Development and Analysis of a Spiral Theory-based Cybersecurity Curriculum

N. Dwight Barnette, Godmar Back, Harinni K.Kumar, Paul E. Plassmann, Calvin J. Ribbens,
Vinod K. Lohani

VIRGINIA TECH

Background

Team: Faculty members and graduate students of the Engineering Education (EngE), Computer Science (CS), and Electrical and Computer Engineering (ECE) Departments in the College of Engineering at VT.

Goal:

Enhance Cybersecurity education opportunities at Virginia Tech by integrating cybersecurity modules into four Computer Science (CS) courses using a spiral theory framework.

Objectives:

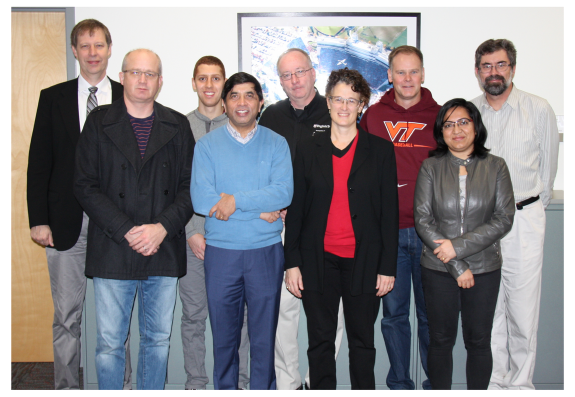
1) Development and implementation of a unique curriculum delivery model in cybersecurity into Computer Science and Computer Engineering curricula using Jerome Bruner's spiral curriculum theory
2) Engineering education research to evaluate students' cybersecurity learning experiences

Scientific Impact:

- Research findings regarding how students learn and are motivated by cybersecurity concepts
- Curriculum development and implementation experiences to infuse cybersecurity into a large engineering program

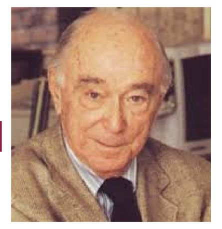
Broader Impact:

- Enhance recruitment of undergraduates into the CyberCorps and VT-Scholarship for Service program at VT
- Increase the number of graduates who accept employment or pursue graduate studies in the cybersecurity field
- Develop an education theory based curriculum model for cybersecurity



Methods

Spiral-theory:

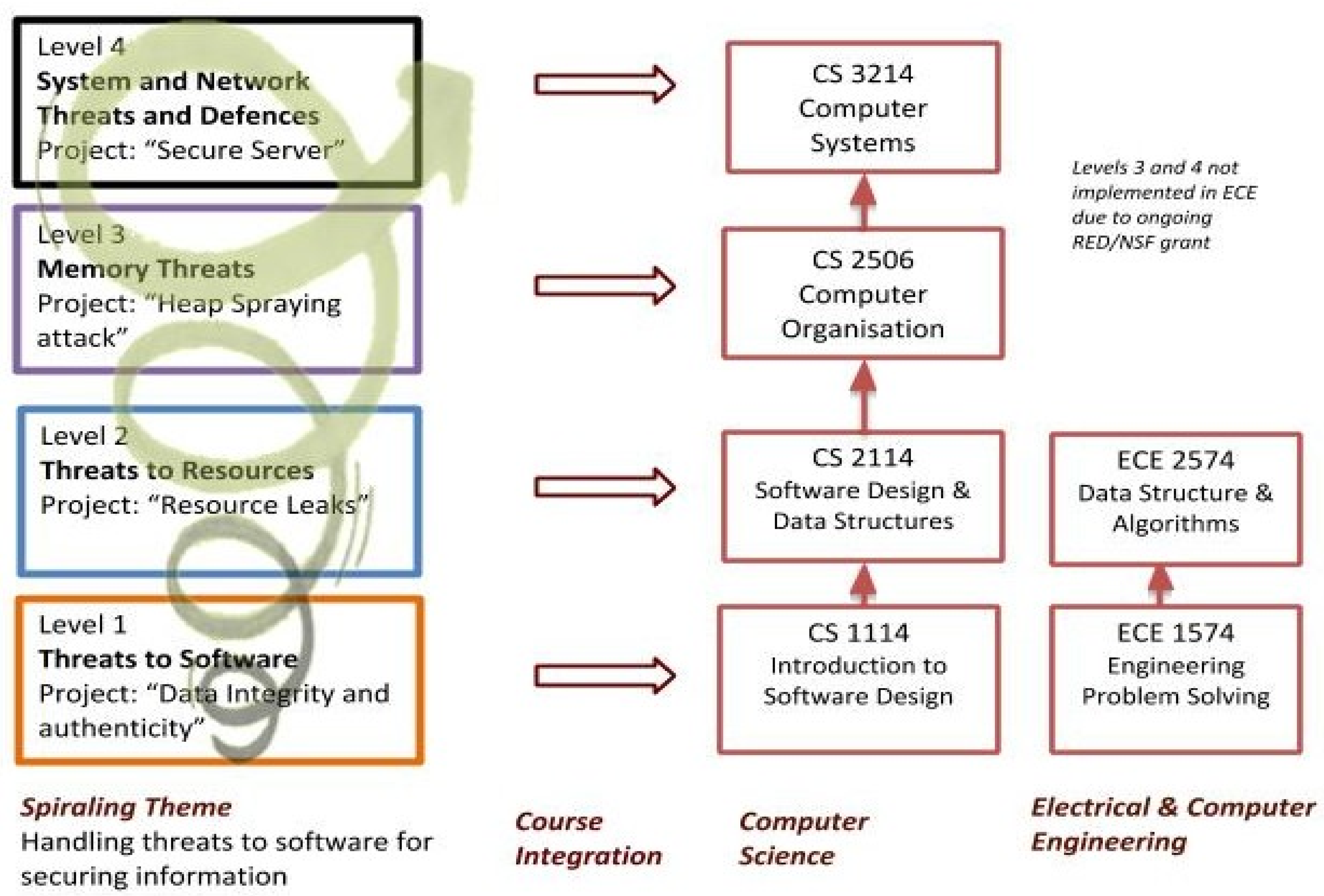


The twentieth century psychologist Jerome Bruner proposed the concept of the spiral curriculum. One key to this idea is that the learning curriculum could be arranged so that the central questions, or themes in a discipline, would be returned to repeatedly as learners advance in their knowledge and intellectual capacity.

Process for the Development and Implementation of Cybersecurity Spiral Curriculum

1) Identification of the foundational courses at four levels in CS and ECE curricula
2) Definition of the spiraling theme
3) Identify the concepts that should be covered for weaving the theme into the CS and ECE curricula
4) "Spiral" the cybersecurity concepts into the foundation courses
5) Develop the spiraling learning objectives based on the concepts
6) Review existing course syllabi to identify where cybersecurity concepts can be presented and where an authentic activity can be implemented
7) Develop learning module including course content and the authentic activity, which is a real-life, open ended problem, situated in social context, resembles cybersecurity practice, involves active student participation and working as a community where each member has different roles
8) Implement the learning modules
9) Develop assessment instruments and conduct pilot evaluation
10) Iterate though steps 6, 7, and 8 depending on the feedback received after analyzing the pilot evaluation data
11) Conduct complete evaluation of the learning modules

Spiral-theory based Cybersecurity Curriculum Model



Current Status: **Learning modules for all 4 levels been designed, developed and implemented in the courses. *Levels 3 and 4 were implemented in CS courses only. Due to an ongoing RED grant in the ECE department, levels 3 and 4 could not be implemented in ECE courses.**

Concepts Covered in the CS Curriculum:

	Confidentiality	Availability	Integrity	Authenticity	Anonymity	Assurance
Level 1						
Level 2						
Level 3						
Level 4						

Concepts Covered in the ECE Curriculum:

	Confidentiality	Availability	Integrity	Authenticity	Anonymity	Assurance
Level 1						
Level 2						

Concept covered in lecture and authentic activity *Concept covered in lecture*

Challenges:

- Coordination with the NSF-Revolutionizing Engineering Departments (RED) grant in the ECE department
- Substantial enrollment growth
- Obtaining IRB approvals to conduct research in timely manner
- Faculty engagement

Examples of Learning Objectives, Modules and Activities

Example Learning Objectives from each level :

L1: Define cybersecurity principles: integrity and authenticity

L1: Explain the purpose of ensuring the integrity and authenticity of data in real-world scenario

L2: Describe potential security threats to resources

L2: Apply defense strategy to protect resources

L3: Describe potential security threats to system integrity

L3: Design exploits that can compromise system integrity

L4: Summarize potential threats to authenticity, confidentiality, and anonymity

L4: Implement a stateless user authentication method for a web server

Lecture topics:

L1: History of Cybersecurity, introduction to the CIA/AAA, cybersecurity goals, Adversary/Threat model and One-Way hash functions

L2: Introduction to Denial of Service attacks with focus on cache flooding

L3: Introduction to Heap Spraying attack

L4: Transport Layer Security review, introduction to stateful and stateless authentication methods and JSON Web Tokens(JWT) to implements stateless authentication

Authentic Activity:

L1: Students developed a Java tool to perform verification on Digitally Signed records

L2: Students implemented a linear cache and improved it by adding LRU eviction policy to handle cache overload.

L3: Students replicated a realistic heap spraying attack using JavaScript with as assumed vulnerable web browser

L4: Students developed a C based web server and implemented stateless authentication using JWT

**L1: Level 1, L2 : Level 2, L3: Level 3, L4: Level 4*

Results for students' level of confidence with the learning modules across all levels

Pre and post-survey: Data collected: 1) demographic information, 2) students' perceptions toward learning objectives, 3) content questions on each of the learning objectives, and 4) students' perceptions on the interest and usefulness of the cybersecurity concepts.

LEVEL	MEAN PRE TEST SCORE	MEAN POST TEST SCORE	P VALUE CHANGE FROM PRE TO POST TESTS
1	2.99	4.29	<0.0001 (pre < post)
2	3.15	4.06	<0.0001 (pre < post)
3	2.54	3.17	<0.0001 (pre < post)
4	2.98	3.38	<0.0001 (pre < post)

- Table on the left represents sample results which reflects students' level of confidence with learning modules across all the levels
- About 1400 student took participated in the surveys across all levels
- Mean scores for pre and post test reflect the student scores on the Likhert scale questions assessing students' perceptions towards learning objectives
- Significant change from pre to post-test (p-value <0.0001) of students' agreement on meeting the learning objectives of each level
- Based on ANOVA test results, no significant difference was observed in student confidence based on gender, academic level or ethnicity

Publications & Posters :

D. Basu, H.K.Kumar, V. K. Lohani, N. D. Barnette, G. Back, P. E. Plassmann, C. J. Ribbens. Integration and Evaluation of Spiral Theory based Cybersecurity Modules into Core Computer Science and Engineering Courses. Paper accepted for SIGCSE 2020.

D. Basu, N. D. Barnette, G. Back, D. McPherson, W. M. Naciri, P. E. Plassmann, C. J. Ribbens, V. K. Lohani, M. Ellis, and K.R. Gantt. 2018. Development and Analysis of a Spiral Theory-based Cybersecurity Curriculum: (Abstract Only). In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)

Acknowledgement: This work has been supported by the National Science Foundation through the Secure &Trustworthy Cyberspace program (Award number: 1623047). This work has also been supported by the Departments of Engineering Education, Computer Science, and Electrical and Computer Engineering in the College of Engineering and the Institute for Critical Technology and Applied Science (ICTAS) at Virginia Tech. Any opinions, findings, conclusions or recommendations expressed in this presentation are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or Virginia Tech.

Presented at
NSF/SaTC Meeting: Oct. 28-29, 2019
Alexandria, VA