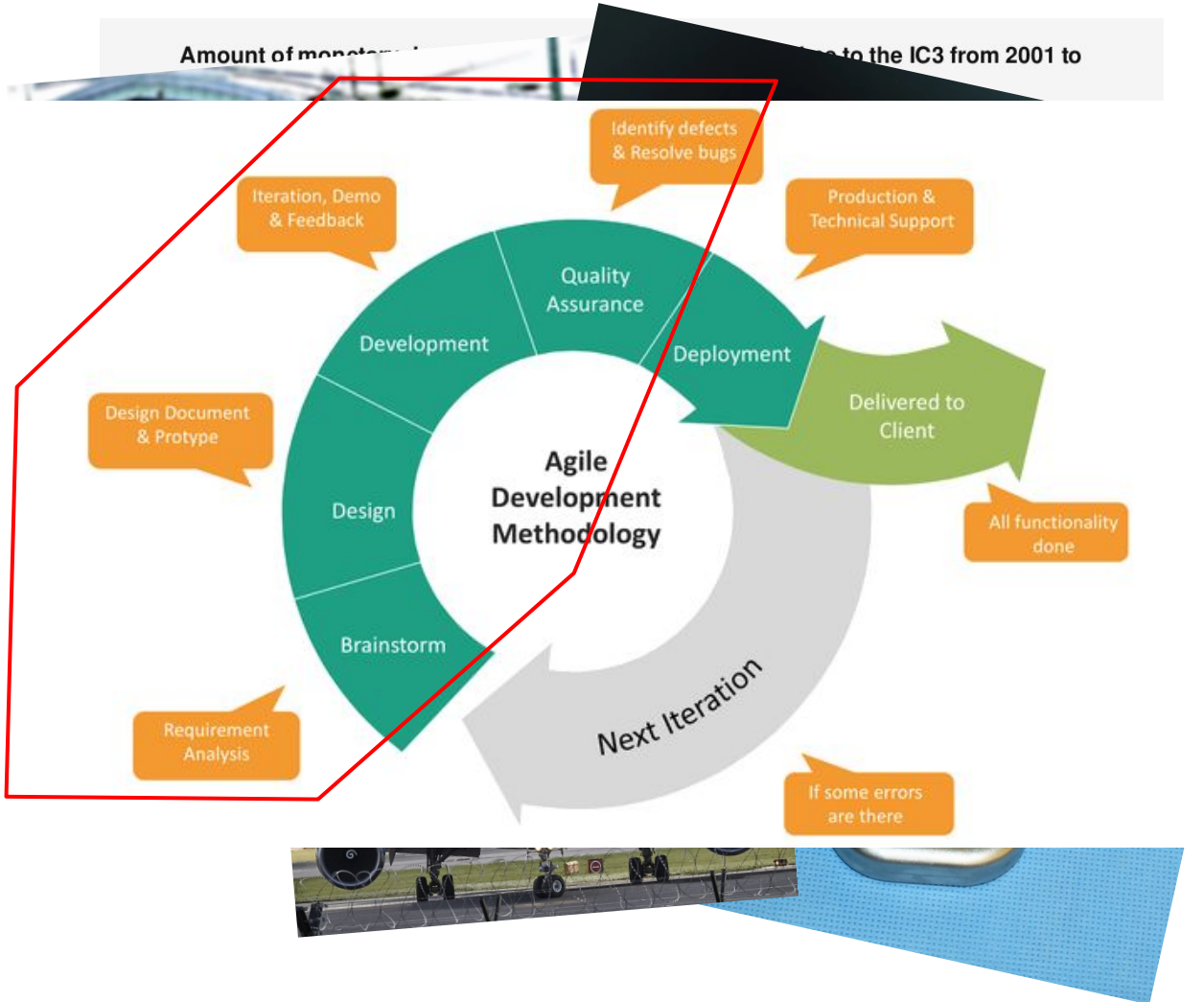
Security and Verification

seminar pre-course meeting

Maximilian Weininger ● Julia Eisentraut ● Jan Kretinsky

Why?

- cyber security is crucial for modern society
- formal methods and verification are a way to provide rigorous answers whether systems are secure
- need to take cyber security into account - from the first draft of the system until the final execution



Formal Methods (FM) - Survey

What FM is good at

- providing structured way to brainstorm on general structure of system
- designing, documenting and prototyping in a formal manner
- automatically checking whether design & prototype meet specification
- automatically identify bugs and executions violating specification

What FM is not so good at

- detecting unknown bugs/security issues
- detecting problems not modeled

Formal Methods for Security

Frankfurt shuts down IT network following Emotet infection

Frankfurt city officials take down IT network to prevent Emotet to be used as a staging point to launch a ransomware attack.

www.zdnet.com

long known trojan

→ problem stems from insufficient implementation of **known** security measures

December 2015 Ukraine power grid cyberattack

From Wikipedia, the free encyclopedia

The **December 2015 Ukraine power grid cyberattack** took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers.

en.wikipedia.org

phishing mails used to access system

→ **human behavior** crucial

Schedule

- First meeting (~20.04.): introduction and scheduling
- Second meeting (TBD): teaser talks
- Final meetings (TBD, TBD): final presentations and discussions

In between: at least two meetings with your supervisor.

Grading

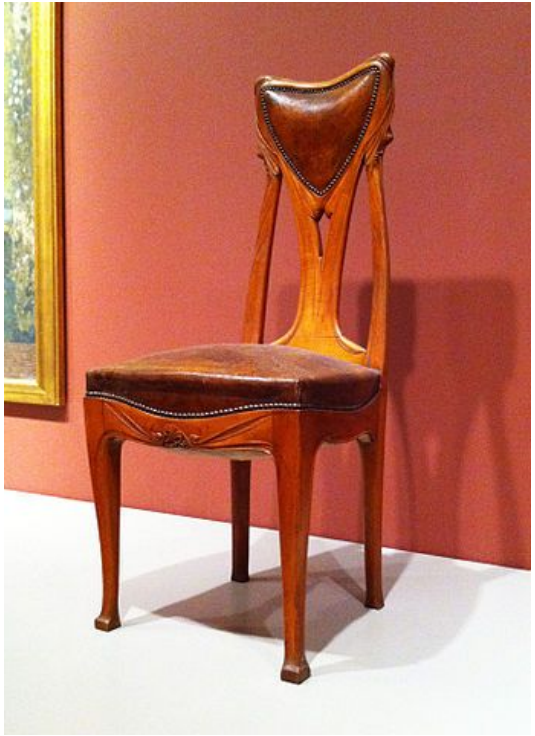
In the first meeting, you will receive the exact criteria, which we use to grade.

Your teaser talk is mandatory (you will fail the seminar if you don’t participate), however, we do not grade it. It is meant for you to receive feedback.

Your final grade will be determined from

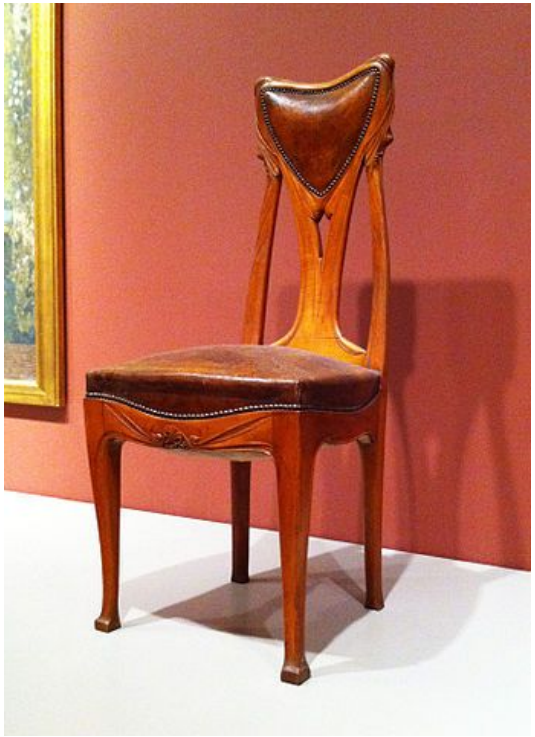
- written work (40%): extended abstract, 2-4 pages
- presentation (40%): talk of ~20min
- discussions (20%): participation, questions for the other talks, **chairing**

Chairing?



https://en.wikipedia.org/wiki/File:Side_Chair,_1900,_Hector_Guimard.jpg

Chairing?



https://en.wikipedia.org/wiki/File:Side_Chair,_1900,_Hector_Guimard.jpg

- Introducing speaker
- Timing of the talk
- Leading discussion

- Extended Abstracts ⟹ 2 Questions

Schedule

- First meeting (~20.04.): Introduction and Scheduling.
- Second meeting (TBD): teaser talks
- Read extended abstracts, send questions
- Final meetings (TBD, TBD): Presentations and discussions (be chair once)

In between: at least two meetings with your supervisor.

List of topics

We give you some papers as pointers. You do not need to stick to these papers if you see fit. In boldface, you find the broader topic of the talk if you want to explore the topic further.

- Attack Trees - **Basic Attack Modelling**
  - Attack Trees, B.Schneier
  - Foundations of Attack Trees, S. Mauw, M. Oostdijk
- Attack Graphs - **Identifying all Ways to Attack**
  - Automated Generation and Analysis of Attack Graphs, O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing
  - Scenario Graphs and Attack Graphs. O. Sheyner
- Attack Fault Trees - **Verifying Safety and Security at once**
  - Quantitative Security and Safety Analysis with Attack-Fault Trees, Rajesh Kumar, Mariëlle Stoelinga
- Attack Defense Trees - **Security Analysis with several parties**
  - Foundations of Attack-Defense Trees, Barbara Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer

List of topics (continued)

- Zoo of Stochastic Timed Automata and Sub Models - **Semantics**
  - As introduced here: http://www.modestchecker.net/
- Security Automata - **Enforcing Security Policies**
  - Enforceable Security Policies, Fred B. Schneider
- ADVISE - **Quantitative Attack Analysis**
  - Model-based security metrics using adversary view security evaluation (advise), Elizabeth LeMay, Michael D Ford, Ken Keefe, William H Sanders, Carol Muehrcke
- **Verifying Security Protocols**
  - Security protocol verification: symbolic and computational models, Bruno Blanchet
  - Automated verification of remote electronic voting protocols in the applied pi-calculus, M Backes, C Hritcu, M Maffei
- **Security Analysis of Smart Contracts**
  - A Semantic Framework for the Security Analysis of Ethereum Smart Contracts, Ilya Grishchenko, Matteo Maffei, Clara Schneidewind
- Attack Defence Diagram - **Analyse the Timing of Attacks**
  - The Value of Attack-Defence Diagrams, Holger Hermanns, Julia Krämer, Jan Krčál, Mariëlle Stoelinga

Next steps

- If you want to participate
  - Send mail with topics and motivation.
  - Prefer us in matching system.
- If you want to dive even deeper into verification and security
  - Checkout bachelor & master theses
  - Checkout this project:

    https://softwarecampus.de/en/project/prosec-proven-security-for-systems-with-human-interaction/

    we offer jobs!
- Else
  - Done.