CERIAS
The Center for Education and Research in Information Assurance and Security

Assessing Secure Programming Knowledge with Pre- and Post-Surveys

presenter: Lauren M. Stuart *professors:* Dr. Melissa Dark, Dr. Ida Ngambeki (Purdue), Dr. Matt Bishop (UC Davis)
with additional thanks to: Steve Belcher (NSA), Dr. Jun Dai (CSUS), Dr. Phil Nico (Cal Poly San Luis Obispo)

Question:
How do we create software with **more robustness**?

Secure programming clinic (SPC):

- Instructors grade for robustness
- students visit standalone clinic
- See other poster at this session

Subquestion:
How do we **assess knowledge** of secure programming? # bugs? # fixes? # points earned? class grade?

Challenges:

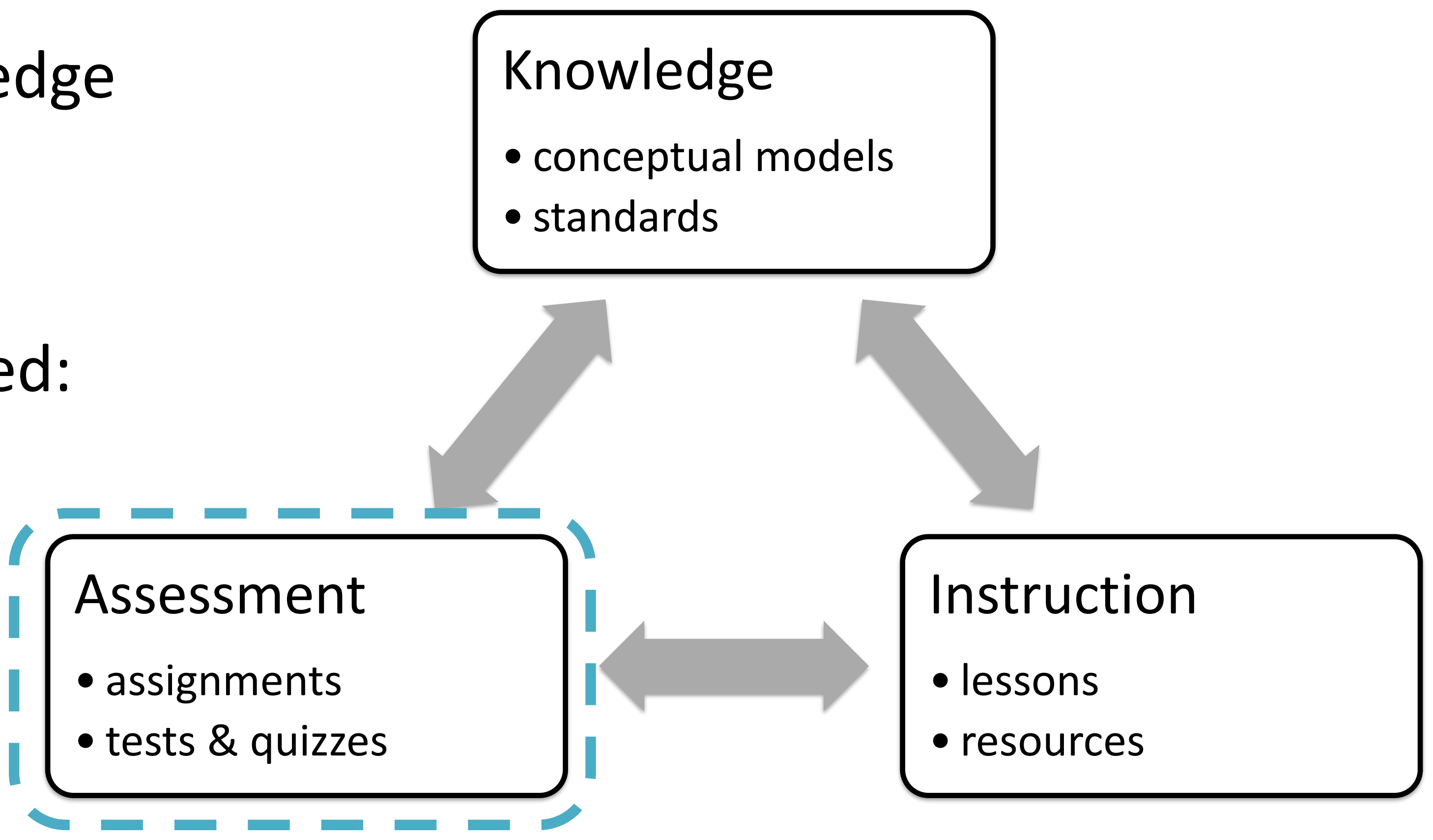
- No standard body of knowledge
- No standard assessments
- No standard instruction

…all three must be developed:

This poster's focus lies inside assessment.

We have related assessment work in:

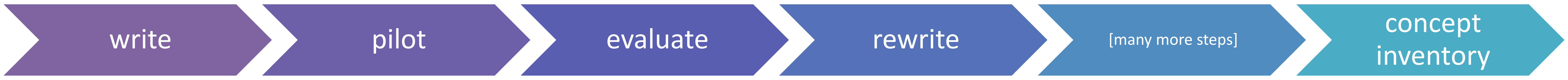
- self-efficacy assessment
- presence & absence of secure coding behaviors
- form & content of students' mental models, etc.


Knowledge
- conceptual models
- standards

Assessment
- assignments
- tests & quizzes

Instruction
- lessons
- resources

Aim: create and vet a question bank to assess secure programming knowledge.



- what knowledge to measure, and how?
- how to analyze student performance?
- do questions measure the knowledge well?
- how can questions measure better?
- (and iteration on previous)
- standard question bank
- covers student errors

Question P15, first draft

Explain the choice of a file descriptor over the filename as the channel to access a file.

A. A file descriptor is a data structure that allows only me to use the file for as long as it is open.

B. The file descriptor is an abstraction that makes for cleaner and more understandable code.

C. The file descriptor is a pointer to the file that stays the same regardless of changes to the file name or location.

D. The file descriptor is a wrapper for the file name and works exactly the same way.

Pilot 1

- California State University Sacramento
- Upper-division Operating Systems class
- 73 usable responses
- 12 questions from bank

Item ease (how many students got item correct)	0.40
Discriminating power (IDP) (item separates high scorers from low)	0.48

	A	B	*C	D
upper 25% of scorers	2	3	14	2
middle 50%	10	8	11	2
lower 25%	6	8	4	3

Results for UC Davis, Cal Poly San Luis Obispo pre-tests not yet available at poster submission.

Evaluation

Is this question…

- precise?
- useful?
- exclusive?
- exhaustive?

Instructor notes, summarized:

- A is a pretty good mistake
- A and B caught a lot of students
- "cleaner" means…? & other wording.
- Additional misconception ID'd.
- There may be 2 questions here.

Question P15, later draft

Explain the choice of a file descriptor over the filename as the channel to securely access a file.

A. A file descriptor is a data structure that allows only me to use the file for as long as it is open, while the file name does not.

B. The file descriptor is an abstraction that makes for ~~cleaner and~~ more understandable code.

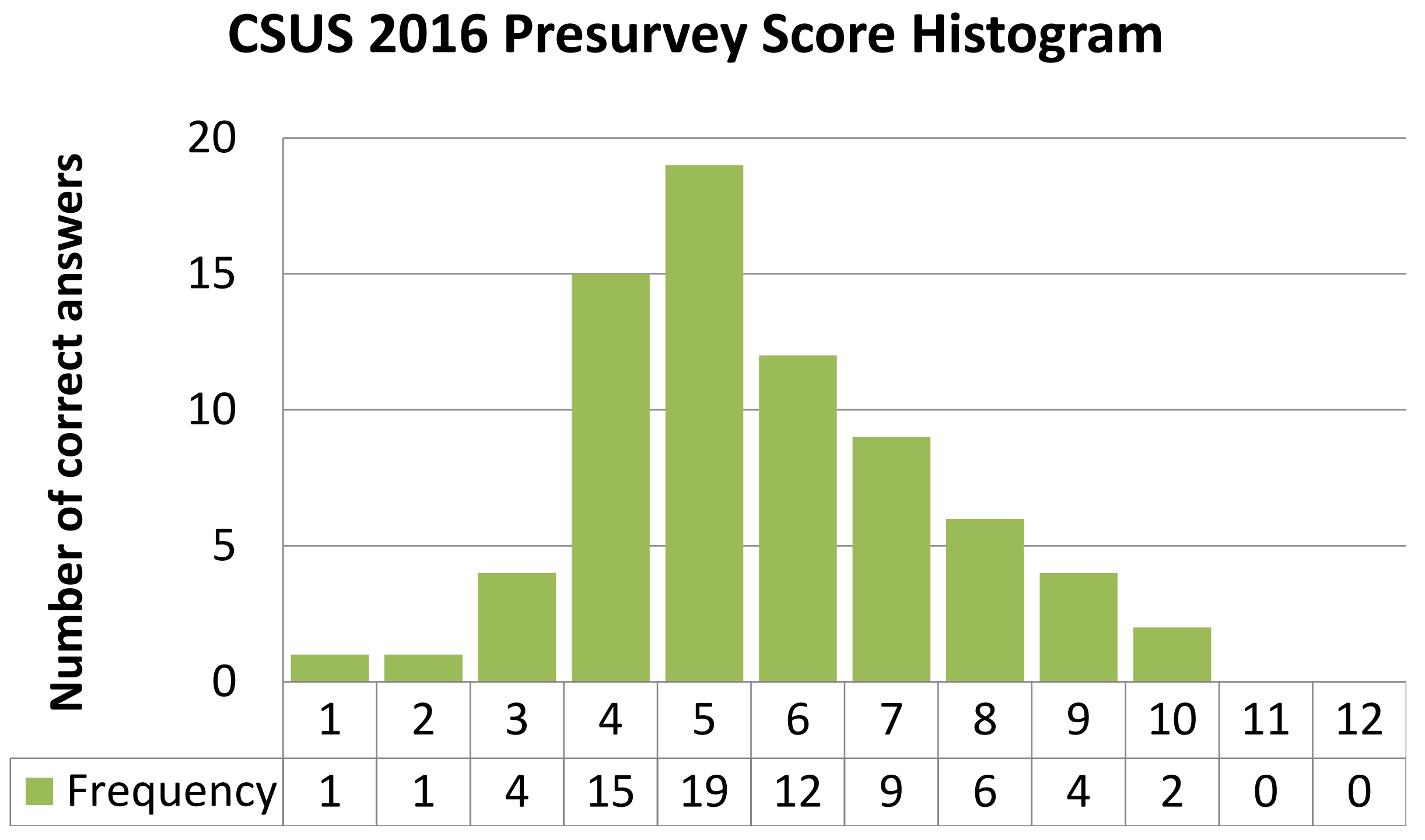
C. The file descriptor is a pointer to the file that stays the same regardless of changes to the file name or location.

D. The file descriptor is a data structure that encapsulates the file name.

E. The file descriptor is a data structure that represents the validated file name.

Pilot 1 Results

Spring semester 2016, Cal State Sacramento


CSUS 2016 Presurvey Score Histogram

	1	2	3	4	5	6	7	8	9	10	11	12
🟩 Frequency	1	1	4	15	19	12	9	6	4	2	0	0

Question	Item ease	IDP	Concern: distractors	Concern: wording
P1	44%	0.43	X	
P2	33%	0.38		X
P3	49%	0.10	X	
P6	69%	0.43		
P7	41%	0.29		X
P8	44%	0.43		
P9	32%	0.29		X
P10	40%	0.48	X	
P11	64%	0.48	X	
P12	41%	0.48	X	
P13	67%	0.19	X	X
P14	37%	0.43	X	

+ additional question
on file descriptor definitions

Upcoming:

- Post-tests: CSUS, UC Davis, Cal Poly San Luis Obispo
- Deeper analysis of questions for adequacy, precision, coverage
- Co-analysis with other SPC data

National Science Foundation
WHERE DISCOVERIES BEGIN

"This material is based upon work supported by the National Science Foundation under Grant No. 1303048. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the National Security Agency."

PURDUE
UNIVERSITY