Introduction

Advanced Internet Security

Adrian Dabrowski, Aljosha Judmayer,
Christian Kudera, Georg Merzdovnik

Aim of the Lecture

- Advanced Internet Security serves as a continuation for the lecture Internet Security
- The lecture deals with common errors and vulnerabilities as well as ways to detect and avoid them
- In order to teach the subject in the most authentic way, the lecture uses an “offensive approach”
  - Security-related topics are viewed from an attacker’s perspective and possible attack scenarios are shown
  - In practical challenges the students need to exploit vulnerabilities inside a controlled challenge-environment

Topics

- Malware
- Mobile Security (Android security concepts)
- Hardware-Software Co-attacks (Timing side channels, Cache attacks, Spectre, Meltdown, Rowhammer)
- IoT Security (Embedded Systems and Firmware)
- Hardware Security (Hardware Analysis and Attacks)
- Binary Analysis (Fuzzing, Instrumentation, Tainting, Symbolic Execution)
- Advanced Memory Corruption
- Advanced Cryptography
- Windows Security

Targeted Audience

- Prerequisites:
  - Understanding of security fundamentals (e.g. as offered by Internet Security VU or equivalent)
  - Good programming/developing skills (C knowledge is advantageous)
  - Some experience with Linux and Windows
  - Time – You will need to solve a minimum of 4 security challenges during the lecture!

- You should attend this lecture, if you ...
  - ... are deeply interested in security
  - ... are willed to solve hard and time-consuming challenges
  - ... are aspire to write your thesis with one of the lecturers

- You should **not** attend this lecture, if you ...
  - ... are hunting for easy credits
  - ... were struggling at solving the challenges from the Internet Security VU

People and Lecture time

- Cooperation between Vienna Seclab (E191) and SBA Research (E194)
- Lecturers:
  - Adrian Dabrowski
  - Aljosha Judmayer
  - Christian Kudera
  - Georg Merzdovnik
- Tutor:
  - Michael Pucher
- Lecture time:
  - Weekly lectures (Wednesday) are held in EI 8 Pötzl HS, 18:00 (s.t.) to 20:00

Contact

- If you have questions regarding the lab challenges, please use the TISS Forum to exchange yourself with other students
  - Our tutor is reading it on a daily basis and usually quick to answer with help
  - Please refrain from posting (partial) solutions, as you will spoil the fun for others

- If you think, you need help beyond that, send a mail to inetsec@seclab.tuwien.ac.at

New Lecture Mode

- There will be 7 challenges, whereas you will need to solve a minimum of 4 challenges
- There will be only one exam (**23.01.2019, 18:00 - 20:00**) at the end of the semester and no retake exams
- Final grade: 2/3 Challenges + 1/3 Exam
  - You can be positive without attending the exam ☺
- Final points [0, 100]:

$$\left(\frac{solved\_challenges}{7} * 100\right) * \frac{2}{3} + \left(\frac{exam\_points}{max\_exam\_points} * 100\right) * \frac{1}{3}$$

  - *solved_challenges* Number of challenges the student solved
  - *exam_points* Reached points at the exam
  - *max_exam_points* Maximum points reachable at the exam
- From the moment you submit your first solution for a challenge (whether right or wrong), a certificate will be issued

Grading


```python
from decimal import *
import math

LECTURE_CHALLENGES = 7  # example, may vary from semester to semester
LECTURE_EXAM_MAX_POINTS = 35   # example, may vary from exam to exam

def min_challenges_to_solve():
    return int(math.ceil((Decimal(LECTURE_CHALLENGES) / Decimal(2)) + Decimal(0.1)))

def grade(student_solved_challenges, student_exam_points):
    challenge_points = (Decimal(student_solved_challenges) / Decimal(LECTURE_CHALLENGES)) * \
        Decimal(100)
    exam_points = (Decimal(student_exam_points) / Decimal(LECTURE_EXAM_MAX_POINTS)) * \
        Decimal(100)

    sum_points = int(math.ceil((Decimal(2) * challenge_points + exam_points) / Decimal(3)))

    if sum_points <= 50 or student_solved_challenges < min_challenges_to_solve():
        return 5
    elif sum_points <= 63:
        return 4
    elif sum_points <= 75:
        return 3
    elif sum_points <= 88:
        return 2
    else:
        return 1

if __name__ == "__main__":
    # student solved 5 challenges and received 25 points on the exam
    print(grade(5, 25))
```

Lab Environment: SecEnv

- Environment:
  - Assignments can be solved at home or any computer with internet connection
  - The environment is remotely accessible via SSH
  - Accounts are created automatically (TISS registration until 10.10.2018, 15:00)
  - We will send your Lab credentials to your E-Mail registered in TISS – But only if your contact details are up-to-date ☺
  - Further details about the environment are described at the SecEnv web page: `https://secenv.seclab.tuwien.ac.at/environment`
    - This is ”Work in Progress” - Details will be finalised as soon as the challenges start

- Submission:
  - Hard deadlines with sufficient time (start early!)
  - automated checks with immediate feedback

Behind the Lecture

- Capture the Flag (CTF) Team: We_0wn_y0u
  - Capture the Flag (CTF) is a special kind of information security competition
  - We try to participate in online CTFs as often as possible
  - You can find further details about the team at the team's web page: `https://w0y.at`
  - Georg Merzdovnik and Michael Pucher are going to give you an introduction on CTFs and our team at the lecture on 17.10.2018

- Praktika, Bachelor theses, Master theses
  - We are always interested in students who are motivated to work with us on security projects
  - If you are interested, contact us: inetsec@seclab.tuwien.ac.at
  - We are able to provide you with a topic, but we are also open minded for your suggestions

Conclusion

We hope you are interested!