Knowledge Reuse: From Threat to Causal Models and Back!

Preliminary Meeting

Amjad Ibrahim
Prof. Dr. Alexander Pretschner

Technische Universität München
Fakultät für Informatik
Informatik 4 - Lehrstuhl für Software und Systems 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

http://www22.in.tum.de/teaching/causal-modeling/
Agenda for today

- Seminar theme
- Goals
- Possible Topics
- Road map
- Rules
- Dates
Accountability: how?

- Establish link between behavior and the cause
- System monitoring
- Causality analysis
Oh, crap! Was that TODAY?
Counterfactual Causality

**Actual World**
- X does occur
- Y does occur

**Possible World**
- X does not occur
- Y does not occur

X causes Y: **But-for test**
Causal Models

- Signature: $S=(U, V, R)$
  - $U$: Set of exogenous variables
  - $V$: Set of endogenous variables
  - $R$: Associates with each variable a set of possible values
- Causal Model: $M=(S, F)$
  - $F$: Associates a function $F_X$ with each $X \in V$
    In words: "$F_X$ tells us the value of $X$ given the values of all other variables in $U \cup V$"
  - Visualization via Causal Networks
Rock-Throwing Example

- **ST/BT** = Billy/Suzy throws
- **SH = ST** (Suzy hits)
- **BH = BT \land \neg SH** (Billy hits)
- **BS = SH \lor BH** (Bottle shatters)

The real world:
- **ST = BT = 1**
- **SH = ST = 1**
- **BH = BT \land \neg SH = 1 \land 0 = 0**
- **BS = SH \lor BH = 1 \lor 0 = 1**
Threat Modeling: Expose Master Key

- Steal_Master_Key
  - Decrypt_The_Key
  - Steal_Decrypted

Assets
- Documents
- Keys
- Logs
Causal Modeling

- Causality is model relative
  - Variable selection
  - Syntax and semantics
- The idea: reuse DAG-based attack modeling
  - 31 different models: attack/Fault trees, attack graphs, Bayesian networks..
  - Used by engineers and scientists
  - Intuitively, visually representing attack paths for managers
  - Engineers build their countermeasures based on it
  - Formal analysis quantitative and qualitative
  - Tool support
  - Some encodes the causal relation already
- Attack tree maps to causal models
  - Acyclic
  - Boolean
  - Probabilities
Possible Topics

Causal modeling +
- Tree Modeling
- Bayesian Networks in security
- Safety Models
- Attack Graphs Generation
- Domain Specific Language for the model generation
- Graph Transformation Systems
- A theory of malicious insiders
- Attack tree generation
- Business Process models
Seminar Goals

- 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: 12

Registration

- Via [http://docmatching.in.tum.de/](http://docmatching.in.tum.de/)
- From 09.02. to 14.02.18
- 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, 2018
  - 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
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
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)