MUNI
C4E

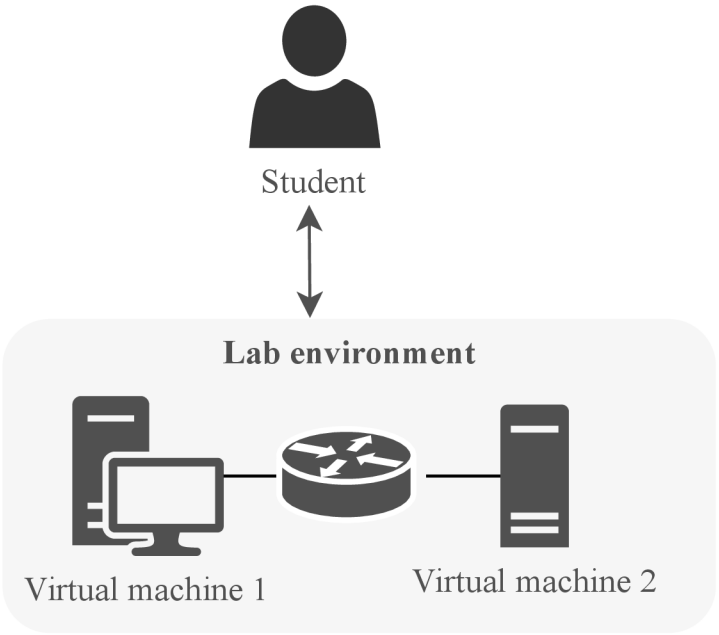
Preventing Cheating in Hands-on Lab Assignments

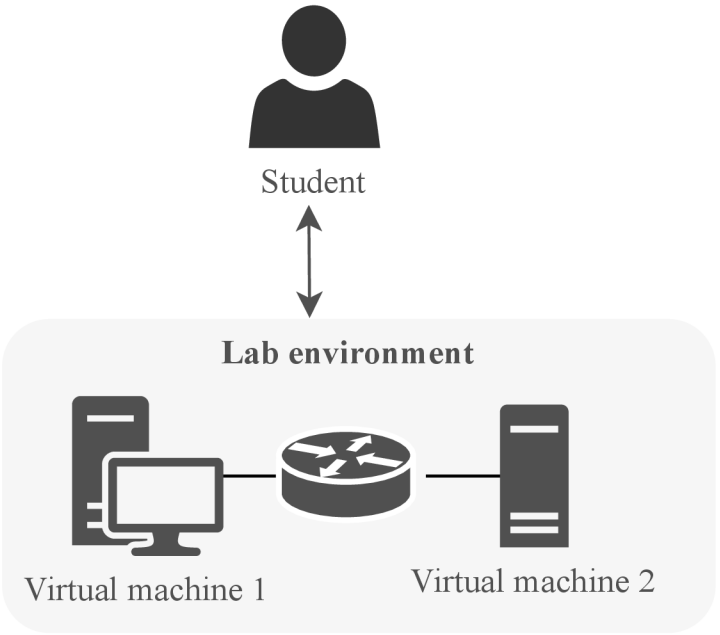
Jan Vykopal, Valdemar Švábenský, Pavel Seda, Pavel Čeleda

Masaryk University, Brno, Czech Republic

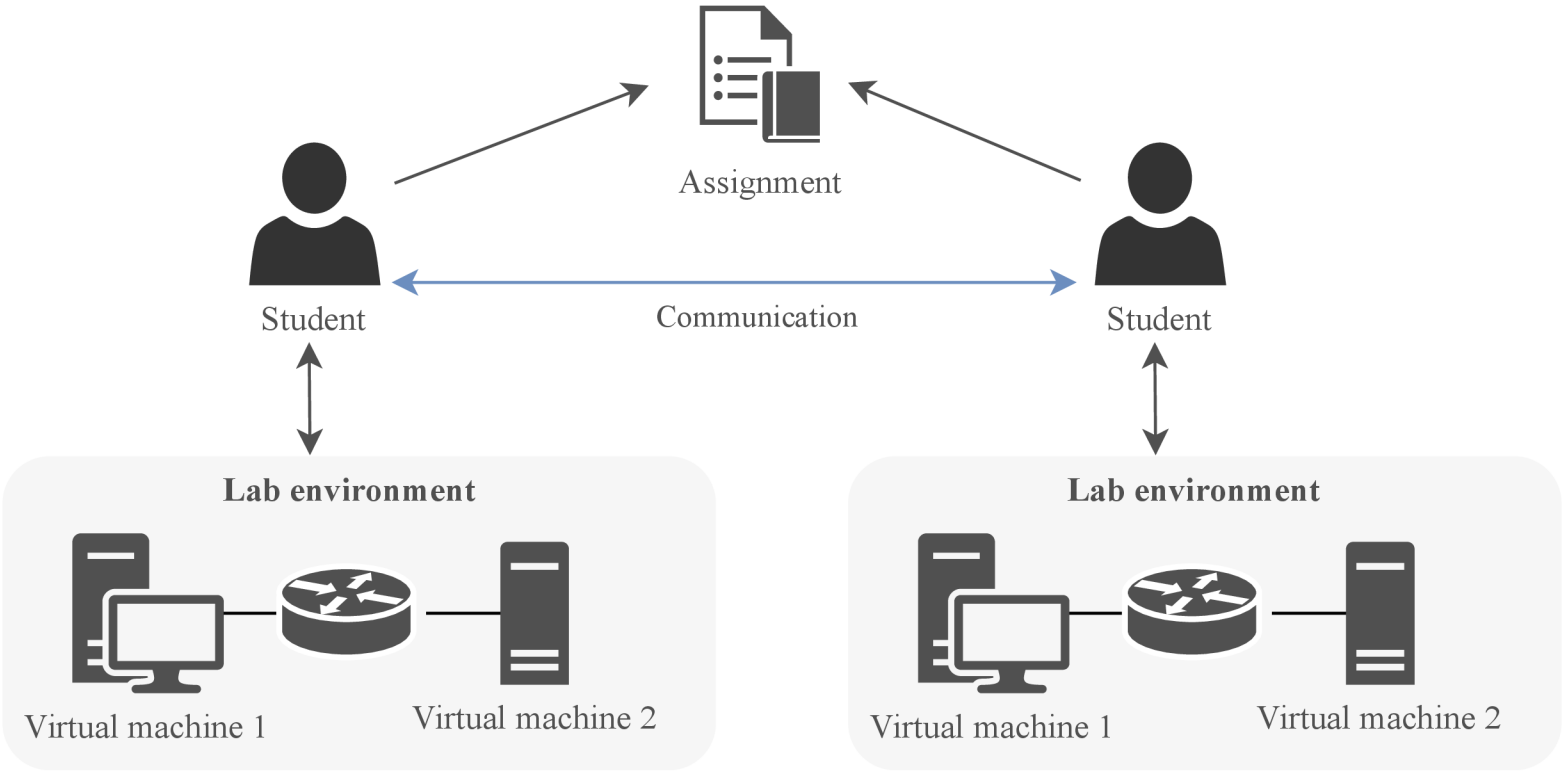
March 2022 | ACM SIGCSE Technical Symposium

Format of Hands-on Cybersecurity Classes



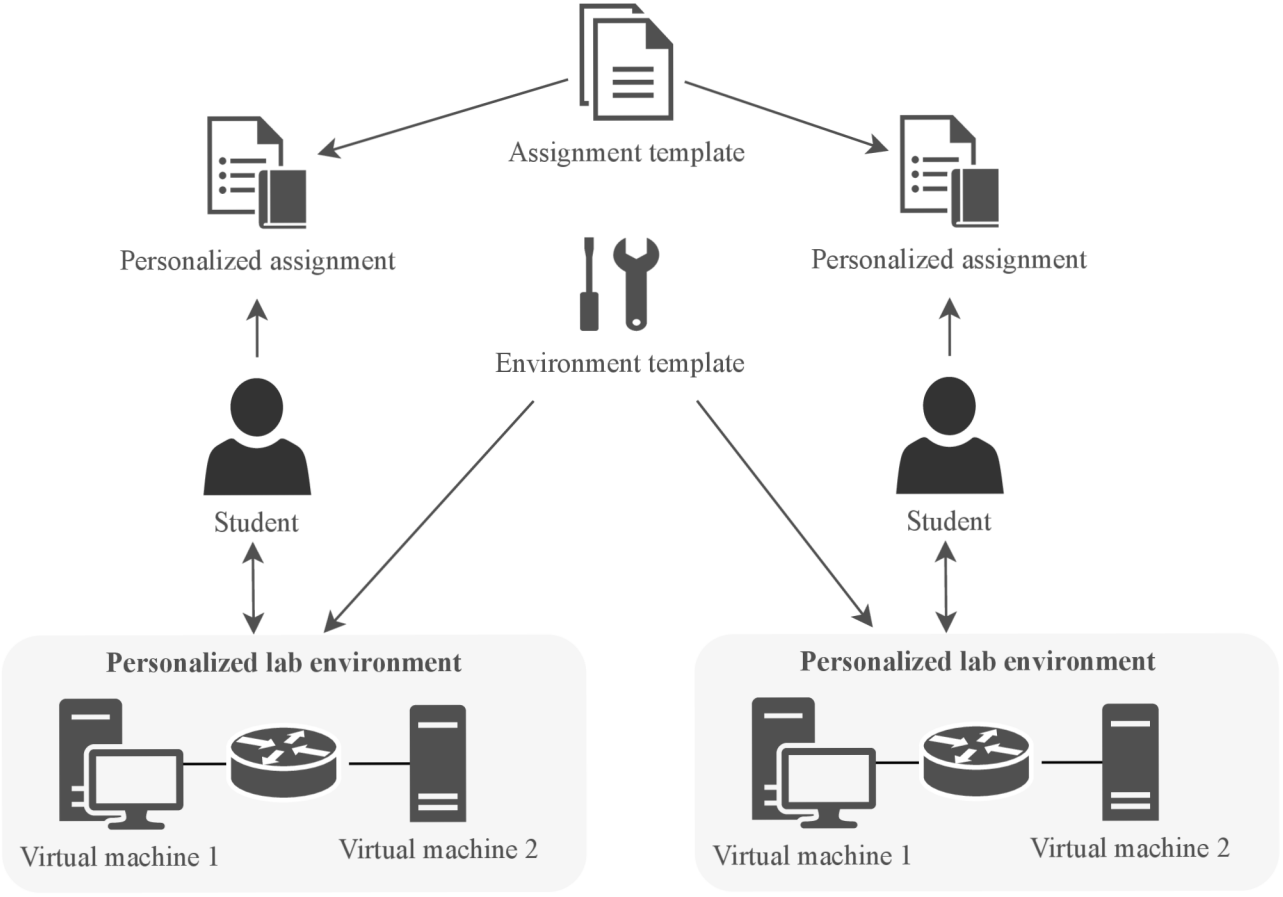


Motivation

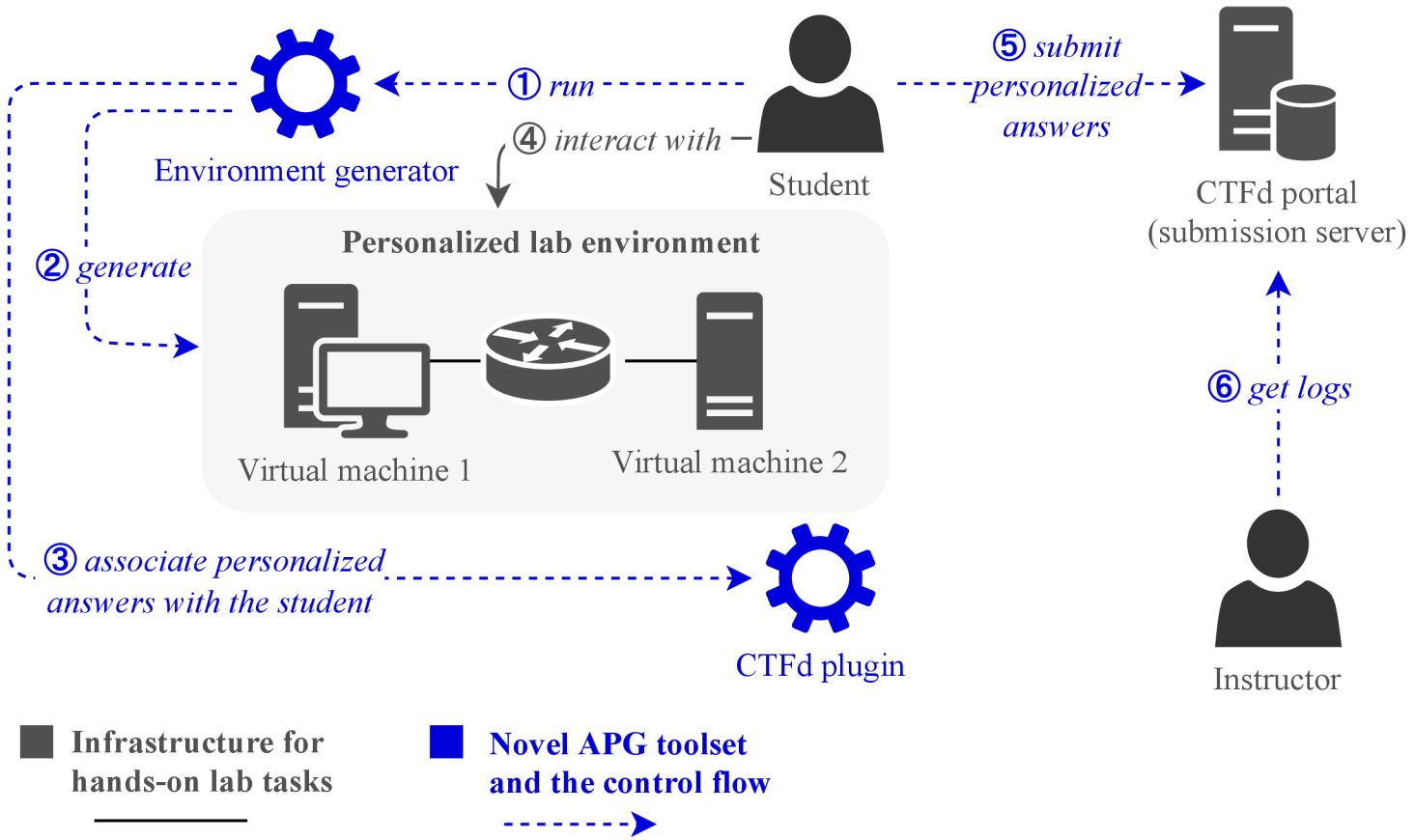

Assignment
Student
Communication
Student
Lab environment
Virtual machine 1
Virtual machine 2
Lab environment
Virtual machine 1
Virtual machine 2

Paper Contribution

- Methods and toolset for automatic problem generation for tasks in a lab environment.
- Case study in an authentic teaching context.



Toolset

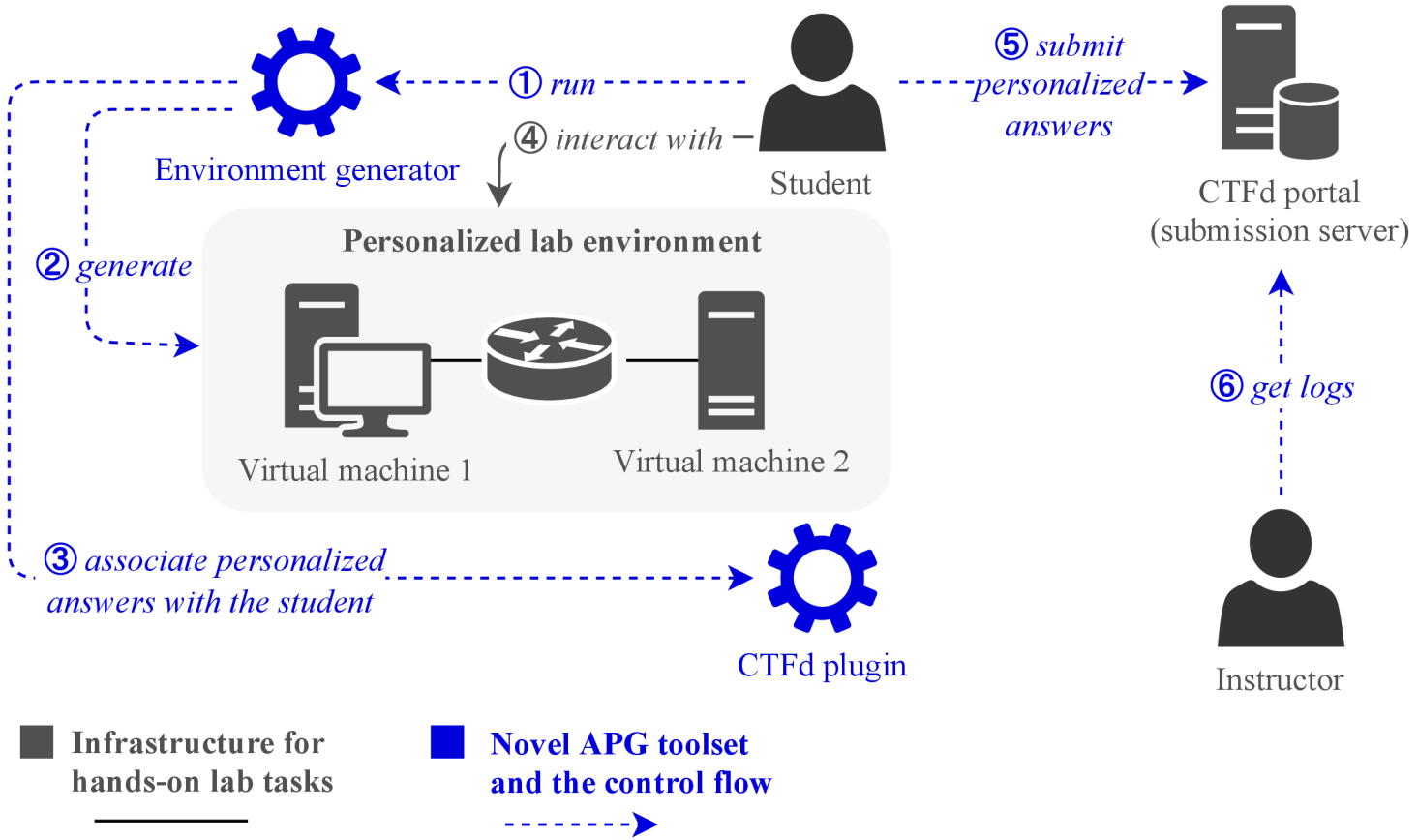

① run
④ interact with
Environment generator
Student
⑤ submit personalized answers
CTFd portal (submission server)
② generate
Personalized lab environment
Virtual machine 1
Virtual machine 2
⑥ get logs
③ associate personalized answers with the student
CTFd plugin
Instructor
Infrastructure for hands-on lab tasks
Novel APG toolset and the control flow

Configuration Generation

```yaml
web:
    type: port
    challenge_id: 1
    min: 8000
    max: 65000
    prohibited: [8080,8888]

secret:
    type: text
    challenge_id: 2
```

Submission Server



Case Study

- Individual homework assignment in an **introductory computer security course**.
- Taught at Masaryk University in the Czech Republic in Spring 2021.
- The course was enrolled by **207 undergraduate students**.
- Topics covered: **network attacks** on authentication of **Telnet** and **SSH** servers, **securing** an SSH server, and **analyzing** SSH **network traffic**.

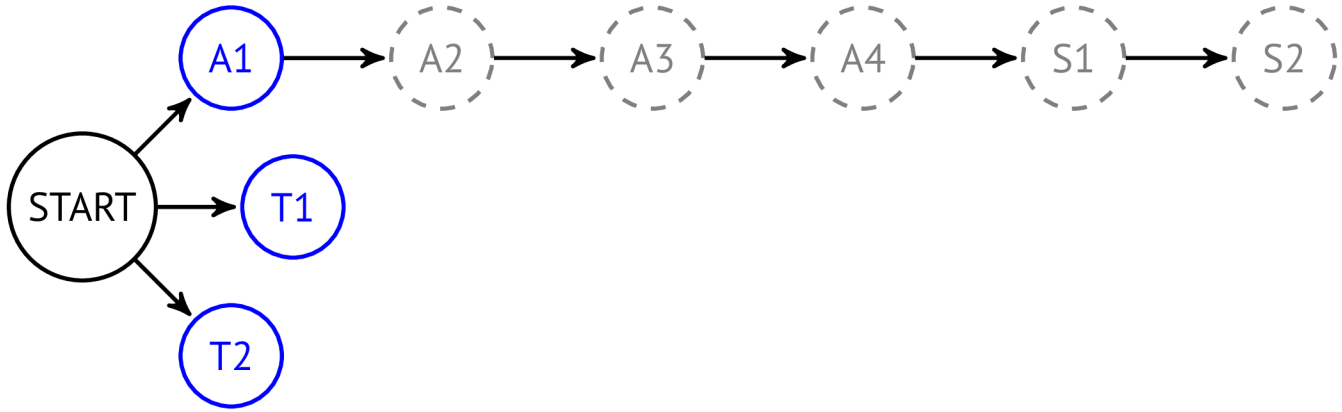
Case Study – Personalized Environment

Each student had a **personalized environment**:

- a host running the Telnet server at a **random network port**,
- one user account with a **random username**,
- another user account with a **random password**, and
- a file containing a **random sentence**.

Tasks

- **8 tasks** in total.
- **1 chain of 6 consecutive tasks**.
- At the beginning, students **can choose from 3 tasks** (A1, T1, and T2).



Cheating Detection

- **Someone else's answers** – the most reliable; incorrect submissions of correct answers of other students.
- **Task chains** – students' solve time for consecutive tasks less than *minimal possible solve time*.
- **Submission proximity** – *time proximity* or *location proximity* of two or more submissions.

Results

- **Someone else's answers** – 3 cases.
  - The most conclusive case:
    Student A submitted the correct answer 41247 for A1.
    Student B submitted the incorrect answer 41247 twice, several days later, and before the first interaction with the lab environment.
- **Task chains (consecutive tasks)** – 2 cases.
  - One of two cases:
    Three students completed the A3 task in 58 seconds.
    The minimal possible solve time was 45 seconds. The assignment text: 102 words.
- **Submission proximity** – 2 cases.
  - One confirmed case using location proximity:
    Students K and L submitted their answers to T2 within 68 seconds.
    Student K confessed he had cooperated with L. They share the same dormitory room.

Post-Homework Survey

- **Optional** survey after the assignment – **45 students** answered.
- **Forty students (89%)** would **prefer the provided format** of completing assignments.
- **Only one student** would prefer the **traditional homework assignment**.
- Students' answers to other questions are reported in our paper.

Limitations

- A single exercise in one course – however, the number of participants is considerably larger than in the vast majority of published works.
- The detection methods analyze only students' actions at the submission server.
- Estimating the location proximity using the same IP address of the submission is a double-edged sword.
- Advanced students may reverse-engineer the environment generator and obtain the answers without interaction with the personalized lab environment.
- The answers of 45 out of 195 students may not represent opinions of all students, particularly the critical voices.

Conclusions

- **Prevention and detection of cheating** in hands-on assignments involving the lab environment is **possible in large and remote classes**.
- Automated provisioning of the lab environment with **personalized values generated locally at students' computers** is a feasible approach.
- Our **case study** revealed **seven suspicious cases** using three detection methods.
- **Students** enjoyed the assignment and its format and **did not perceive cheating prevention disruptively**.

Publicly Available Contributions

Full paper and slides:
https://www.muni.cz/en/research/publications/1816366

Open-source toolset:
https://gitlab.fi.muni.cz/cybersec/apg

Stay in Touch

Jan Vykopal
vykopal@ics.muni.cz

Cybersecurity Laboratory
https://twitter.com/cybersecmuni

Acknowledgments

- ERDF project “CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence” (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

- Special thanks to Daniel Košč for developing the toolset.

MUNI
C4E

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ