Teaching Secure Supply Chain Risk: Experiment in an 'Introduction to Cybersecurity' Course

BY: TERRY DOWNING-HARRIS, SIDDHARTH KAZA, BLAIR TAYLOR, YEONG-TAE SONG

28TH COLLOQUIUM
FOR INFORMATION SYSTEMS SECURITY EDUCATION

CISSE™

TOWSON UNIVERSITY

Importance of Teaching Secure Supply Chain Risk Management (SCRM)

- The Software Supply Chain and the security of software applications purchased through Commercial-Off-The-Shelf (COTS) is a focus of government and industry

- President Biden's "Executive Order Improving the Nation's Cybersecurity," 5/12/2021. Improve the security of software supply chain [1]

- **Government and academic organizations**
  - NIST NICE framework
  - NSA, DHS
  - ACM, and IEEE

All calling for academia to teach **secure Supply Chain Risk Management (SCRM) practices**

Importance of Teaching Secure SCRM:
Challenges: Software Supply Chain & Academia

- Vulnerabilities introduced within Software Supply Chain [2], [3], [4]

- Origin of software used to develop COTS software is usually unknown to customer.
  - Can result in Insecure Source Code
  - Potential for Malicious Objects Embedded into Code [2], [3], [4]

- Supply Chain Attacks (e.g., Solar Winds attack in 2020, Colonial Pipeline and Kaseya).

- Most software engineering programs generally do not teach how to use **secure SCRM**. [5]

Teaching Secure SCRM: Based on NIST Standards

- Higher education institutions can help by teaching undergraduate students

-**secure Supply Chain Risk Management (SCRM)**

-based **on NIST standards**

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

-To help secure COTS software applications [2]

Integration of secure SCRM into Software Engineering Curriculum (for Undergraduates)

- A controlled experiment in “Introduction to Cybersecurity” course at Towson University
- Results, the integration of secure SCRM was effective in teaching secure SCRM to students
- Goal is to develop a model universities can easily replicate to teach secure SCRM

Research Background

- The “faster-cheaper-better” mentality; organizations often purchase COTS third-party software products [2], [3]

- When acquiring software, it moves through a software supply chain
  - It is difficult to oversee, control and ensure its security [2], [3]

- Supply chains can extend globally [2], [4], [5]

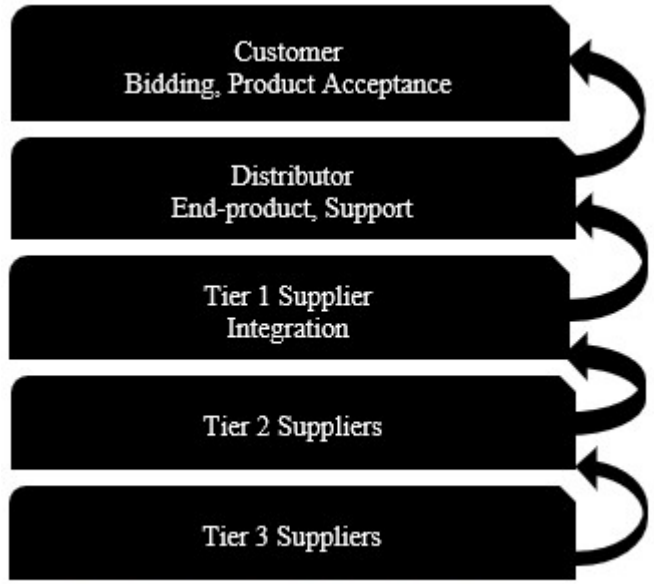

Fig. 1. Software Supply Chain Hierarchy

Research Background

- Generally, supply chain management involves tangible products, that can be controlled [2]

- With software, the product to be delivered is [2], [3]
  - invisible
  - highly complex
  - coded rather than manufactured

- High-profile supply chain attacks increased concern over supply chain attacks and third-party risk [2], [3]

Research Background
Recommendations to Teach secure SCRM

- The National Institute of Standards and Technology (NIST), and the National Initiative for Cyber-security Education (NICE), together known as the NIST NICE Framework. [6], [7]

- In partnership with government, academia and the private sector

- Consist of specified Knowledge, Skills, and Abilities (KSAs) [7]

- KSAs needed to perform cybersecurity work and tasks necessary for each work role in industry

Research Background
Recommendations to Teach secure SCRM

- Table I: knowledge statements from NIST NICE Framework for work role of IT Project Management
- Emphasizes knowledge in secure SCRM. [8], [9]

Table I. Knowledge Statements from NICE framework with a focus on SCRM

Knowledge ID	IT Project Manager (Work Role ID: OV-PMA-002)
	Knowledge Description
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
K0154	Knowledge of supply chain risk management standards, processes, and practices.
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)

Research Background
Recommendations to Teach secure SCRM

- DHS and NSA sponsor the National Centers of Academic Excellence in Cybersecurity (NCAE-C)

- Designate higher educational institutions as a NCAE-C, based on their close alignment to specific cybersecurity-related Knowledge Units (KUs) [10]

- DHS and NSA emphasize the need to teach supply chain security; [10]
  - The part of supply chain management that focuses on managing risk of external suppliers and vendors.

Research Background
Recommendations to Teach secure SCRM

- NCAE-C is currently recommending the following KUs for supply chain security, in Table II [11], [12]

Table II. NSA CAE Knowledge Units focused on Supply Chain Security

KUs	NCAE- C Knowledge Units (KUs)	
	Descriptions	Intent of KUs
2020 KUs	Supply Chain Security (SCS)	The Intent of the Supply Chain Security Knowledge Unit is to provide students with an understanding of the security issues associated with building complex systems out of third party components of unknown (and potentially unknowable) origin.
2019 KUs	Supply Chain Security (SCS)	The Intent of the Supply Chain Security Knowledge Unit is to provide students with an understanding of the security issues associated with building complex systems out of third party components of unknown (and potentially unknowable) origin.

Need More Work on secure SCRM

- Need for more work on secure SCRM
- Using NIST standards
- Taught to undergraduate students in software engineering course.

Integration of Secure SCRM in Software Engineering Curriculum at Towson University

- **Study Design**
- Learning Module Design
- Experiment
- Results

Study Design

- A module-based approach used to integrate secure SCRM into computer science curriculum

- Accomplished by incorporating several NIST standards into software engineering curriculum
  - NIST.IR.7622 Mitigate supply chain risk, in the SDLC
  - NIST SP 800-30r1 Provide guidance on conducting risk assessment
  - NIST SP 800-161r1 Emphasize how cybersecurity risk can exist in software supply chain

- Learning modules contained NIST standards, instructional materials to teach secure SCRM

Integration of Secure SCRM in Software Engineering Curriculum at Towson University

- Study Design
- **Learning Module Design**
- Experiment
- Results

Learning Module Design

- The secure SCRM learning modules fit easily into software engineering course and are self-paced
- Three learning modules created with outcomes defined by Bloom's taxonomy [13]
  - Module#1: Software Supply Chain
  - Module#2: Challenges in Software Supply Chain
  - Module#3: Software Acquisition and Security
- Modules include real-world examples, learning objectives, instructional materials, list of terms

Integration of Secure SCRM in Software Engineering Curriculum at Towson University

- Study Design
- Learning Module Design
- **Experiment**
- Results

Experiment (Pretest)

- An experiment conducted in course: CIS377 Introduction to Cybersecurity at Towson University
  - Experiment group (CIS377.406), twenty-three student participants
  - Control group (CIS377.101), twenty-three student participants

- **Both groups** completed an online **Pretest** in a face-face Lab setting.
  - The **Pretest** did not require any prior knowledge or preparation
  - **Pretest** tested for any previous knowledge or awareness of secure SCRM practices

Experiment (Post-test)

- After Pretest, **Experiment Group** accessed the online secure SCRM learning modules for a week

- After Pretest, **Control Group** was exposed to standard lesson plan for course CIS377

POST-TEST:

- Finally, **Both groups** completed an online **Post-test** in a face-face Lab setting.
  - Experiment group (CIS377.406), eighteen student participants
  - Control group (CIS377.101), twenty student participants

Integration of Secure SCRM in Software Engineering Curriculum at Towson University

- Study Design
- Learning Module Design
- Experiment
- **Results**

Results (Pretest Scores)

- **Independent samples t-tests** were run, and analysis of **Gain Scores** from **Pretest** and **Post-test**

First, Pretest scores were analyzed

- An independent samples t-test revealed that the
  - Experiment group's pretest mean (M = 3.70, SD = 1.490) was not significantly different (at the $p<0.10$ level) than the control group's pretest mean (M = 3.30, SD = 1.222)

- This indicated that the two groups were starting at the same level of knowledge

Results (Post-Test Scores)

Post-test scores were analyzed

- On completing the experiment an independent samples t-test revealed that the
  - **Experiment Group** had a higher mean (M = 9.94, SD = 1.474) in the **Post-test** than the **Control group**'s post-test mean (M = 7.65, SD = 2.231)

- The difference was statistically significant at the $p<0.05$ level.

Results (Post-Test Scores)

- **Experiment Group** had a higher mean (M = 9.94, SD = 1.474) in the **Post-test**

Fig. 2 Mean of Post-test Scores

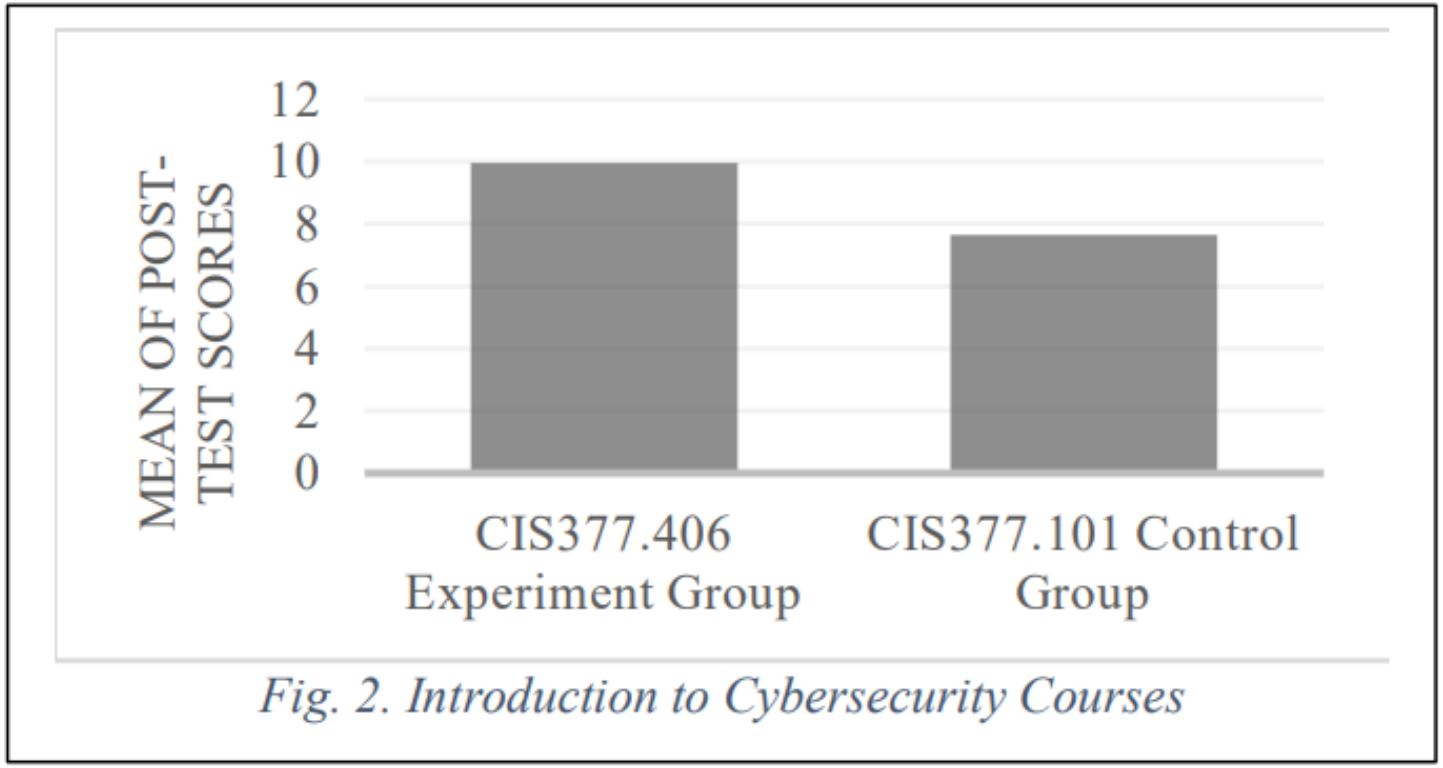

Fig. 2. Introduction to Cybersecurity Courses

Results (Post-Test Scores)

Post-test scores analysis continued

- The **Experiment Group**'s **Post-test** mean (M = 9.94, SD = 1.474) was higher than its **Pretest** mean (M = 3.70, SD = 1.490)
- The difference was statistically significant level ($p<0.05$).

Table III. Experiment Group Higher Gain Score

CIS377 Class Sections	Pretest	Post-test	Gain Score
406 Experiment Group	3.70	9.94	6.24
101 Control Group	3.30	7.65	4.35

Conclusion

- This work **integrated secure SCRM practices** into **software engineering curriculum**

- A successful experiment showed that this integration effectively

  - Taught undergraduate students secure SCRM based on NIST standards

  - Exposed undergraduate students to risks and security issues associated with the software supply chain

Conclusion

- Equips students to meet industry's need for securing the software supply chain
- A model for all universities for integrating secure SCRM into software engineering curricula
- Helps address President Biden's call to improve the security of software supply chain

Future Work

- The findings from this work will be the catalyst for future work involving
- Further experiments in integrating secure SCRM into the cybersecurity curricula
- Further experiments in integrating secure SCRM into the software engineering curricula

Questions

References

- [1] J. R. Biden, “Executive order on improving the nation’s cybersecurity,” *Federal Register The Daily Journal of the United States Government*, vol. 14028, no. 1, pp. 1–47, May 2021.
- [2] N. R. Mead, A. Kohnke, and D. Shoemaker, “Secure sourcing of COTS products: A critical missing element in software engineering education,” in *Proc. of 32nd IEEE Intl. Conference on Software Engineering Education & Training*, May 2020. https://doi.org/10.1109/CSEET49119.2020.9206233
- [3] D. Shoemaker, N. R. Mead, and A. Kohnke, “Teaching secure acquisition in higher education,” IEEE Security & Privacy, vol. 18, no. 4, pp. 60–66, 2020. https://doi.org/10.1109/MSEC.2020.2989644
- [4] S. Weigand. (2021) Supply chain breaches negatively affect 97% of study respondents. [Online]. Available: https://www.scmagazine.com/news/breach/supply-chain-breaches-negatively-affect-97-of-study-respondents
- [5] K. Sigler, D. Shoemaker, and A. Kohnke, *Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product (internal Audit and IT Series) 1st Edition*. Tylor and Francis Group, CRC Press, 2018.

References

- [6] Cybersecurity Education And Workforce Development, National Institute of Standards and Technology (NIST), 2021. [Online]. Available: https://www.nist.gov/cybersecurity-awareness-training-education-and-workforce-development
- [7] National Initiative for Cybersecurity Careers and Studies (NICCS) (2022) Workforce framework for cybersecurity (NICE Framework) [Online]. Available: https://niccs.cisa.gov/workforce-development/cyber-security-workforce- framework#:~:text=The%2520NICE%2520Framework%2520is%2520comprised,grouping%2520of%2520common%2520cybersecurity%2520functions&text=Work%2520Roles%2520(52)%2520%25E2%2580%2593%2520The,tasks%2520in%2520a%2520Work%2520Role
- [8] NICCS. Using the NICE Framework. [Online]. Available: *https://niccs.cisa.gov/sites/default/files/documents/pdf/using%20the%20nice%20framework_pdf.pdf?trackDocs=using%20the%20nice%20fram ework_pdf.pdf*
- [9] ——. (2022) Knowledge IDs: (NICE) cybersecurity framework workforce knowledge. [Online]. Available: https://performatron.risk-redux.io/nice_work_roles/OV-PMA-002

References

- [10] ——. (2022) National centers of academic excellence in cybersecurity (NCAE–C). [Online]. Available: https://niccs.cisa.gov/formal-education/national-centers-academic-excellence-cybersecurity-ncae-c
- [11] ——. (2020) 2020 knowledge units. [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf
- [12] ——. (2019) 2019 knowledge units. [Online]. Available: *http://www.itm.iit.edu/faculty/CAE-CD_2019_Knowledge_Units.pdf*
- [13] L. W. Anderson and D. R. Krathwohl, *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. New York: Allyn & Bacon, 2001.