# Captivology-Stimuli-based Learning (CAPITAL) of Big Data Security (BigSec): Towards a Science/Engineering, Career-Oriented Training
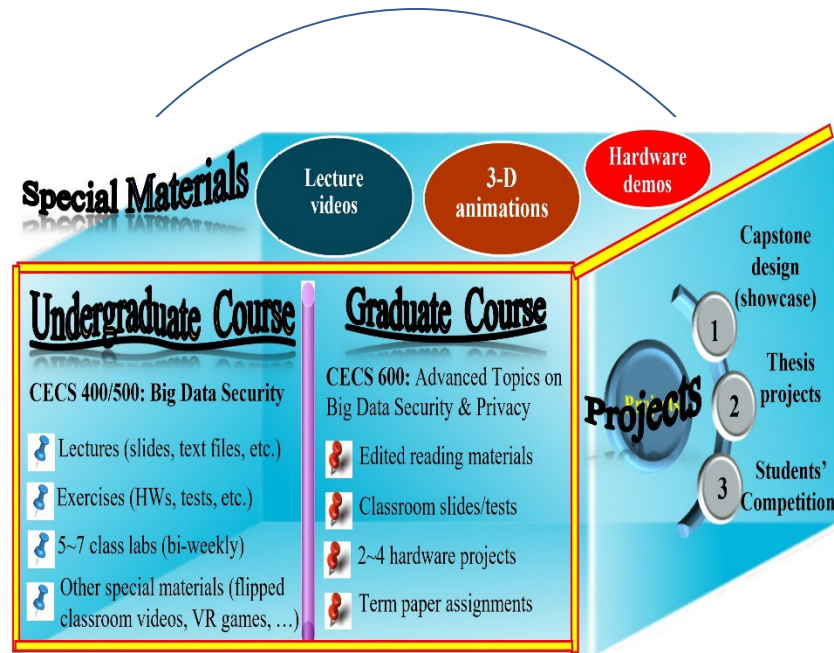
## Challenges:

● In today's higher education, there are very limited BigSec (big data security) educational activities that target the comprehensive, profound understanding of the technical details (BigSec attack models, defense solutions, security software design, etc.), for both undergraduate and graduate students.

## Solution:

We propose to enhance the students' BigSec education through two types of learning stimuli: Feeling of freshness (FoF) and sense of accomplishment (SoA).

**Special Materials**
- Lecture videos
- 3-D animations
- Hardware demos

**Undergraduate Course**

**CECS 400/500: Big Data Security**
- Lectures (slides, text files, etc.)
- Exercises (HWs, tests, etc.)
- 5~7 class labs (bi-weekly)
- Other special materials (flipped classroom videos, VR games, …)

**Graduate Course**

**CECS 600:** Advanced Topics on Big Data Security & Privacy
- Edited reading materials
- Classroom slides/tests
- 2~4 hardware projects
- Term paper assignments

**Projects**
1. Capstone design (showcase)
2. Thesis projects
3. Students' Competitions

Education/training materials developed:

Two complete, semester-long Bigdata security courses: . lecture videos, interactive 3-D animations, and hardware-based demos.

## Scientific Impact:

The proposed CAPITAL-based pedagogy is *transformative* to the education of other cybersecurity areas, such as cyber crime, digital forensics, reverse engineering, software assurance, etc.

## Broader Impact and Broader Participation:

This development will also enhance the UA's minority education through our unique support program - *Multicultural Engineering Program (MEP)* that has achieved an overwhelming success in the last decade.