Kick-off Seminar: Intrusion Detection Systems

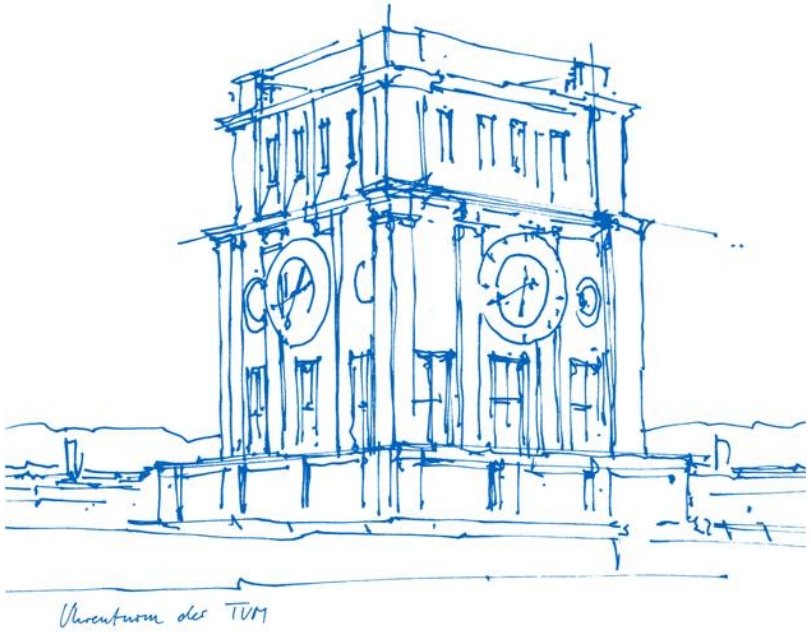
Mohammad Reza Norouzian

Technische Universität München

Fakultät für Informatik

Lehrstuhl für IT Sicherheit

04.02.21



Outline

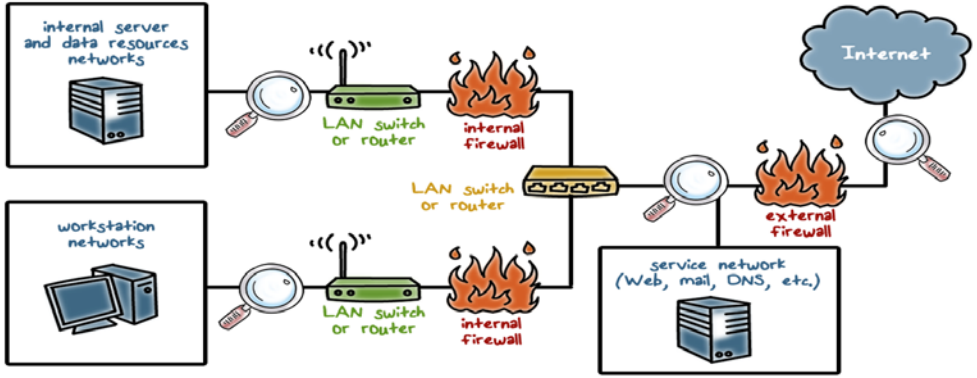
- Definition of Intrusion Detection
- Organization
- Goal of Seminar
- Seminar Topics
- Prerequisites
- Student Assignments
- Literature Research
- Grading
- Timetable
- How to Apply

What's An Intrusion?

- Successful attack is usually (but not always) associated with an access control violation
  - A buffer overflow has been exploited; now the code is being executed inside a legitimate program
  - Outsider gained access to a protected resource
  - A program or file has been modified
  - System is not behaving "as it should"
- The goal of an intrusion detection system (IDS) is to detect that bad things are happening (intrusion)
  - Just as they start happening (hope so)
  - How is this different from a firewall?

Intrusion Detection Styles

- Misuse detection
  - Precise descriptions of known malicious behavior



- Anomaly detection
  - Have a notion of normal activity and flag deviations from that profile
- Specification-based detection
  - Defining allowed types of activity in order to flag any other activity as forbidden.

Detection Styles in Actual Deployments

- Striking imbalance deployments:
  - Almost exclusively only misuse detectors in use
  - Detect signatures (characteristic byte sequences)
- However, anomaly detection is extremely appealing!
  - Promises to find novel attacks
  - Machine learning works so well in other domains
- But it’s hard to find any machine learning NIDS in real-world deployments, why?

Organization

- Familiarize with the research topic (Intrusion Detection Systems)
- Related works research in the Individual assigned topic
- Deep into the 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 systems (ICS)
  - e.g., Stuxnet, Havex, Industroyer, APT attacks
- Adversarial learning in NIDS use cases

Prerequisites

- Master students of Informatics or similar
  - Bachelor students are welcome too!
- Basics of IT security
- Machine learning - very beneficial
- English speaking and writing skills :)

Student Assignments

- Report + Presentation + Experiments (not mandatory)
- Pick a topic from the proposed list or propose papers
- Present **one or both** papers (30‘ + 15‘ discussion)
- Write a report on **both papers**
  - At least **10** pages **IEEE** template[1], excluding sources and appendix
- You must 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/ss2021/intrusion-detection-systems

Literature Research

- Students highly recommend studying similar literatures for their report and specially for their **presentation**
- Goal for relevant literatures:
  - Find, understand and 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 consists of different parameters:
  - Report: **50%**
  - Presentation: **40%**
  - Participation and discussion: **10%**
    - Almost neglected!
  - Implementation / Experiments: **0.3** bonus

Timetable

- 04.02.21 – Kick-off meeting
- 13.04.21 – Introduction to the seminar
- 18.05.21
- 25.05.21
- 01.06.21
- 08.06.21
- 15.06.21

How to Apply?

- Attend the kick-off
- Send a short CV or motivation latter to:
  - norouzian@sec.in.tum.de until **16.02.21**
- Register on the matching system
  - Look up http://docmatching.in.tum.de/
- If you cannot use the matching system for some reasons, let me know!

Contact

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