**Goal:** Enhance cybersecurity learning experiences of students at Virginia Tech’s large engineering program

**Objectives:**
- 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
- Engineering education research to evaluate students’ learning experiences

**Scientific Impact:**
- Research findings regarding how students learn and get motivated about cybersecurity concepts
- Curriculum development/implementations and experiences to infuse cybersecurity into a large engineering program

**Development and pilot implementation of learning level-1 (L1) completed during Fall 2016**

**Learning Objective of L1:**
LO1: Define cybersecurity principles: integrity and authenticity
LO2: Define and explain an adversary model
LO3: Describe potential security threats from non-validated input
LO4: Explain the purpose of ensuring the integrity and authenticity of data in real-world scenarios
LO5: Apply the process of ensuring data integrity and authenticity through authentic problem solving

**Implementation in CS1114 with 423 students**

**Lecture topics:**
- The Cyber security CIA/AAA goals (Confidentiality, Integrity, Availability / Authenticity, Anonymity, Assurance) was stressed
- The Adversary/Threat model assumptions and attack vectors were covered
- The Diffie-Hellman public-key cryptography algorithm was explained and demonstrated to students
- Concept of Digital Signatures was introduced
- One-way hashing, as used in digital signing, and its differences from encryption was presented
- The processes of Digital Signature generation and verification were covered

**Authentic Activity:**
Students coded a Java program to perform verification upon records in file that were digitally signed generating a report

**Research Questions:**
1. How effective are the spiral theory-based learning levels in enhancing students’ core-knowledge and skills in cybersecurity?
2. How does students’ motivation vary across gender, ethnic backgrounds, academic levels, and disciplines when participating in the cybersecurity learning levels?

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

**Post-Survey Results (n=199 out of 600+ students)**
Computer Science: 25%; Computer Eng.: 11.22%; General Eng.: 18.37%; Other Disciplines: 45.41%

**Students’ Perceptions on Motivational Constructs**

<table>
<thead>
<tr>
<th>Perception</th>
<th>Strongly Agree (%)</th>
<th>Agree (%)</th>
<th>Somewhat Agree (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>the cybersecurity initiative was useful to his/her future</td>
<td>20.10</td>
<td>39.03</td>
<td>25.10</td>
</tr>
<tr>
<td>the instructional method and cybersecurity initiative were interesting or enjoyable</td>
<td>15.39</td>
<td>36.45</td>
<td>26.00</td>
</tr>
</tbody>
</table>

Interested in meeting the PIs? Attach post-it note below!