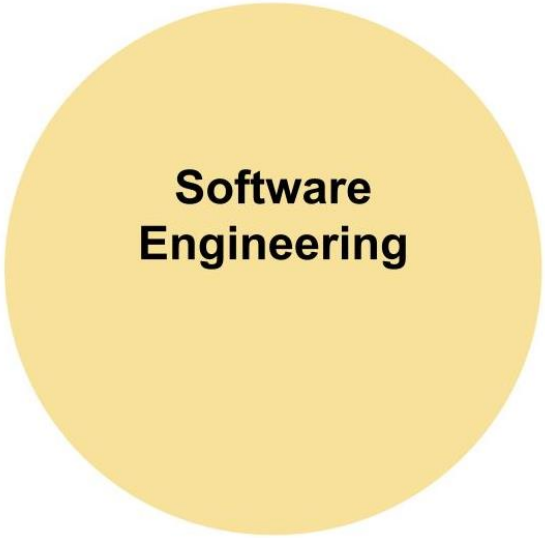
Cognitive Processes, Trust, and Biases in Cybersecurity

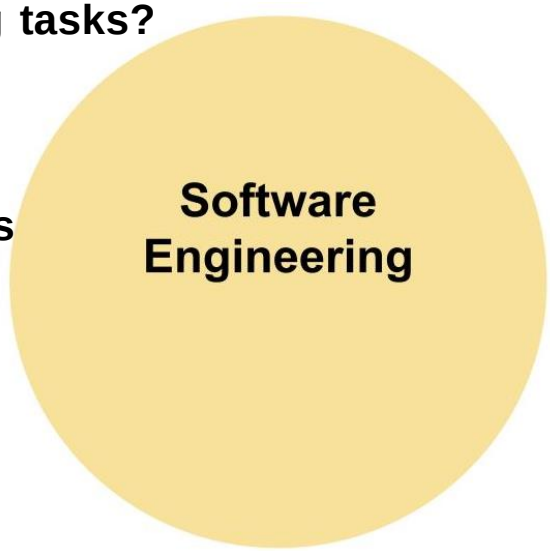
Yu Huang
Assistant Professor
Computer Science, Insitute for Software Integrated Systems
Vanderbilt University
https://yuhuang-lab.github.io/
yu.huang@vanderbilt.edu

SE: Improve productivity and assure quality in software development and maintenance.



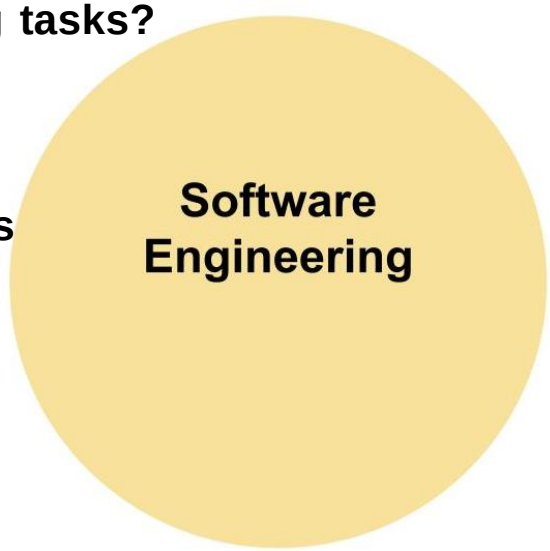
SE: Improve productivity and assure quality in software development and maintenance.

- How do programmers think in programming tasks?
- How do experts become experts?
- How do novices and experts solve problems differently?
- What affects programmers' productivity?
- What are the effects of human biases in programming tasks?
- How does trust and bias issue affect developers' behaviors?



SE: Improve productivity and assure quality in software development and maintenance.

- How do programmers think in programming tasks?
- How do experts become experts?
- How do novices and experts solve problems differently?
- What affects programmers' productivity?
- What are the effects of human biases in programming tasks?
- How does trust and bias issue affect developers' behaviors?

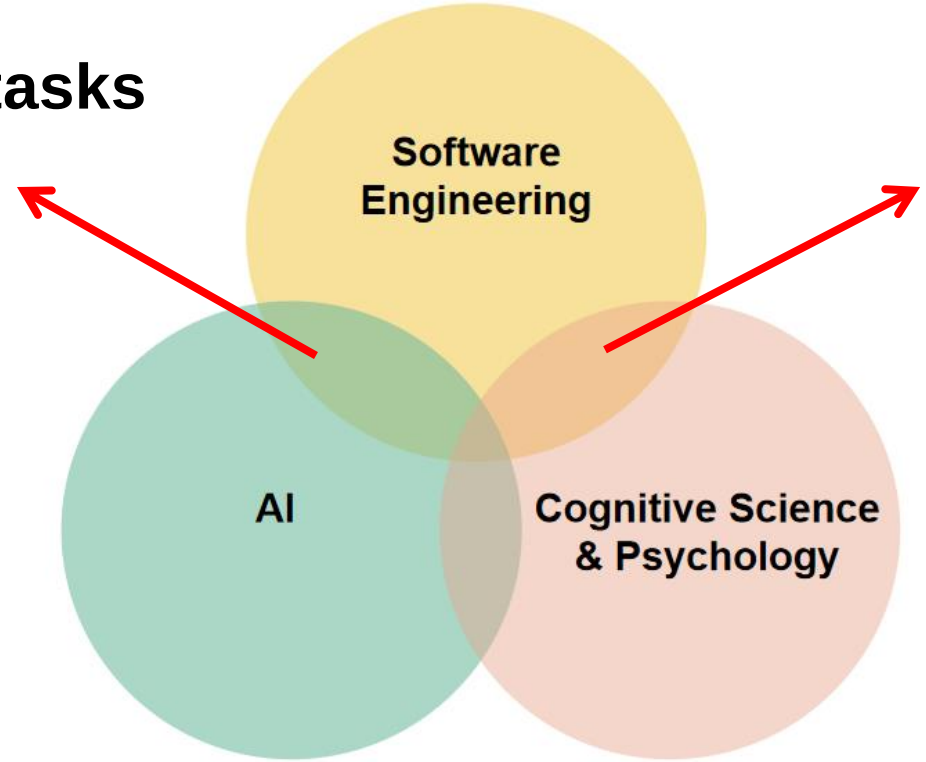


- How can we design automated tools and models to conduct programming tasks efficiently and effectively?
- How can we develop more human-like AI models leveraging human behaviors?

Yu.huang@vanderbilt.edu

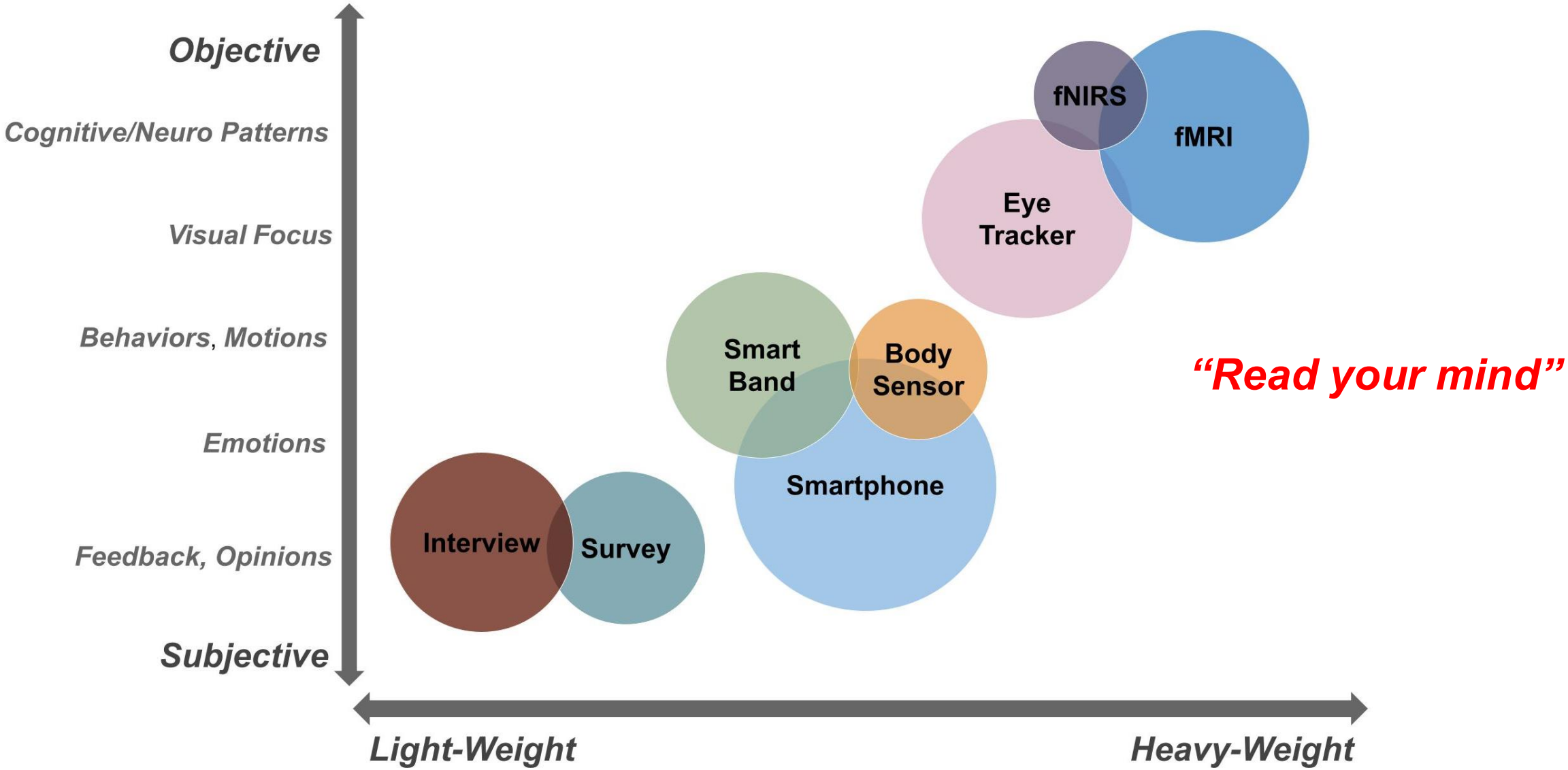
SE: Improve productivity and assure quality in software development and maintenance.

AI4SE: downstream tasks



- **Cognitive processes**
- **Behaviors**
- **Visual patterns**

How do we measure human aspects in SE tasks?



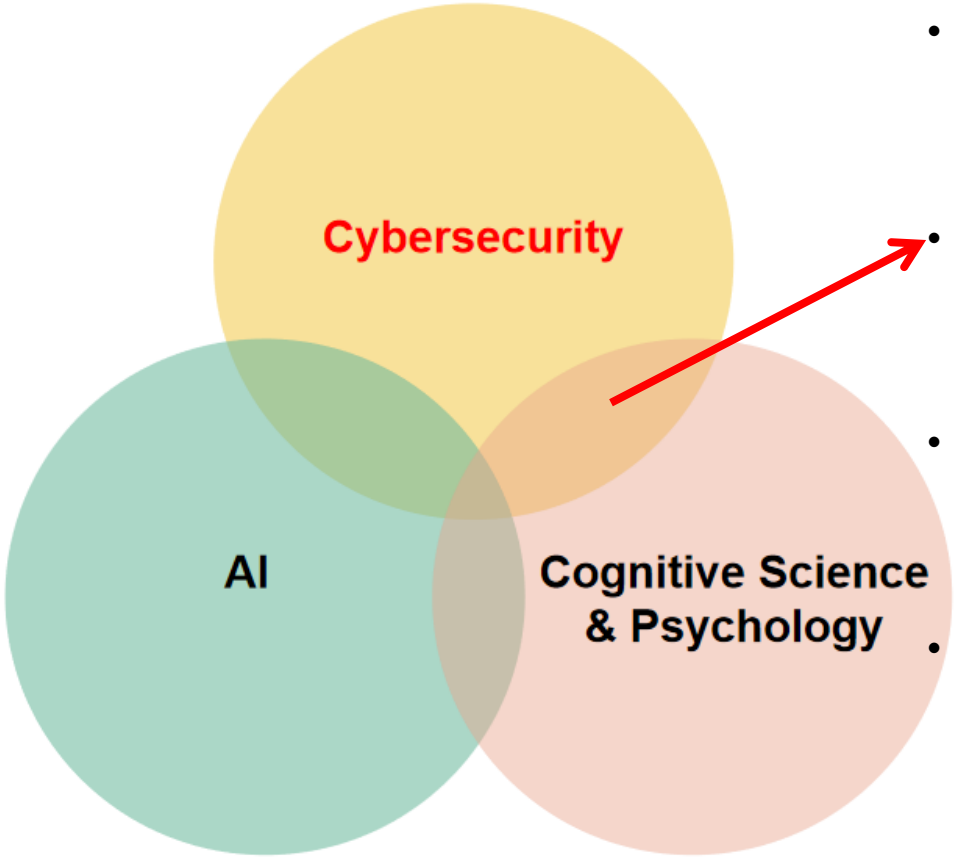
"Read your mind"

Yu.huang@vanderbilt.edu

How do we measure human aspects in SE tasks?

"Read your mind"

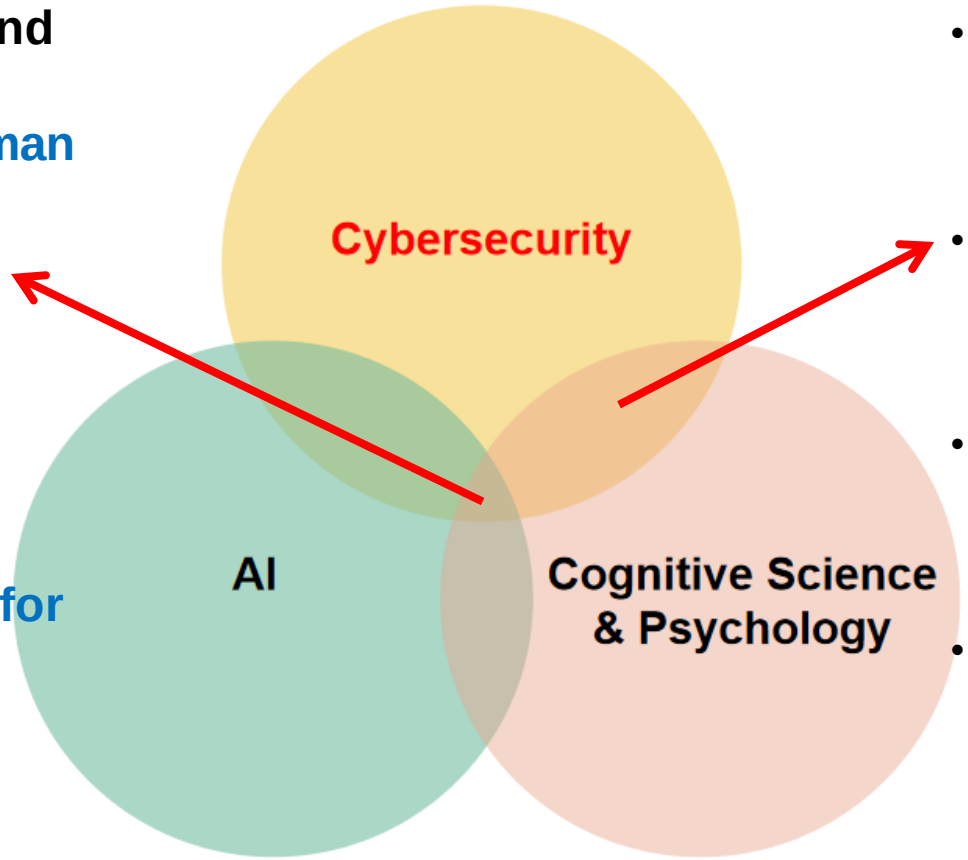
Software Engineering → Cybersecurity (Attack + Defense)



- How do novices and experts attack/defend a system (modeling cognitive patterns)?
- What are the beacons (signals) attackers use to exploit vulnerabilities?
- Can we leverage attackers' cognitive patterns to lure attacks?
- How does trust and bias issue affect defender's behaviors and strategies?

Software Engineering → Cybersecurity (Attack + Defense)

- Does the model design and evaluation align with human judgement?
- How can we learn from programmers to design human-centered models for Cybersecurity?



- How do novices and experts attack/defend a system(modeling cognitive patterns)?
- What are the beacons (signals) attackers use to exploit vulnerabilities?
- Can we leverage attackers' cognitive patterns to lure attacks?
- How does trust issue affect defender's behaviors and strategies?

Yu.huang@vanderbilt.edu

Software Engineering → Cybersecurity (Attack + Defense)

- **Expertise**
  - **Qualitative and quantitative analysis**
  - **Human-system experimental design**
  - **Longitudinal study and training**
  - **AI4SE, program analysis, CS education**
- **Facility support**
  - **Eye tracking**
  - **Medical imaging**
  - **Body sensors**
  - **Human study support: IRB, space, software support, recruitment, etc.**