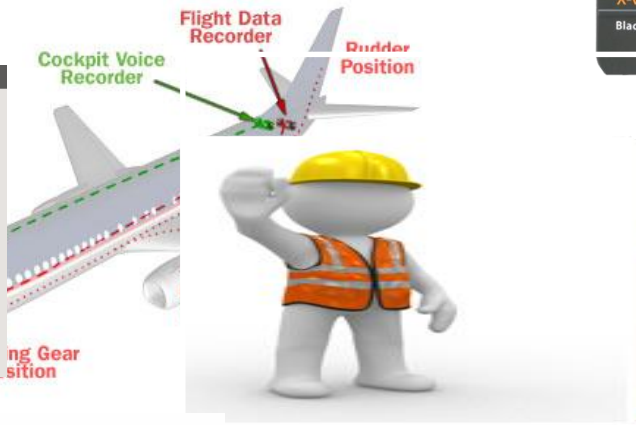
- “Hide it or lose it”!
- I did but “they” hacked it!

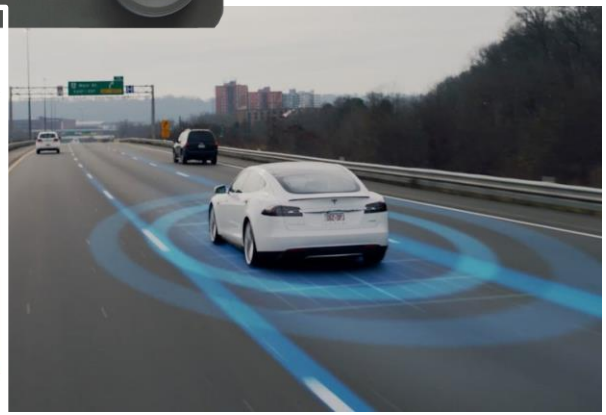
Accountability: a definition

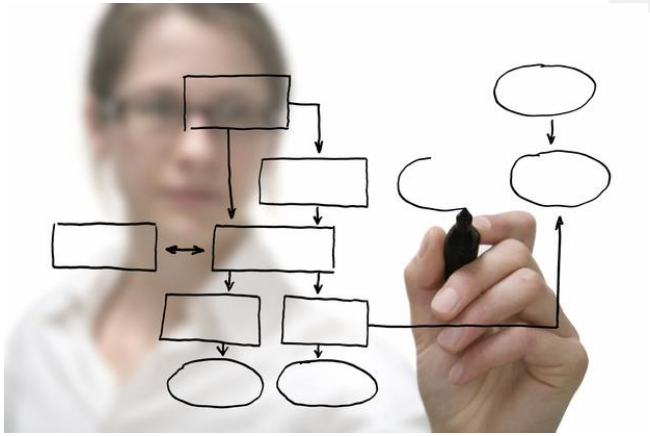
- “The capability of a system to answer **questions** concerning the why, how, by whom, where and when **specific events** have happened...” [Pretschner]
- ”A capability of a Socio-technical system to answer **questions** regarding the cause of occurred **unwanted events**” [Beckers et. al.]
- A ….. of a system that enables linking an unwanted behavior at run time to its possible cause.

Accountability: Where?





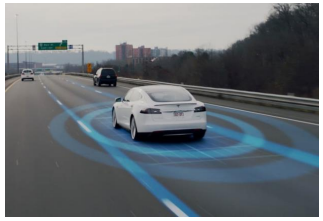




Accountability is cross-domain

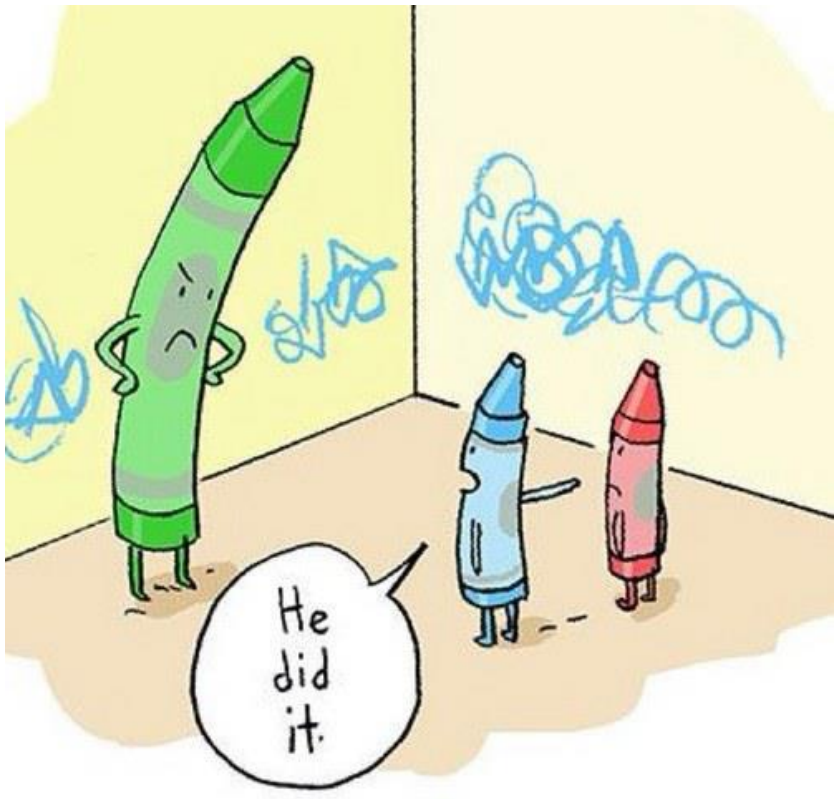
Accountability: why?

- Open platforms and marketplaces
  - On-boarding, off-boarding of services
- Cloud deployment model
  - Hosts
- Autonomous systems
  - Microservices
    - Make decisions
    - Act independently



Accountability: how?

- Establish link between behavior and the cause
  - System monitoring
  - Causality analysis



Accountability blocks

System Modeling

Evidence

Logs Pre-processing

Causality

Supporting

Accountability is cross-domain…

Related disciplines

- BlockChain
- Model checking
- Runtime verification (offline mode)
- Digital Forensics
- Log auditing
- Model based testing/analysis
- Intrusion detection systems
- Causality
- Fault localization and Delta debugging
- Accountability in Cyber-physical systems
- Anomaly detection

Seminar Literature

1. Accountability

a) Papanikolaou, Nick, and Siani Pearson. "A Cross-Disciplinary Review of the Concept of Accountability A Survey of the Literature." (2013).

b) Weitzner, D., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.: Information accountability, Communications of the ACM 51(6):82-87, 2008

c) Beckers, Kristian, Jörg Landthaler, Florian Matthes, Alexander Pretschner, and Bernhard Waltl. "Data Accountability in Socio-Technical Systems." International Workshop on Business Process Modeling, Development and Support. Springer International Publishing, 2016.

d) Pretschner, Alexander. "Achieving accountability with distributed data usage control technology." *The 2nd International Workshop on Accountability: Science, Technology and Policy at MIT*. 2014.

e) Feigenbaum, Joan, Aaron D. Jaggard, Rebecca N. Wright, and Hongda Xiao. Systematizing “Accountability” in Computer Science (Version of Feb. 17, 2012). YALEU/DCS/TR-1452, Yale University, New Haven, CT, 2012.

f) Kacianka, Severin, Florian Kelbert, and Alexander Pretschner. "Towards a Unified Model of Accountability Infrastructures." arXiv preprint arXiv:1608.07882 (2016).

Seminar Literature (continued)

2. Causality

a) Gössler, G., Le Métayer, D.: A General Trace-Based Framework of Logical Causality. [Research Report] RR-8378, 2013.

b) Halpern, J., Pearl, J.: Causes and Explanations: A Structural-Model Approach. Part I: Causes. arXiv:cs/0011012v3 [cs.AI] 7, 2005

3. Model checking

a) Clarke, Edmund M., Orna Grumberg, and Doron Peled. Model checking. MIT press, 1999.

b) Baier, Christel, Joost-Pieter Katoen, and Kim Guldstrand Larsen. Principles of model checking. MIT press, 2008.

c) Visser, Willem, Klaus Havelund, Guillaume Brat, SeungJoon Park, and Flavio Lerda. "Model checking programs." Automated Software Engineering 10, no. 2 (2003): 203-232.

d) (Survey) Ranjit Jhala and Rupak Majumdar. 2009. Software model checking. ACM Comput. Surv. 41, 4, Article 21 (October 2009), 54 pages. DOI=http://dx.doi.org/10.1145/1592434.1592438

Seminar Literature (continued)

4. Runtime verification

a) Leucker, Martin, and Christian Schallhart. "A brief account of runtime verification." The Journal of Logic and Algebraic Programming 78, no. 5 (2009): 293-303.

b) Andreas Bauer, Martin Leucker, and Christian Schallhart. 2011. Runtime Verification for LTL and TLTL. ACM Trans. Softw. Eng. Methodol. 20, 4, Article 14 (September 2011), 64 pages. DOI=http://dx.doi.org/10.1145/2000799.2000800

c) Falcone, Ylies, Jean-Claude Fernandez, and Laurent Mounier. "Runtime verification of safety-progress properties." In International Workshop on Runtime Verification, pp. 40-59. Springer Berlin Heidelberg, 2009.

5. Digital Forensics

a) Garfinkel, Simson L. "Digital forensics research: The next 10 years." digital investigation 7 (2010): S64-S73.

b) Casey, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.

c) Reith, Mark, Clint Carr, and Gregg Gunsch. "An examination of digital forensic models." International Journal of Digital Evidence 1, no. 3 (2002): 1-12.

d) Freiling, Felix C., and Bastian Schwittay. "A Common Process Model for Incident Response and Computer Forensics." citeseerx.ist.psu.edu/viewdoc/download

Seminar Literature (continued)

6. Log auditing/ minning

a) Roger, Muriel, and Jean Goubault-Larrecq. "Log auditing through model-checking." In Proceedings of the 14th IEEE workshop on Computer Security Foundations, p. 220. IEEE Computer Society, 2001.

b) Iváncsy, Renáta, and István Vajk. "Frequent pattern mining in web log data." Acta Polytechnica Hungarica 3, no. 1 (2006): 77-90.

c) van Aalst, Wil MP, Kees M. van Hee, Jan Martijn van Werf, and Marc Verdonk. "Auditing 2.0: using process mining to support tomrrow's auditor." Computer 43, no. 3 (2010): 90-93.

7. Delta debugging and Fault localization

a) Ghassan Misherghi and Zhendong Su. 2006. HDD: hierarchical delta debugging. In Proceedings of the 28th international conference on Software engineering (ICSE '06). ACM, New York, NY, USA, 142-151. DOI=http://dx.doi.org/10.1145/1134285.1134307

b) Andreas Zeller. 2002. Isolating cause-effect chains from computer programs. In Proceedings of the 10th ACM SIGSOFT symposium on Foundations of software engineering (SIGSOFT '02/FSE-10). ACM, New York, NY, USA, 1-10. DOI=http://dx.doi.org/10.1145/587051.587053

Seminar Literature (continued)

8. Model based testing/analysis

a) Apfelbaum, Larry, and John Doyle. "Model based testing." In Software Quality Week Conference, pp. 296-300. 1997.

b) Pretschner, Alexander. "Model-based testing." In Proceedings. 27th International Conference on Software Engineering, 2005. ICSE 2005., pp. 722-723. IEEE, 2005.

c) Arilo C. Dias Neto, Rajesh Subramanyan, Marlon Vieira, and Guilherme H. Travassos. 2007. A survey on model-based testing approaches: a systematic review. In Proceedings of the 1st ACM international workshop on Empirical assessment of software engineering languages and technologies: held in conjunction with the 22nd IEEE/ACM International Conference on Automated Software Engineering (ASE) 2007 (WEASELTech '07). ACM, New York, NY, USA, 31-36. DOI=http://dx.doi.org/10.1145/1353673.1353681

9. Intrusion detection systems

a) Hervé Debar, Marc Dacier, Andreas Wespi, Towards a taxonomy of intrusion-detection systems, Computer Networks, Volume 31, Issue 8, 23 April 1999, Pages 805-822, ISSN 1389-1286, dx.doi.org/10.1016/S1389-1286(98)00017-6.

b) Debar, Hervé, Marc Dacier, and Andreas Wespi. "A revised taxonomy for intrusion-detection systems." In Annales des télécommunications, vol. 55, no. 7-8, pp. 361-378. Springer-Verlag, 2000.

Seminar Literature (continued)

10. Accountability in cyber-physical systems

a) Datta, Anupam, et al. "Accountability in cyber-physical systems." Cyber-Physical Systems Workshop (SOSCYPS), Science of Security for. IEEE, 2016.

b) M. C. Tschantz, A. Datta, J. M. Wing, "Information flow investigations", Tech. Rep. 2013 CMU-CS-13–118.

c) M. C. Tschantz, A. Datta, A. Datta, J. M. Wing, "A methodology for information flow experiments", IEEE 28th Computer Security Foundations Symposium CSF 2015, pp. 554-568, 13–17 July, 2015

11. Anomaly detection

a) Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM computing surveys (CSUR) 41, no. 3 (2009): 15.

b) Jones, Austin, Zhaodan Kong, and Calin Belta. "Anomaly detection in cyber-physical systems: A formal methods approach." Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on. IEEE, 2014.

c) Emmott, Andrew F., et al. "Systematic construction of anomaly detection benchmarks from real data." Proceedings of the ACM SIGKDD workshop on outlier detection and description. ACM, 2013.

d) Gavrilovski, Alek, et al. "Challenges and Opportunities in Flight Data Mining: A Review of the State of the Art." AIAA Infotech@ Aerospace. 2016. 0923.

Seminar Goals

- Understanding with respect to accountability
- Critical reading and understanding
- Comparing
- Classification
- Writing an exposé
- Presentation skills

Task Overview

- Independent work
  - Read and understand concepts
  - Look for papers/material beyond the initial suggestions
    - E.g. Academic publication portals, TUM library etc.
    - No Wikipedia! (Except if a source is picked – discuss with the supervisor)
    - No blogs!
- Discuss with your colleagues
- Talk with your supervisor whenever required

Roadmap

- Topic selection
- Literature review
- Intermediate submission
- Peer review
- Final submission 50 %
- Talks/Presentation 50 %

Administrative

- Master Seminar
- Maximum participants: 10
- Registration
  - Via matching.in.tum.de
  - From February 3rd – 8th
  - Do you want to be our preference?

Registration

- Choose 3 topics from the list (after matching)
  - Mail Ibrahim@in.tum.de latest by 1st March, 2017
  - Order of preference - 1 highest, 3 lowest
  - Include - Full name, IMAT number, TUM email ID
- Get a topic by email after end of matching round

Thanks!

Rules

- Grading
  - Intermediate submission
    - Table of contents
    - Extended abstract
    - Bibliography
  - Exposé (50%) + Presentation (50%)
  - Penalty for all late submissions

- In case of any issues (E.g. can’t find a paper)
  - Google
  - Ask your colleagues
  - Write to your supervisor

Rules

- Compliance with the prescribed deadlines
- Compliance with all templates
- Presence in all meetings
- Participation in the final presentations in a two (or three) day block-seminar

Intermediate Submission

- Ca. 2 pages

- Extended abstract
  - Introduction
  - Problem statement and goals
  - Short description of content of each subsection
  - Description of your own contribution/critique

- Bibliography

Exposé

- Max. 15 pages including appendix, LNCS format

- No plagiarism!
  - blatant copy-paste, summarizing others' ideas/results without reference etc. will result in immediate expulsion from the course.

- Discussion of own contribution
- Complete bibliography
- Appendix, if needed

Content

- Don’t deviate from allotted topic
- Logical and contradiction-free reasoning
- Argue with proper sources
- If any contradictions in the source paper, don’t hide them.

Content

- Clear distinction between scientific facts and own logical conclusion
  - E.g. if something is “good” according to you, why?
  - Proper references

- Language
  - Easy to understand, simple (and short) sentences
  - Precise
  - Sensible titles
  - Sensible paragraphing

Content

- Tables and pictures
  - Cite sources
  - Must not be blurry
  - Large enough to be read in print
  - Must be referenced in text
  - Consistent numbering
- Bibliography
  - Must be referenced in text
  - Consistent numbering
  - Citation must include - Authors' names, title, year of publication, venue (or publisher)

Possible Structure

- Title & abstract
- Introduction
- Topic content
- Results
- Related work
- Discussion & conclusion
- Bibliography
- Appendix

Presentation

- Ca. 30 minutes of talking
  - Clear, linear storyline.
  - Must match the exposé, but should not be a text dump
  - Possibility of discussing slides with supervisor

- Ca. 10 minutes of discussion
  - Be prepared for questions on the topic
  - Ask questions on the presented topic

Finding Literature

- TUM Library
  - Informatik
  - Others…

- Online portals
  - Springer (www.springerlink.com/)
  - ACM (dl.acm.org/)
  - IEEE (ieeexplore.ieee.org/Xplore/guesthome.jsp)
  - Google Scholar (scholar.google.com)
  - Scopus (scopus.com)

Important Dates

- Intermediate submission deadline: TBA
- Submission deadline for first exposé draft: TBA
- Discussion (paper+slides) with supervisor and revision: TBA
- Exposé submission deadline: TBA
- Receive peer's paper for review: TBA
- Peer review deadline: TBA
- Camera ready deadline (paper+slides): TBA
- All documents must be submitted as PDF-files
- After submission of the slides, individual appointments for feedback for all students
- Block-seminar date(s). TBA.