

# TOWARD AN AUTOMATED FEEDBACK SYSTEM IN EDUCATIONAL CYBERSECURITY GAMES

MUNI  
FI

Valdemar Švábenský, Jan Vykopal, Pavel Čeleda

Masaryk University, Czech Republic  
Faculty of Informatics & Institute of Computer Science  
{svabensky|vykopal|celeda}@ics.muni.cz

MUNI  
ICS

## Motivation

**16,500**  
security vulnerabilities  
discovered in 2018


**\$6 trillion**  
worldwide damage  
from cybercrime yearly

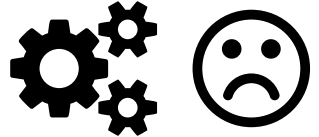
**1.8 million**  
cybersecurity jobs  
unfilled by 2022

## State of the Art


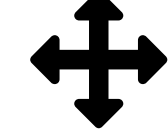
 CTF is growing in popularity  
as a method of active learning

 Regular feedback is crucial  
to support beginners

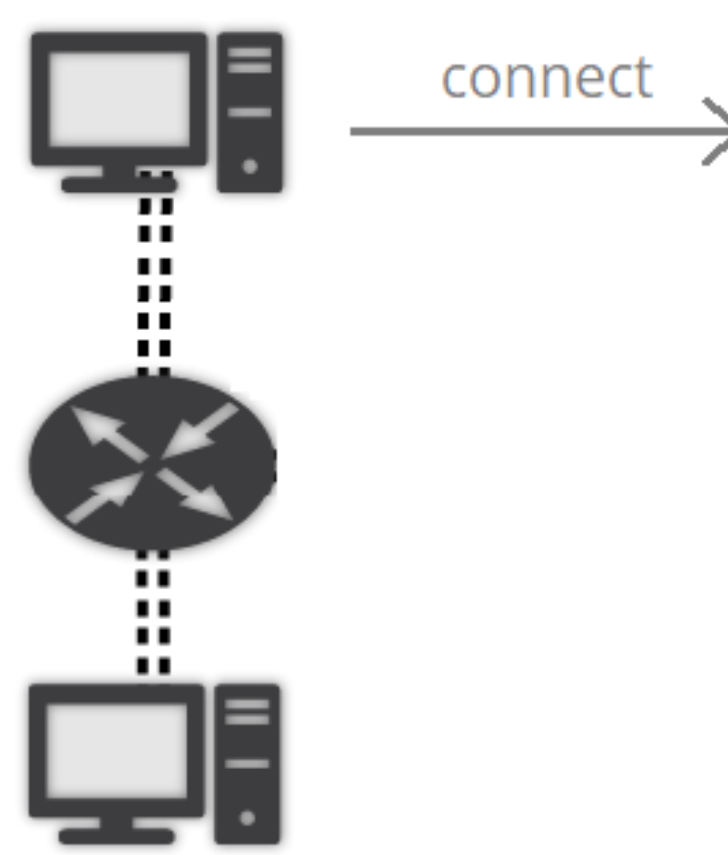
 Manual feedback requires the  
time of an expert instructor

 Current automated feedback  
in games is insufficient

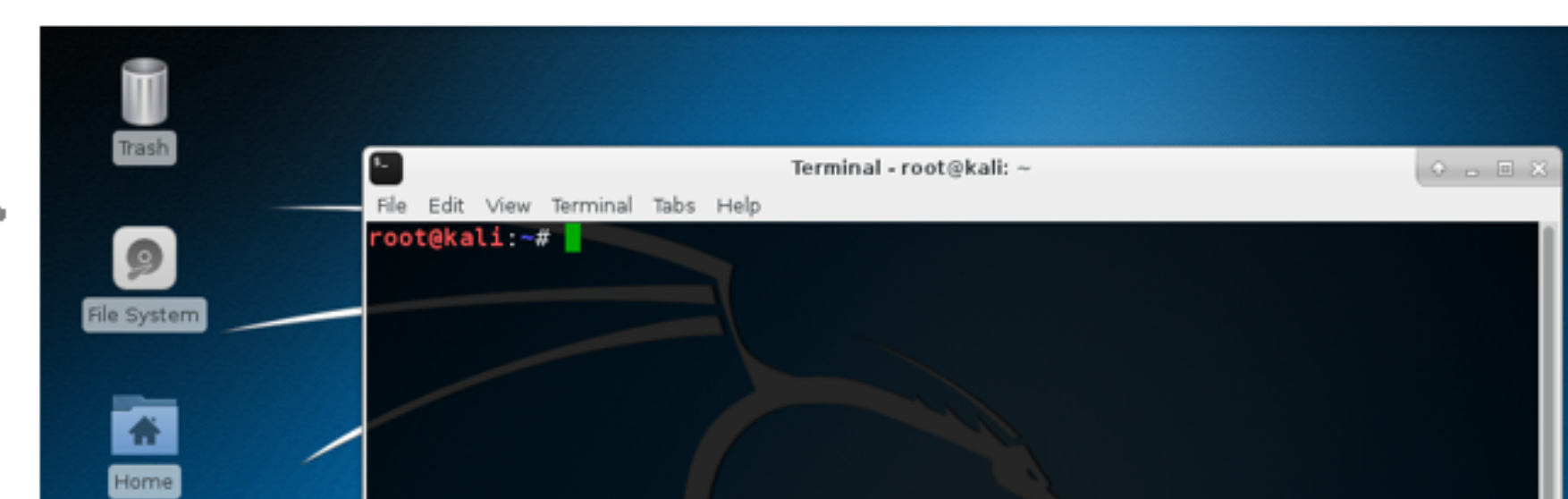
## Capture the Flag (CTF) Games

-  Training activities for exercising cybersecurity skills
-  Practice tasks with multiple approaches to the solution

Kali-attacker / 10.10.20.2



HTTP-server / 10.10.10.2



Level 1

**Task:** Scan the HTTP server.  
**Flag format:** The number  
of the highest open port.

Enter the flag here.

Points available: 6/8



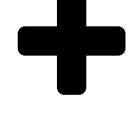
Need help?

**Hint 1:** What tool to use  
**Hint 2:** How to use the tool




Show Hint 1 (-2 points)

Use nmap.

## Research Problem

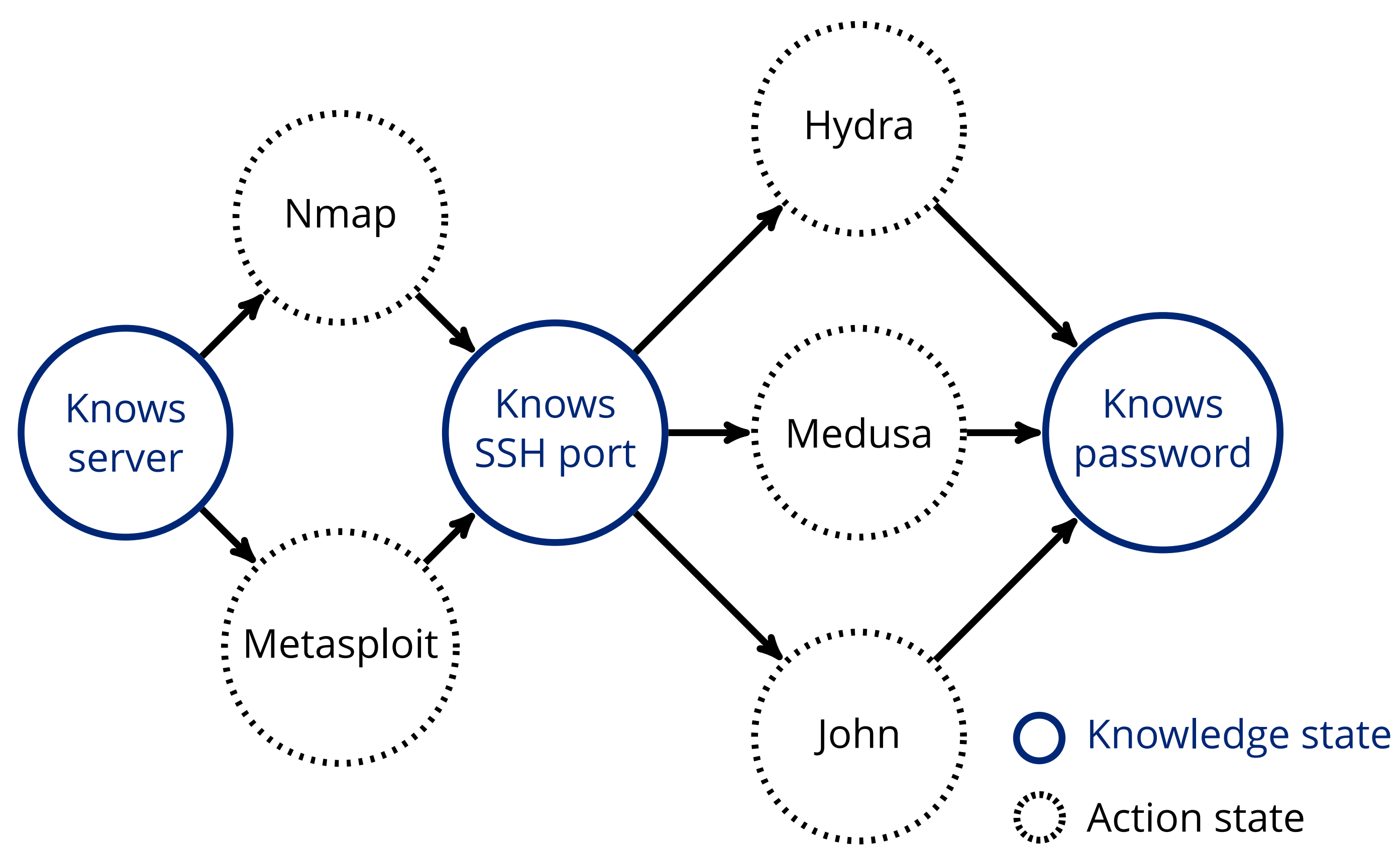
-  **Aim:** Automate in-game feedback for learners
-  **Challenge:** Heterogeneous data, domain-specific tools
-  **Novelty:** Methods from programming domain are often inapplicable

## Expected Contributions

-  Effective learning at an individual pace
-  More students will be able to practice cybersecurity skills
-  Reduced dependency on human instructors

## RQ1: Modeling Solution Paths in Game Levels

**Goal:** Describe a general approach to modeling game levels and apply it in practice on selected games.



## RQ2: Exploring Interactions of Players

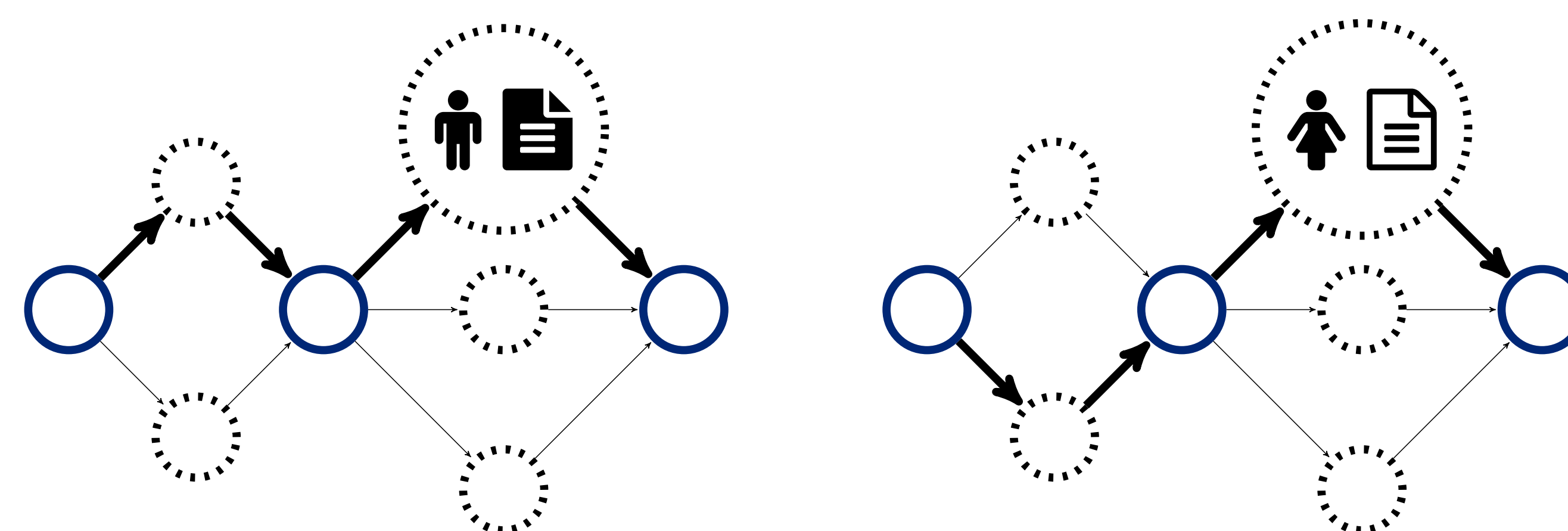
**Goal:** Develop data analysis methods for deriving information about solution patterns and errors of each player. Leverage this data to improve the model.

```

2018-08-20 16:53:02 # hydra -l yda -P pass.txt
2018-08-20 16:53:15 # hydra -l yoda -P pass.txt
2018-08-20 16:53:34 # hydra -h
2018-08-20 16:57:28 # hydra -l yoda -P pass.txt ssh:172.18.1.14
2018-08-20 16:57:54 # hydra -l yoda -P pass.txt ssh://172.18.1.14
  
```

## RQ3: Providing Automated Formative Feedback

**Goal:** Employ the model to provide personalized hints and feedback.



Players who progress differently may receive different feedback.

## Contact and Acknowledgements

 kypo.fi.muni.cz  
kypo.cz

 svabensky@fi.muni.cz

 @csirtmu

This research was supported by the Security Research Programme of the Czech Republic 2015–2020 (BV III/1 – VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019014 – Simulation, detection, and mitigation of cyber threats endangering critical infrastructure. Computational resources were provided by the European Regional Development Fund Project CERIT Scientific Cloud (No. CZ.02.1.01/0.0/0.0/16\_013/0001802).