Teaching Computer Science with Cybersecurity Education Built-in

ASE '16
AUGUST 9, 2016
AUSTIN, TX
usenix.org/ase16

Chuan Yue, chuanyue@mines.edu

COLORADOSCHOOLOFMINES
engineering the way

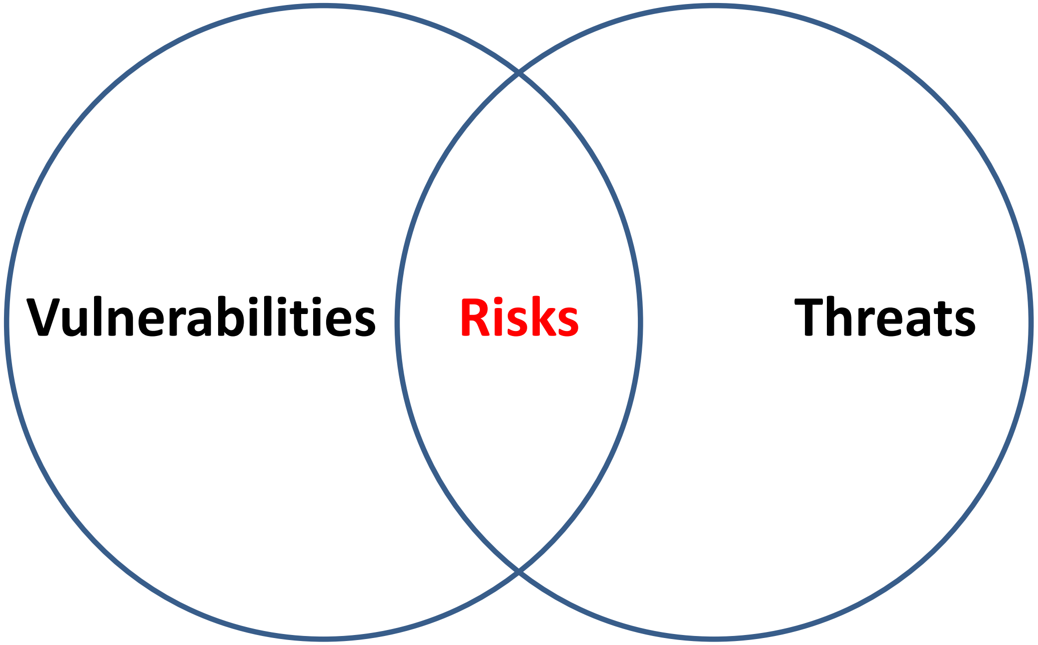
Security & Privacy Vulnerabilities

- The Path to Exploitation

- "Where a threat intersects with a vulnerability, risk is present"
  – NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers
- Vulnerabilities are pervasive in computer & network systems:
  - Req. analysis, design, implementation, deployment, maintenance, ...
  - Web-based, cloud-based, mobile-based, ...
  - Application, middleware, OS, VMM, Hardware, ...
  - Functionality related, usability related, ...
  - Human users
- Security threat trends (Symantec, Gartner, SANS, etc.)
  - targeting end users, online underground economy, rapidly adaptable attacking techniques

Security & Privacy Protection

- Great need and importance, much more challenging!
- Technical solutions
- Educational solutions



Vision: Security-integrated CS Education

- Integrate (inject) relevant cybersecurity topics into non-security courses
  - CS students have no way to escape cybersecurity education
    - none of the top 50 CS programs in U.S. includes cybersecurity in the core of their curricula based on our survey in June 2016
  - CS students understand the correlation and interplay between cybersecurity and other sub-areas of CS
  - Job, career, ...

- Evaluate the teaching and learning effectiveness

- Promote the adoption of this approach

The Security Integration Approach

- Its necessity and importance have been emphasized for over one decade, e.g., SIGCSE 2002 (“Panel on integrating security concepts into existing computer courses” [3]).
- Unfortunately, this approach has received insufficient attention, and it still severely lags behind in adoption.
  - (Section 2 Related Work : mainly on low level courses)
- Our effort complements those existing efforts by providing a new viable implementation solution and focuses more on the (limited existing) integration in upper and graduate level non-security courses.

Outline

- Introduction and Background
- Our Integration Implementation
- Evaluation Results
- Conclusion

Basic Idea of our Integration Implementation

- Leveraging the expertise of cybersecurity researchers to incorporate relevant security topics into upper and graduate level non-security courses.
  - consult with the instructors of non-security courses
  - identify the relevant cybersecurity topics
  - discuss the corresponding topics in the classes
- A viable solution
  - relevant and current content, no training overhead as in [13]
  - use travel time of non-security course instructors, thus address the concern that “something else will have to be sacrificed [3]”

Integration Implementation Effort So Far

- 8 Courses (9 topics, 10 sessions)
  - Computer Communication (A Case Study of Heartbleed Vulnerability)
  - Software Engineering (Engineering Your Password Security)
  - Operating Systems (VM Introspection and the Semantic Gap)
  - Software Testing for Mobile & Embedded Systems (Crypto-misuse in Android Apps)
  - Computer Networks (Web Security and Privacy Topics)
  - Database Management (SQLi Attacks and Defenses)
  - Database Management (Access Control and Database Security)
  - Advanced High Performance Computing (Scientific Computing Integrity)
  - Data Structures and Algorithms (Command Injection)

Computer Communication
- A Case Study of Heartbleed Vulnerability

- SSL, TLS, and HTTPS
- DTLS (Datagram TLS)
- TLS Heartbeat Extension
- OpenSSL Heartbleed Vulnerability and Impact
- OpenSSL Heartbleed Vulnerability Security Patch
- Discussions
  - HTTPS Administration
  - Certificate Revocation and Scalability
  - Support for Critical Projects
  - Vulnerability Disclosure
  - Notification and Patching
  - ……

Software Engineering

- Engineering Your Password Security

- Problems of Passwords
- Some Popular Solutions
- Password Creation
- Password Management
- Single Sign-On (SSO) Systems Security

Operating Systems

- VM Introspection and the Semantic Gap

- Virtualization, VM, VMM
- Virtualization and Security
- Virtual Machine Introspection (VMI) can be very useful in security applications
  - Semantic gap exists
  - Weak semantic gap has been largely addressed
  - Strong semantic gap is still there

Software Testing for Mobile & Embedded Systems
- Crypto-misuse in Android Apps

- Commonly Used Crypto Primitives
- Common Rules in Cryptography
- CryptoLint --- a light-weight static analysis tool
  - System Design and Implementation
  - Evaluation and Results
  - Case Studies
  - Limitations
  - Mitigations

Computer Networks

- Web Security and Privacy Topics

- Symantec Internet Security Threat Report
- Vulnerability Analysis of Browser-based Password Managers
- Automatic Detection of Information Leakage Vulnerabilities in Browser Extensions
- Phishing Susceptibility Measurement & Analysis, Design, Education

Class Session Information

Session Symbol	Course Title	Course Level	Institution/ Semester	Class Size
CC	Computer Communication	Grad.	I / I	11
ST	Software Testing	Grad.	I / I	5
SE	Software Engineering	Undergrad.	I / I	24
OS1	Operating Systems	Grad. & Undergrad.	I / I	27
OS2	Operating Systems	Grad. & Undergrad.	I / II	23
CN	Computer Networks	Undergrad.	II / II	17

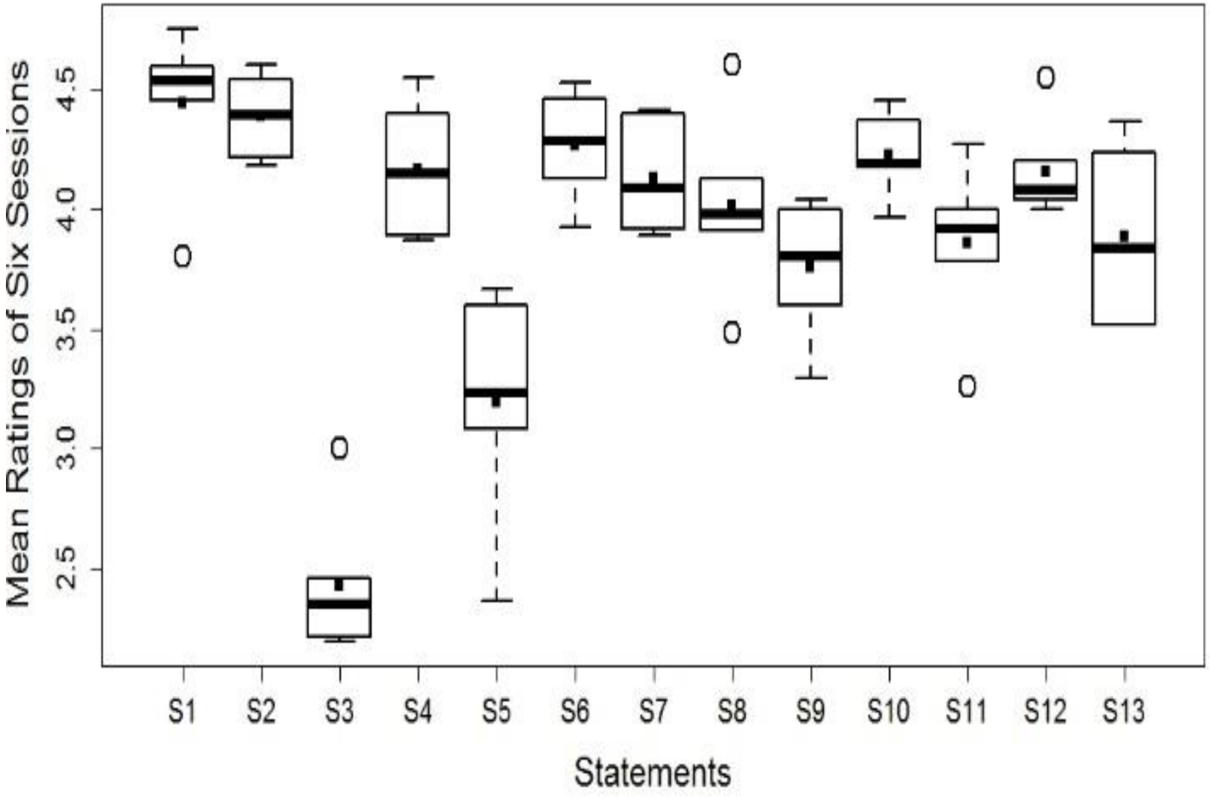
Fourteen Common Survey Questions (1~7)

- General Questions
  - S1: Learning cybersecurity knowledge & skills is important for computer science students.
  - S2: I am interested in learning cybersecurity knowledge & skills.
  - S3: Please rate your current cybersecurity knowledge & skills: (clueless, beginner, intermediate, advanced, total guru)
- Overall Perception of the Cybersecurity Topic
  - S4: The cybersecurity topic discussed in today's class is interesting.
  - S5: The cybersecurity topic discussed in today's class is difficult.
  - S6: The cybersecurity topic discussed in today's class is useful.
  - S7: The cybersecurity topic discussed in today's class is relevant to this course.

Fourteen Common Survey Questions (8~14)

- Overall Perception of the Cybersecurity Topic (cont.)
  - S8: The cybersecurity topic discussed in today's class improved my cybersecurity knowledge and skills.
  - S9: The cybersecurity topic discussed in today's class is helpful for me to prepare for my career.
  - S10: The instructor(s) effectively discussed the cybersecurity topic in today's class.
  - S11: I effectively learned the cybersecurity topic discussed in today's class.
  - S12: I would like to have cybersecurity topics dis-cussed in other non-cybersecurity courses in the future.
  - S13: Today's class motivates me to systematically learn cybersecurity knowledge and skills in the future.
- Open Comments:
  - S14: Please write down comments and suggestions about today's class and learning cybersecurity knowledge & skills in general.

Mean Ratings of Six Class Sessions to S1~S13



(answer options for Likert-scale statements were converted to numeric values)

- The majority of students found the discussed cybersecurity topics interesting, useful, and relevant.
- They would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future.

Specific Questions and Results

- Each questionnaire also contains some questions specific to the cybersecurity content discussed in the class session.
- The questions are designed in pairs for us to evaluate the learning effectiveness in terms of the students' understanding of certain details of the discussed content (**B**)efore the class session and (**C**)urrently.
- Students effectively learned the corresponding cybersecurity topics discussed in the class sessions.

Specific Questions for Operating Systems

SS1B: I understood the basic idea of the Intrusion Detection System (IDS) before reading the paper recommended by the instructor(s) and before today's class.

SS1C: Currently, I clearly understand the basic idea of IDS.

SS2B: I understood that VMI can be useful in security systems such as IDS before reading the paper recommended by the instructor(s) and before today's class.

SS2C: Currently, I clearly understand that VMI can be useful in security systems, especially IDS.

SS3B: I understood the technical details about using VMI in security systems, especially IDS, before reading the paper recommended by the instructor(s) and before today's class.

SS3C: Currently, I clearly understand the technical details about using VMI in security systems, especially IDS.

SS4B: I understood the meaning of the semantic gap in VMI before reading the paper recommended by the instructor(s) and before today's class.

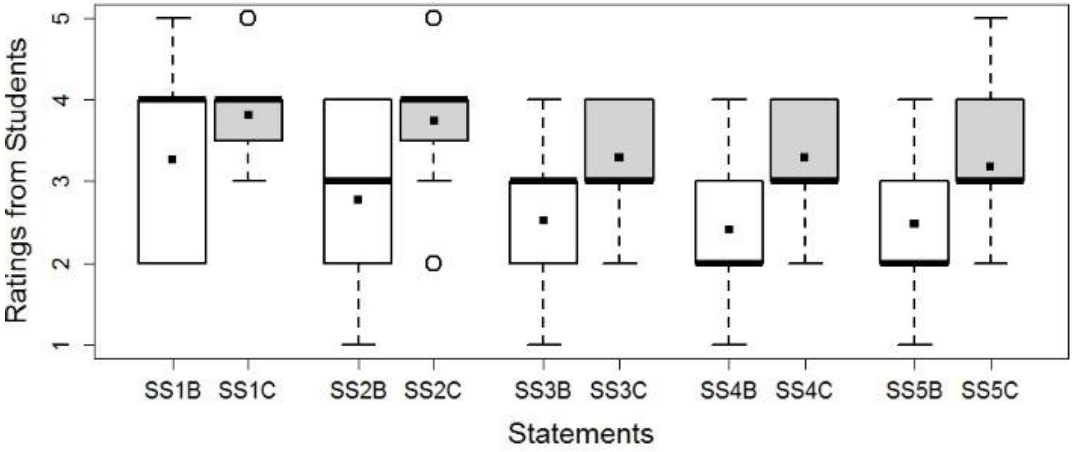
SS4C: Currently, I clearly understand the meaning of the semantic gap in VMI.

SS5B: I understood the difference between the weak semantic gap and the strong semantic gap in VMI-based security systems, especially IDS, before reading the paper recommended by the instructor(s) and before today's class.

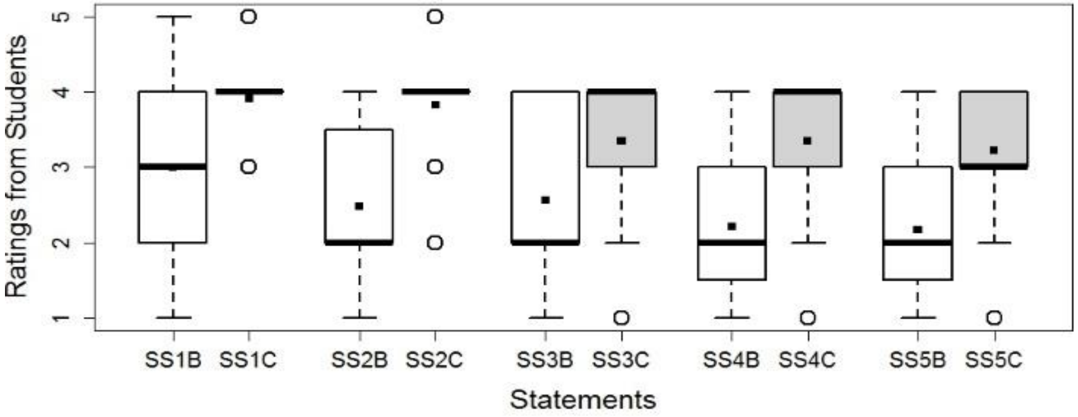
SS5C: Currently, I clearly understand the difference between the weak semantic gap and the strong semantic gap in VMI-based security systems, especially IDS.

Ratings to Specific OS Questions

OS1



OS2



- Students improved their understanding of the IDS and VMI related concepts.
- Mean ratings for all the five paired questions are improved (statistically significant) in both class sessions.
- The spread for all the ratings to the current understanding are also relatively small.

COLORADOSCHOOLOFMINES
engineering the way

Conclusion

- Advocate to further explore the security integration approach
- Explored a viable implementation solution and evaluated its effectiveness
- Evaluated the teaching and learning effectiveness
- Our experience is very encouraging

Thank You!

National Science Foundation
WHERE DISCOVERIES BEGIN

(NSF DGE-1619841) Big Thanks!