Kick-off Seminar: Intrusion Detection Systems

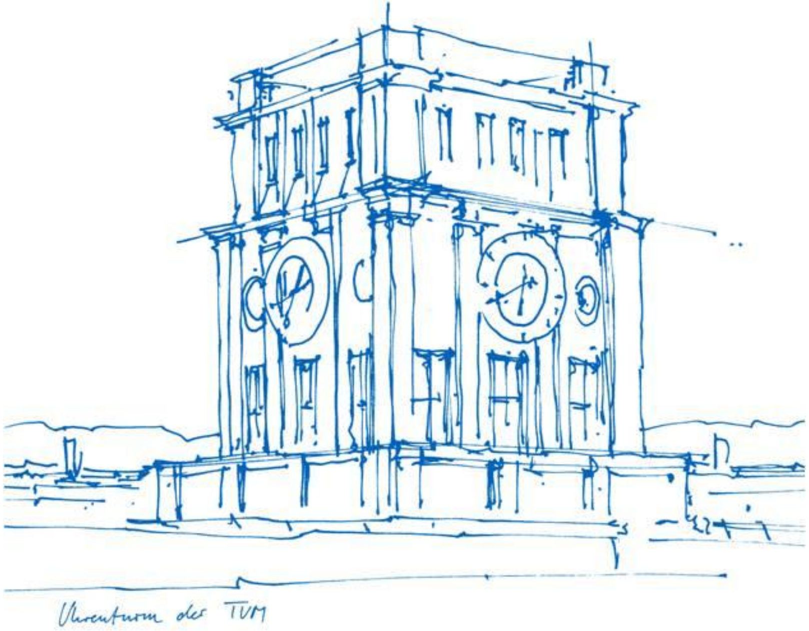
Mohammad Reza Norouzian

Technische Universität München

Fakultät für Informatik

Lehrstuhl für IT Sicherheit

29.01.18



Outline

- Organization
- Goal of Seminar
- Seminar Topics
- Prerequisites
- Student Assignments
- Literature Research
- Grading
- Time Table
- How to Apply

Organization

- Familiarize with the research topic (Intrusion Detection Systems)
- Literature research in your topic
- Deep into your individual topic
- Students Talk

Goal of Seminar

- Learn how IDSs detect malicious activities
- Another look at NIDSs with high cost of errors
- How to address the challenges in NIDS
- Use machine learning to solve some challenges
  - Detection
  - Analysis
  - Making conclusions, countermeasures

Seminar Topics

- Network Intrusion Detection Systems (NIDS)
  - Machine Learning based
  - Signature based
  - Hybrid based
- IDS for Industrial Control System (ICS)
  - e.g. Stuxnet, Havex, Industroyer, APT attacks
- Feature Selection in NIDS

Prerequisites

- MSc students of Informatics or similar
- Basics of IT security
- Machine Learning/Data Mining – very beneficial
- English speaking skills :)

Student Assignments

- Presentation (1 paper) + Report (1+1 papers)
- Pick **2 papers** from the list (which will be published later in the course homepage[1]), or propose papers
- 1 paper used for a seminar presentation (20' + 10‘ discussion)
- Write a report about **both papers** (14 pages LNCS format)
- You have to write the report on your own words, direct copy and paste will be determined as a plagiarism!

[1] - *https://www.sec.in.tum.de/i20/teaching/ss2018/intrusion-detection-systems*

Literature Research

- Students highly recommend to search similar literature for their report and specially their **talk paper**
- Goal of relevant literatures:
  - Find, understand, explain main:
    - Arguments
    - Approaches
    - Techniques

Literature Research & Sources

- http://scholar.google.com/
- http://dblp.uni-trier.de/
- http://citeseer.ist.psu.edu/
- http://portal.acm.org/
- http://www.springerlink.com/
- http://www.computer.org/
- You can access to the majority of literatures by Shibboleth Authentication or using Library webpage:
    - https://eaccess.ub.tum.de

Grading

- Grading consist of different parameters:
- Report (60%)
- Presentation (30%)
- Participation and discussion (10%)
  - Almost neglected!

Time Table

- 29.01.18 – Kick-off Meeting
- 17.04.18 – Introduction, Rules and Division of papers
- 05.06.18 – Students Presentation
- 12.06.18 – Students Presentation
- 19.06.18 – Students Presentation
- 26.06.18 – Students Presentation
- 03.07.18 – Students Presentation
- 10.07.18 – Students Presentation

How to Apply?

- Attend the Kick-Off
- Send a short CV to:
    - norouzian@sec.in.tum.de until **07.02.17**
- Register on the matching system
    - look up http://docmatching.in.tum.de/
- If you cannot use the matching system for some reason, let me know!

Contact

- For any questions, ask now or contact me later:
  - norouzian@sec.in.tum.de