An Exploratory Study of Hardware Reverse Engineering Technical and Cognitive Processes

Steffen Becker[1,2], Carina Wiesen[1,2], Nils Albartus[1,2], Nikol Rummel[1], Christof Paar[2]

[1] Ruhr University Bochum; [2] Max Planck Institute for Cybersecurity and Privacy

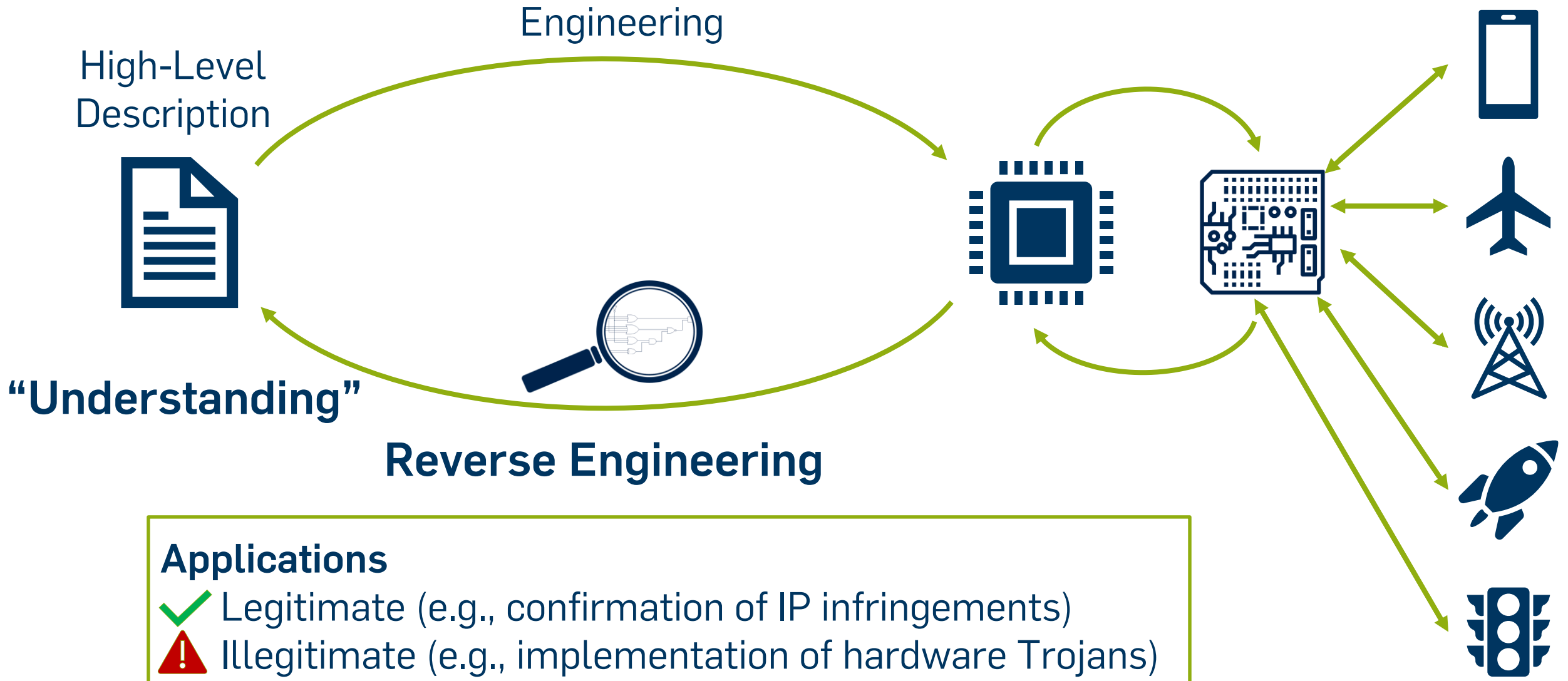
SOUPS 2020, Virtual Conference

August 11th, 2020

RUB

Hardware Reverse Engineering (HRE)

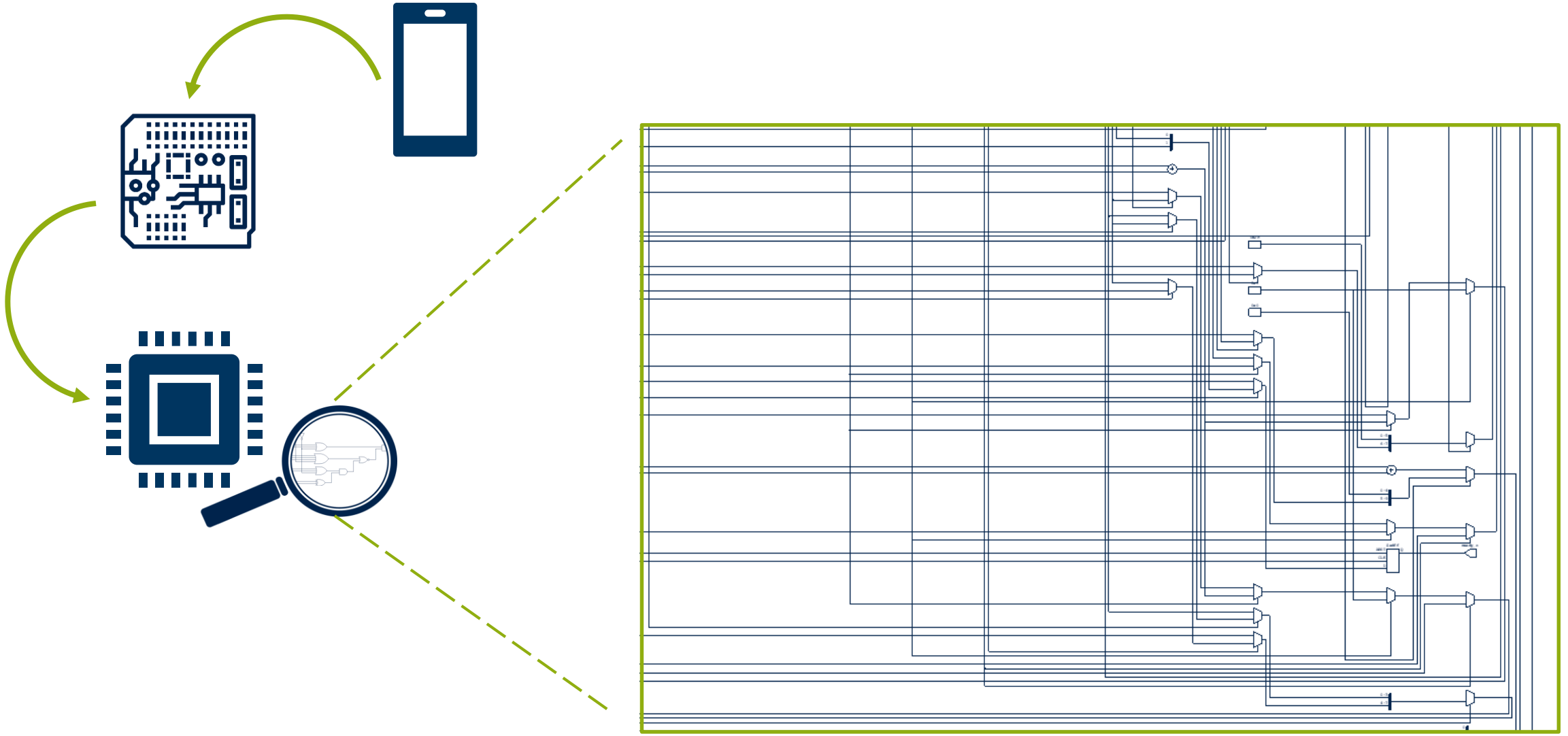
Hardware Reverse Engineering (HRE)



Applications

- ✓ Legitimate (e.g., confirmation of IP infringements)
- ⚠ Illegitimate (e.g., implementation of hardware Trojans)

Netlist Reverse Engineering



Model of HRE and Research Gap

Netlist Reverse Engineering

Semi-automated Processing

+

Cognitive Processes

Research Gap

Underlying **cognitive processes** of HRE are **poorly understood**

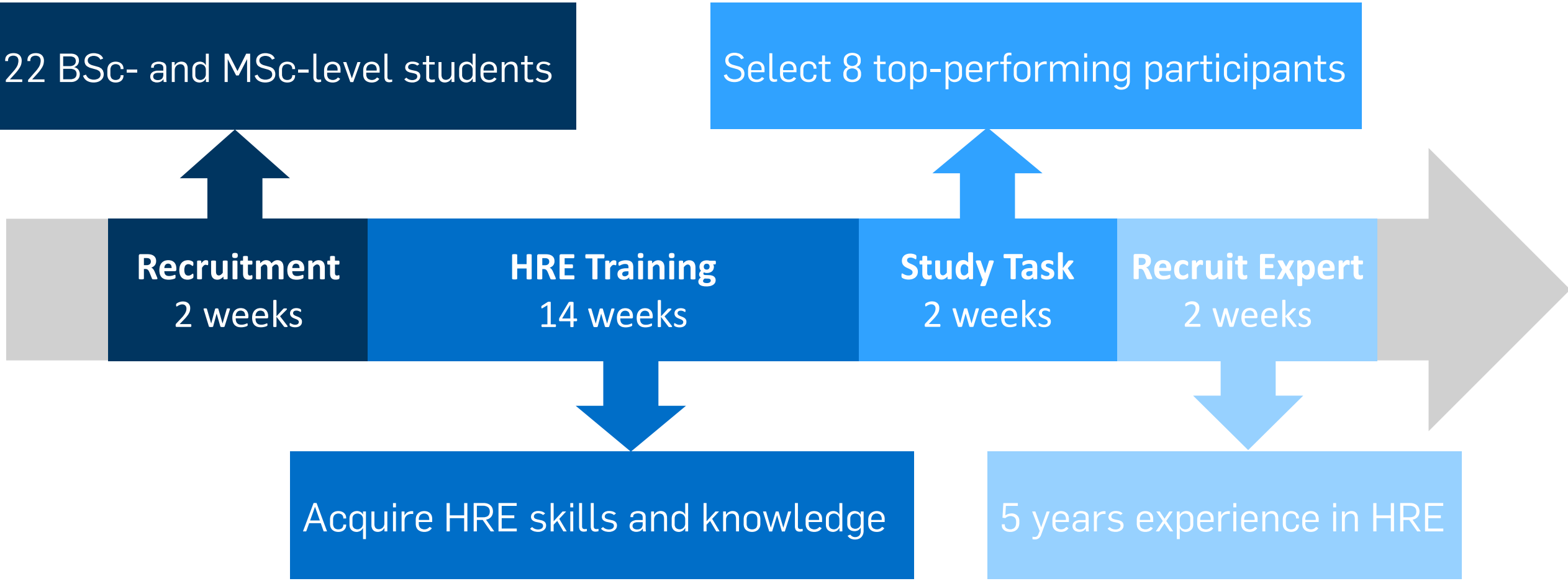
Research Questions

Research Questions

- RQ1: Which are the crucial **phases of human sense-making** during HRE?
- RQ2: Which **strategies** distinguish more and less efficient reverse engineers?
- RQ3: Which **cognitive prerequisites** play a role for the success of HRE?
- RQ4: Which hypotheses can be derived for **cognitive obfuscation**?

Exploratory Study

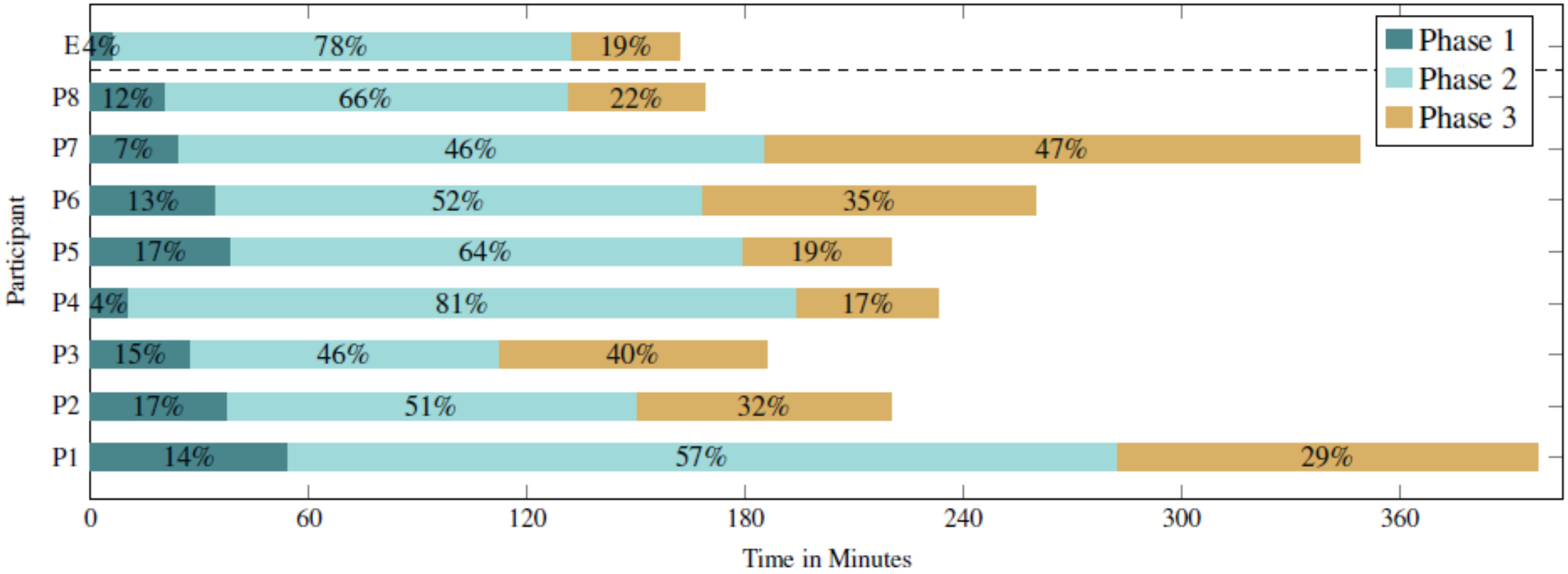
Exploratory Study & Participants



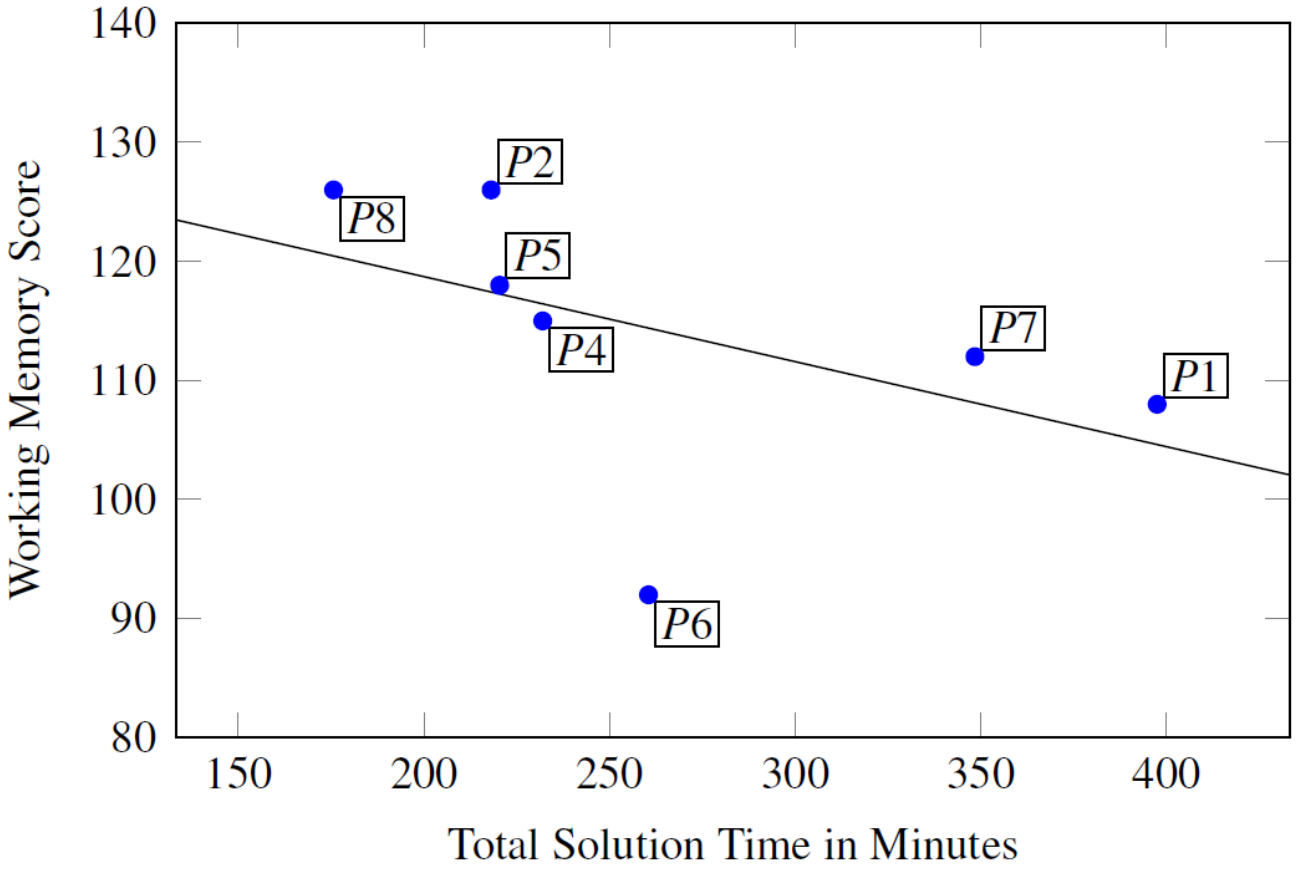
Results

RQ1: 3 Human Sensemaking Phases in HRE

1. Candidate Identification → 2. Candidate Verification → 3. Realization



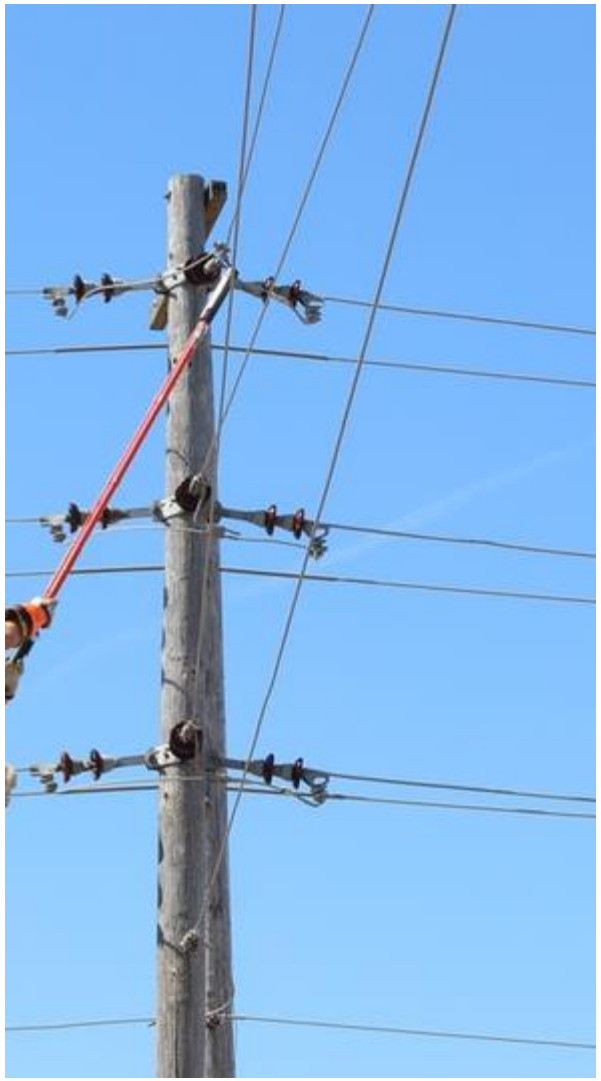
RQ3: Cognitive Factor Working Memory

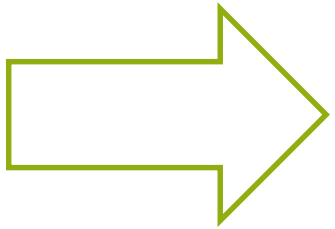


Disclaimer: only descriptive analysis; further research needed!

Future Work: Cognitive Obfuscation

Cognitive Obfuscation





Source: www.constructionknowledge.net

Idea: Overload capacity of reverse engineers' working memory
(e.g., by employing dummy wires or camouflaged gates)

Conclusion & Future Work

- **Results:**
  - First step towards a better understanding of cognitive processes in HRE
  - Three-phase model
  - Combination of manual and semi-automated analyses
  - Working memory might influence HRE

- **Limitations:**
  - Small sample size of students; only one expert
  - Validity for other HRE problem settings unclear

- **Future Work:**
  - Novel class of countermeasures against HRE: *cognitive obfuscation*
  - Quantification of cognitive influences

Thank You for Your Attention!

Hardware Security Squad

Christof Paar

Steffen Becker

Nils Albartus

Psychology Squad

Nikol Rummel

Carina Wiesen

Please contact us: **Steffen.Becker@rub.de** and **Carina.Wiesen@rub.de**

Ruhr University Bochum

RUB

Max Planck Institute For Cybersecurity and Privacy