Development of Peer Instruction Questions for Cybersecurity Education

William E. Johnson, Allison Luzader, **Irfan Ahmed,**
Vassil Roussev, Golden G. Richard III
Department of Computer Science
University of New Orleans

Cynthia B. Lee
Department of Computer Science
Stanford University

Peer Instruction

- Introduced by Eric Mazur, a physicist at Harvard University
- Tested and used in several scientific disciplines including
  - Physics,
  - Biology, and
  - Computer science
- Results of using peer instruction are promising
  - Improving student learning
  - Halving failure rates
  - Increasing student retention in their respective major

Peer Instruction Methodology

- Pre-class preparation by students
  - Reading material
  - Quiz
- In Class, a topic is covered as
  - A question is asked to students
    - Conceptual
    - Multiple choice
  - Two to three minutes for reply
  - Group discussion of students
  - Students reply to the question again
  - Instructor may further discuss the answers

Iterative

Peer Instruction in CS

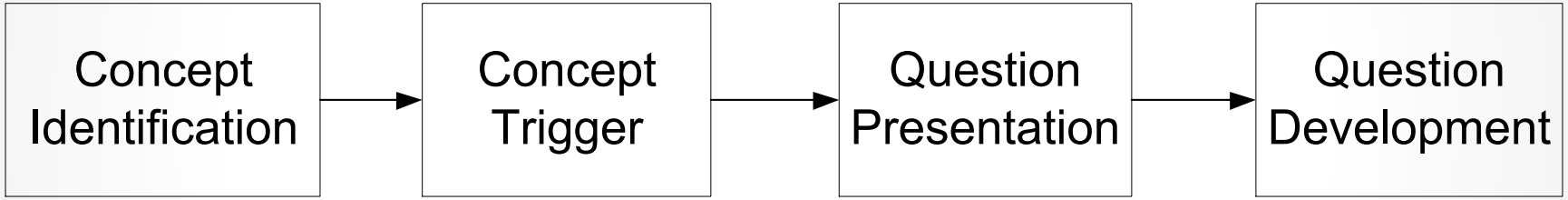
- 6% higher grades on final exams over traditional lecture style
- 61% reduction in failure rates
  - Theory of Computation, and Computer Architecture
- 31% improvement in student retention
- Instructors find peer instruction effective
- Real learning occurs during discussions among students
- Students recommend that more instructors should use peer instruction

Challenges for Developing Questions

- Quiz vs. Peer Instruction Questions
  - Should be conceptual
  - Should facilitate peer discussion

- Plausible Incorrect Answers
  - Creating incorrect answers for peer instruction questions that seem plausible

Question Development Methodology



Concept Trigger

- Provoke a student's thinking process
- Set the desired direction of peer discussion
- Examples: (Beatty *et al. [1]*)
  - Deliberate ambiguity
  - Trolling for misconceptions
  - Omit necessary information
  - Identify a set or subset
  - Compare and contrast
  - Trap unjustified assumptions

Question Presentation

- Putting concept and concept trigger together
  - Better presentation
  - Easier understanding
- Examples:
  - Scenario
  - Example
  - Diagram
  - Definitional
  - Feature

Example Question # 1

An attacker deletes files on a system, denying access to system users. Which element of CIA triad is violated?

a) Confidentiality

b) Integrity

c) Availability

d) None/Other/More than one of the above

Deconstruction # 1

- Concept trigger
  - None of the above
  - Identify a set or subset
  - Multiple defensible answers
- Question Presentation
  - Example

Example Question # 2

Estimate the fraction of disk blocks affected by formatting a hard disk:

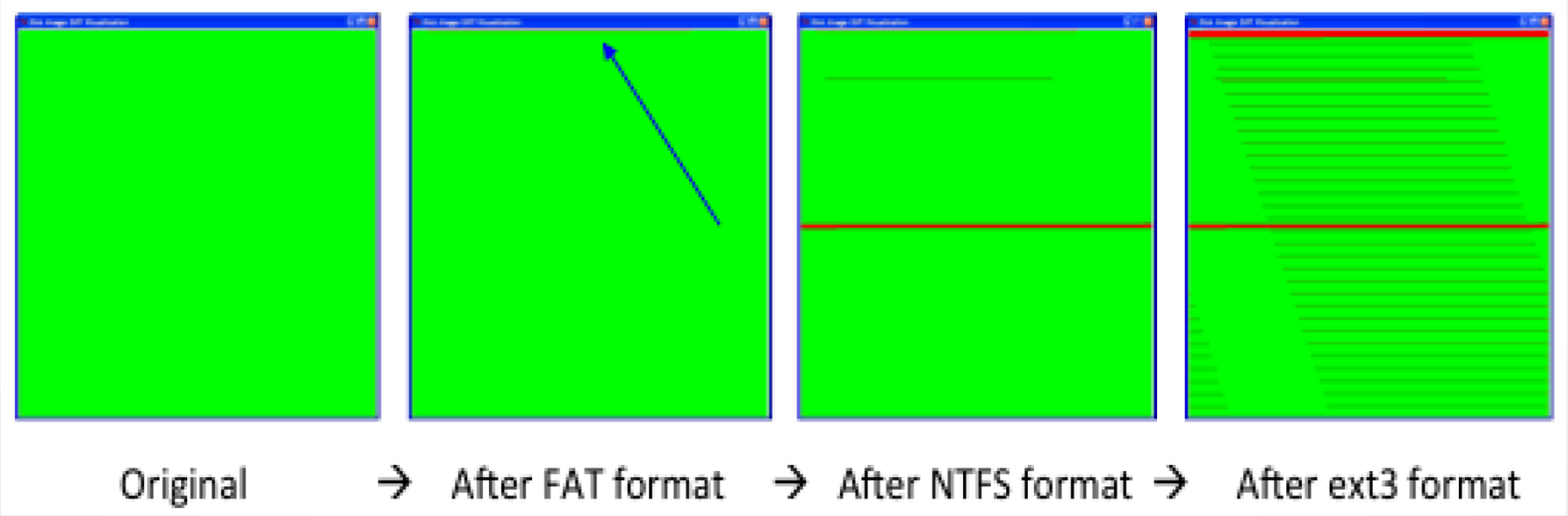
a) 100%

b) 65%

c) 20%

d) Less than 5%

Formatting Flash Drive



Deconstruction # 2

- Concept Trigger
  - Omit necessary information
  - Trap unjustified assumptions
  - Trolling for misconceptions
- Question Presentation
  - Feature
    - Understanding disk formatting to guess correct percentage

Example Question # 3

```
Start:
        mov word    ptr loc_10106+1, 152h
loc_10106:    ;DATA XREF:
        mov ax, 168h
        mov word ptr loc_10129+5, ax
loc_10129:    ;DATA
        mov word ptr es:0, 4D4Ch
```

After executing these instructions while single stepping inside a debugger on an 80486 processor, what is the value of the 16-bit word at location Loc_10129+5?

a) 168h,
b) 152h
c) 4D4Ch
d) Value is unknown
e) None of the above

Deconstruction # 3

- Concept Trigger
  - None of the above
- Question Presentation
  - Example

Example Question # 4

You obtain a leaked database of unsalted SHA-1 password hashes. What would be the most effective way to obtain as many passwords as possible in a short amount of time?

a) Brute force

b) rainbow tables

c) dictionary attack with a large wordlist

d) passing the hash

e) birthday attack

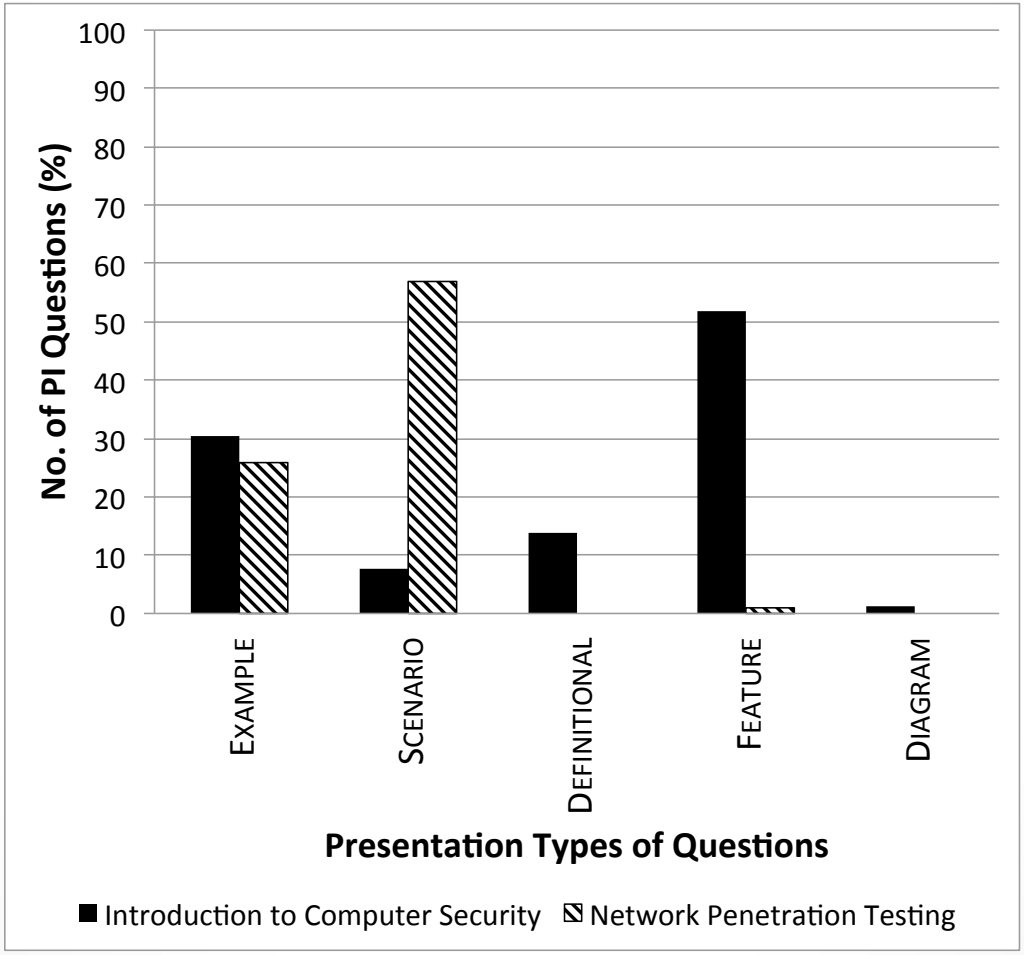
Deconstruction # 4

- Concept Trigger
  - Interpret representations
  - Strategize only
- Question Presentation
  - Scenario

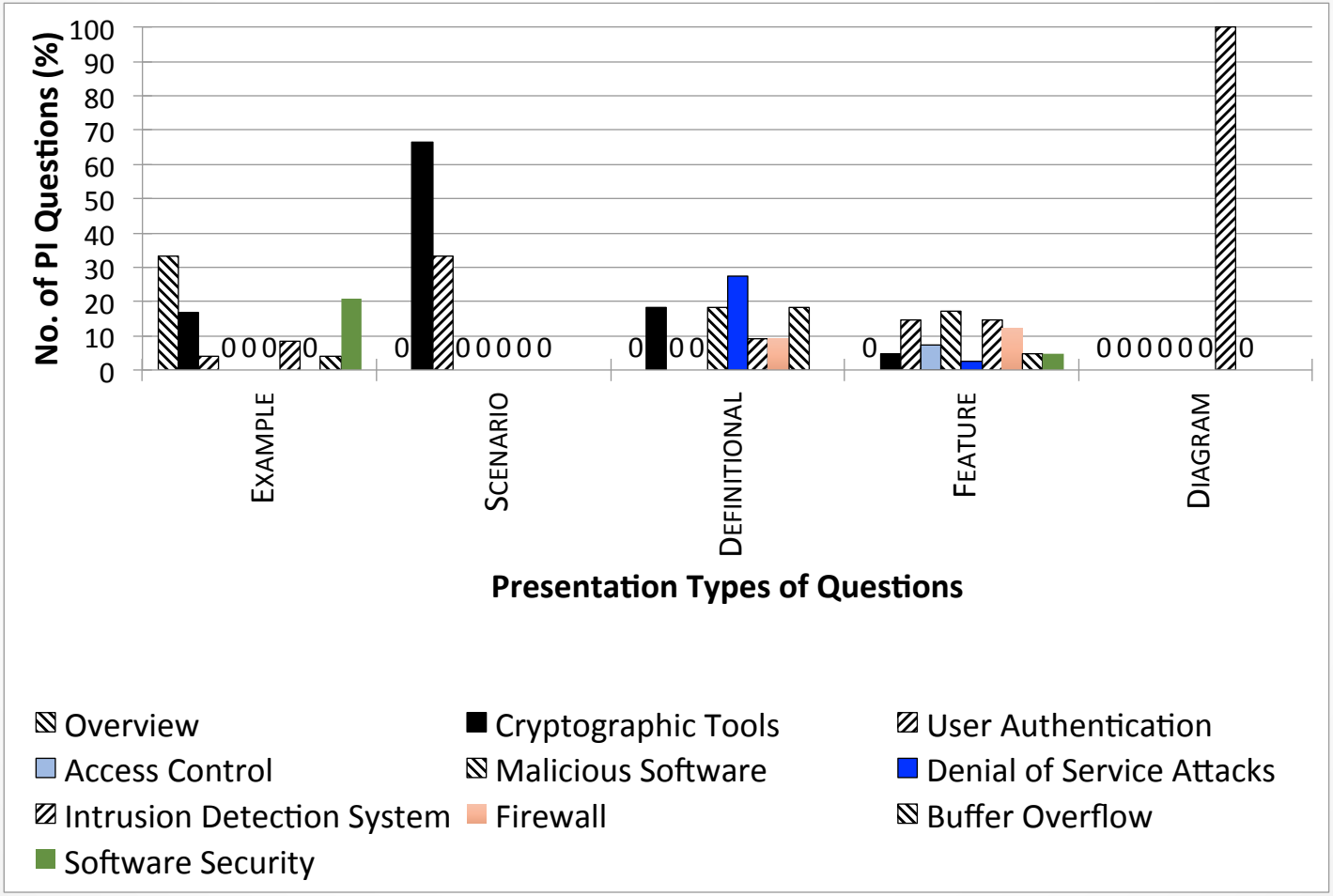
Analysis of Questions

- 172 questions for two cybersecurity courses
  - Introduction to Computer Security (93 questions)
  - Network Penetration Testing (79 questions)
- Goal of Analysis is to identify concept triggers and presentation types in the questions

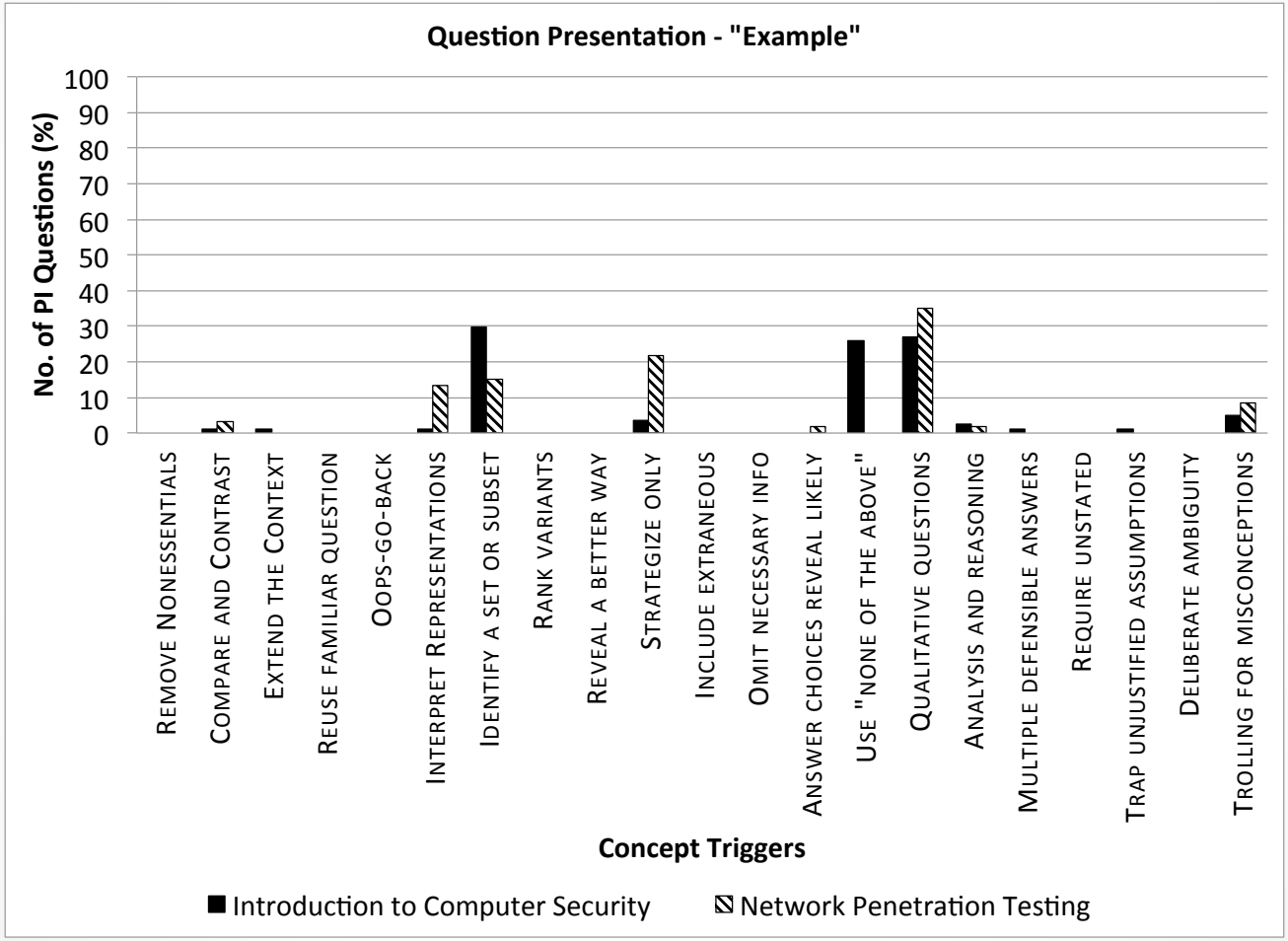
Presentation types



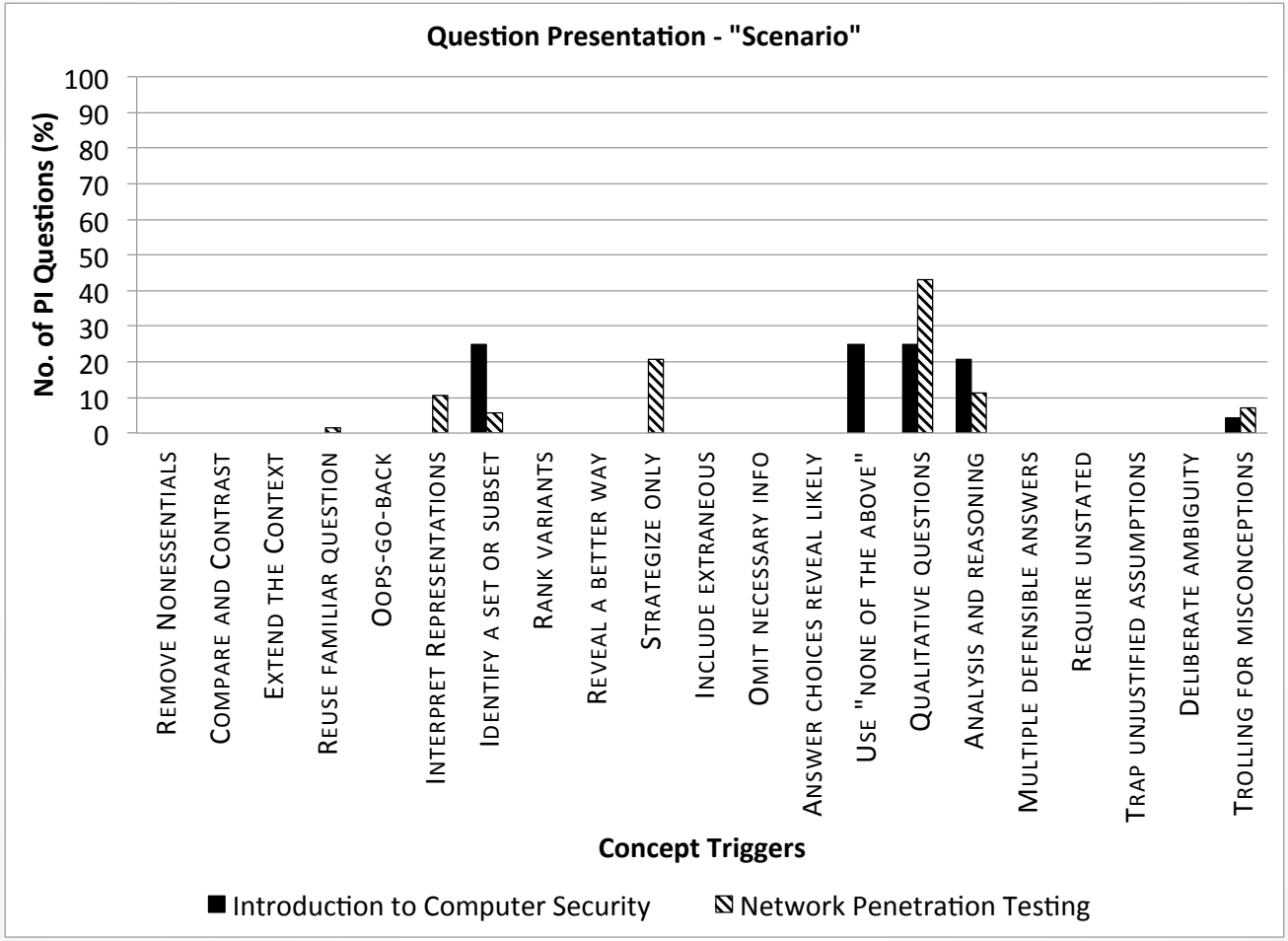
Presentation-types & Topics



Concept Trigger - Example



Concept Trigger - Scenario



Conclusion

- Question development methodology allows instructors to
  - systematically create questions, and
  - smoothly transition from lecture style format to peer instruction
- Analysis of question set
  - example and scenario based questions are often used
  - The use of concept triggers may vary depending on the course content
- Contents will be available at http://www.peerinstruction4cs.org/
- As part of future, evaluate efficacy of peer instruction questions in cybersecurity courses

Questions ??