MASTER SEMINAR WS16/17

PROF. DR. ALEXANDER PRETSCHNER
SAAHIL OGNAWALA

FUZZING FOR VULNERABILITY DETECTION

WHO WE ARE

Prof. Dr. Alexander Pretschner

Head of Chair XXII – Software Engineering @TUM
since May 1st, 2012

Saahil Ognawala

Office: MI - 01.11.041

Email: ognawala@in.tum.de

Our website: http://www22.in.tum.de/

FUZZING (OR FUZZ TESTING) FOR VULNERABILITY DETECTION

- Introduction to fuzzing
  - Popular software testing technique
  - Fast, automated, coverage driven
  - Variety of domains
    - command line, GUI, mobile, web-apps etc.
- Seminar homepage
  - http://www22.in.tum.de/en/fuzz-testing-seminar/

GOAL

- Understanding with respect to fuzzing
  - Concepts of pure fuzzing
  - How are input mutations performed?
  - How is whitebox fuzzing different from blackbox fuzzing?
  - How can whitebox information be used to enhance fuzzing?
  - Advanced techniques and target-specific implementations
- Others
  - Critical reading and understanding
  - Summarizing
  - Classification
  - Writing an exposé
  - Presentation skills

OVERVIEW OF FUZZING

- Start testing with “seed inputs”
- Observe (record) program behaviour
  - Blackbox
- Change input (flip-bits, XOR, etc.) and test again
- New program behaviour?
  - SUCCESS!

OVERVIEW OF FUZZING

- Variant of random testing
  - Input mutation, instead of random sampling.
  - Basic fuzzers mutate inputs randomly.
- Automation is the key!
  - *"~~Move~~ Mutate fast, break things"*
  - Dependant only on (input,output)
  - High path coverage* due to lots of testing rounds

**highly subject to conditions*

TASKS OVERVIEW

- Independent work
  - Read and understand concepts
  - Look for papers/material beyond the initial suggestions
    - Eg. Academic publication portals, TUM library etc.
    - NO Wikipedia! (Except if a source is picked - discuss with the supervisor)
    - NO blogs!
- Discuss with your colleagues
- Regularly get (and hopefully incorporate) reviews on your drafts from your supervisor.
- Talk with your supervisor whenever required (use this power judiciously)

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

RULES

- Grading
  - Intermediate submission (~~0.3 grade point bonus*~~ mandatory!)
    - Table of contents
    - Extended abstract
    - Bibliography
  - Exposé (50%) + Presentation (50%)
  - Penalty for all late submissions
- In case of any issues (eg. can’t find a paper)
  - Google
  - Ask your colleagues
  - Write to the Saahil Ognawala

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
  - Eg. 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: 31st October, 2016
- Submission deadline for first exposé draft: 28th November, 2016
- Discussion (paper+slides) with supervisor and revision: 5th Dec. - 19th Dec. 2016
- Exposé submission deadline: 3rd January, 2017
- Receive peer's paper for review: 6th January, 2017
- Peer review deadline: 13th January, 2017
- Camera ready deadline (paper+slides): 20th January, 2017
- All documents must be submitted as PDF-files
- After submission of the slides, individual appointments for feedback for all students
- Block-seminar date(s) during the end of January. TBA.

REGISTRATION

- Matching system: http://docmatching.in.tum.de/
- Choose 3 topics from the list
  - Mail ognawala@in.tum.de latest by Thursday, 30th June, 2016
    - 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

OVERVIEW OF TOPICS

- Blackbox testing with fuzzing
- Blackbox vs. whitebox fuzzing
- Advanced fuzzing strategies with whitebox optimizations
- Input mutation strategies in fuzzing
- Role of machine learning in fuzz testing
- Role of genetic algorithms in fuzz testing
- Compositional analysis of large-scale software with fuzzing
- Vulnerability discovery in mobile applications
- Vulnerability discovery in web applications
- File format and protocol fuzzing
- ….or agree upon a topic with the supervisor….

ognawala@in.tum.de

THANK YOU