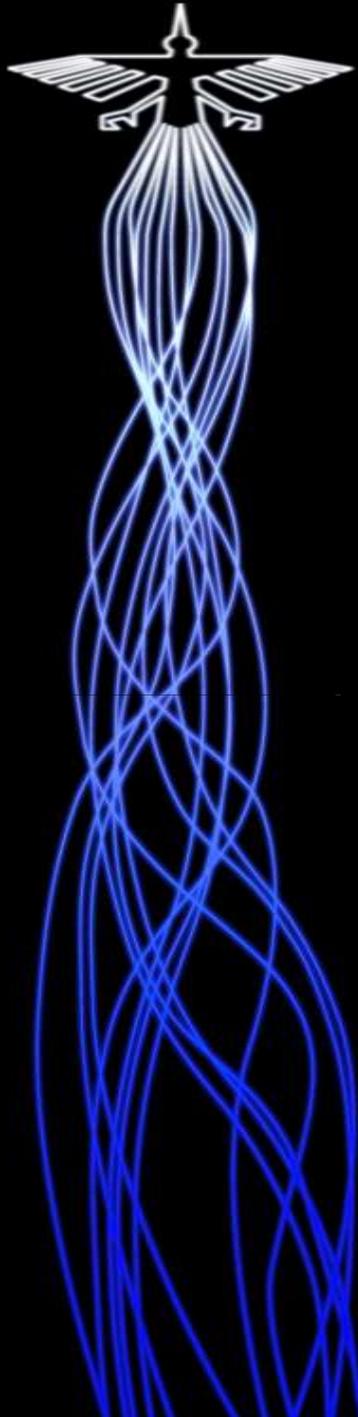# Moving Secure Software Assurance into Higher Education:

A Roadmap for Change

The Issue

Software defects are avenues of attack that criminals, terrorists, or hostile Nations can exploit.

Since software defects are a historical given the entire industry will have to alter its behavior in order to have effective change

The only way to get leverage for such massive social change is through formal education programs

These might start as low as middle school and articulate upward all the way to advanced graduate study
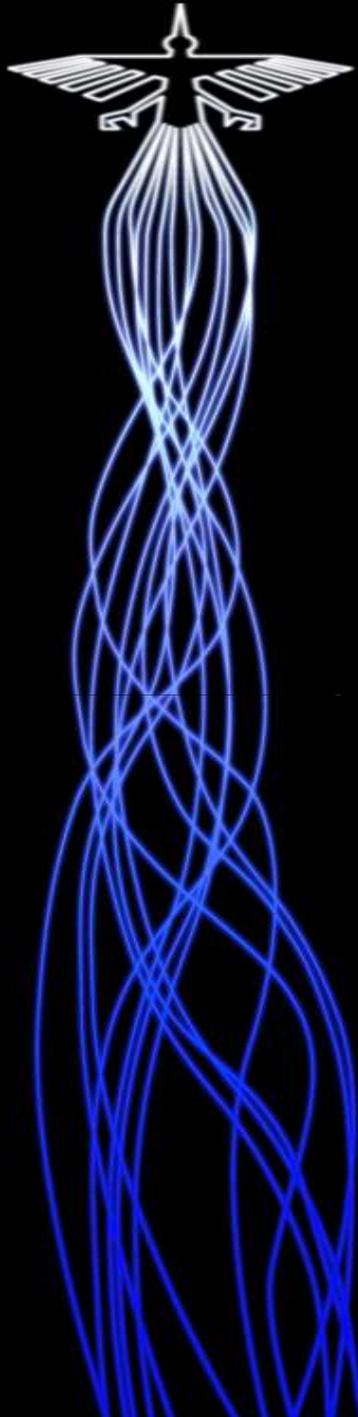
The Current Problem in Education

We still do not fully understand the shape of the field

It is not exactly clear what knowledge and skills ought to be taught.
- **There are 13 separate "official" definitions for SwA**
- **77 synonyms**
- **Practically no literature in most categories**

Worse, there is no common agreement about the activities that might legitimately comprise the SwA process itself
- **Most SwA knowledge used to be called SQA**
- **There are five different disciplines**

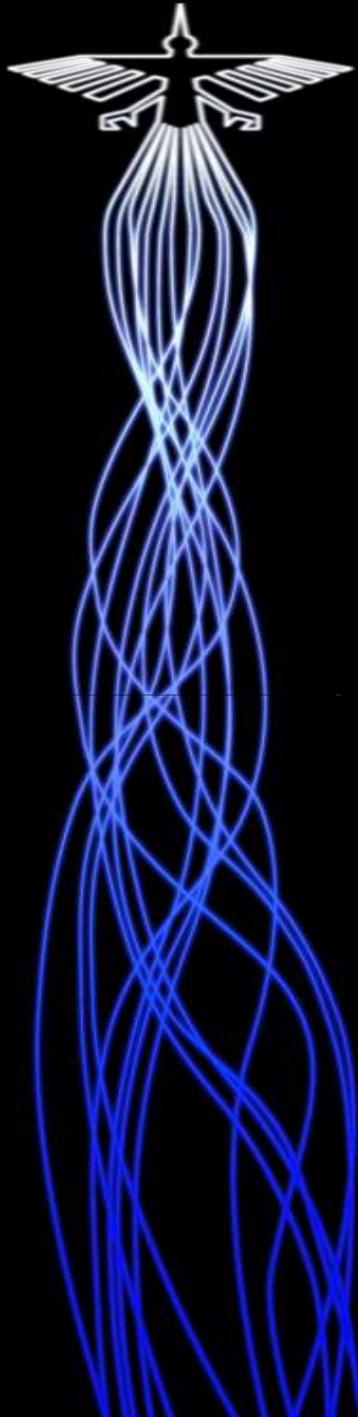CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

The Other Problem with Education

It is not clear how to best deliver that knowledge to all of the relevant constituencies.

Educational institutions are very diverse

Computer education programs are also very diverse and focused at all levels from CCs to Doctoral work
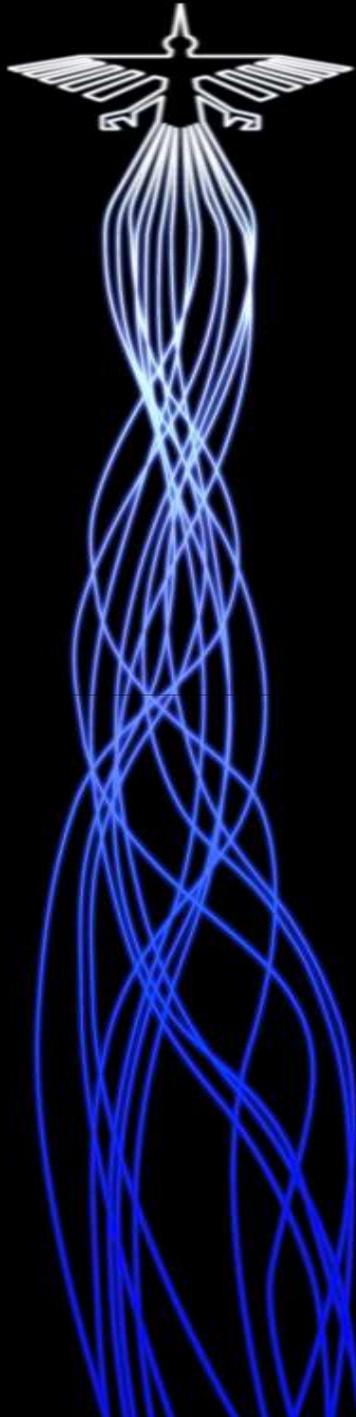
Our Approach

This presentation outlines the results of a two year intensive effort to catalogue all available software assurance knowledge.

It will also explain how we packaged that knowledge in a form that can be used best:

- By all types of educators

- In all types of learning situations.

Packaging the Knowledge for Dissemination

- The aim of the project was to *create customizable courseware content and teaching/learning strategies*

- *For the purpose of disseminating secure software assurance knowledge*

- The objective of year one of this study was to formally characterize all available Software Assurance knowledge

- Then we identified the educational requirements by:
  - Developing a learning topic list using conceptual roadmap
  - Breaking down each topic into discrete learning elements
  - Defining learning objectives for each element

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES
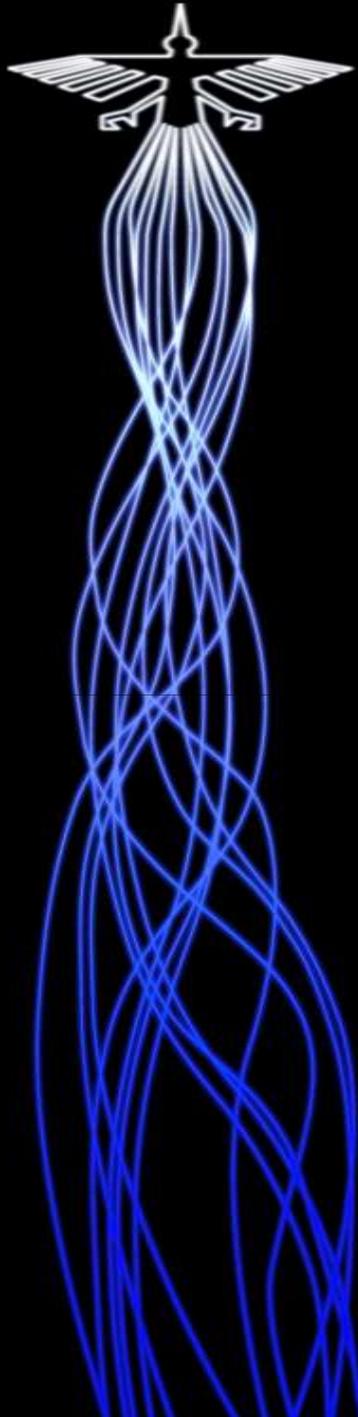
Building the Teaching and Learning Process

– ISO 12207/IEEE 12207.0 Specifies Three Topic Areas
  - Development of Secure Code
  - Sustainment of Code Security
  - Acquisition of Secure Code

– Development of Secure Code was Decomposed further to
  - Understanding the Threatscape (Threat Modeling)
  - Secure Coding Methods and Techniques

– Sustainment of Secure Code was Decomposed further to
  - Ethical Hacking (as operational testing)
  - Secure Sustainment
  - Secure Software Process Management

Teaching and Learning Process

Threat/ Risk Identification → Specification of Security & Functional Requirements

Architectural Risk Understanding → Design of Software Functionality based on Requirements

Secure Coding Techniques → Coding of Security & Functional Requirements

Ethical Hacking → Testing of Security & Functional Requirements

Secure Sustainment → Sustainment of Security & Functional Requirements

Acquisition of Secure Products

involves

involves

involves

Packaging of Content

- We then packaged all relevant software assurance content into discrete learning elements

- Each learning element is applicable to one or more competencies and/or learning environments

- The packaging approach required us to:
  - **Develop content from the NSAR by learning requirement**
  - **Prepare table of learning specifications for each module**
  - **Estimate Bloom learning level for each element**
  - **Define behavioral objectives**
  - **Define Evaluation Criteria**
  - **Define Evaluation Process**
  - **Define Delivery Approach for learning module**

CENTER for CYBER SECURITY and INTELLIGENCE STUDIES

Mapping Content into Existing Curricula

- As a final step, the project team conducted a beta test of the train-the-educator sessions in five divergent settings.
    - Training environments
    - Major State Universities
    - Smaller and Private Universities
    - Community Colleges
    - High Schools

- The partner schools of the International Cybersecurity Coalition were given training in the use of the i-pad based Software Assurance Mobile Instructional (device) SAMI

- The SAMI contains and conveys all of the material developed as part of this project.

CENTER for
CYBER SECURITY
and
INTELLIGENCE
STUDIES

Mapping Content into Existing Curricula

- Thus educators will have six fully developed courses at their fingertips at all times

- Recommendations on how to best utilize the SAMI to disseminate secure software assurance knowledge were the final deliverable for this project

- The results of the beta test of the SAMI approach will be reported at SSTC and AMCIS

CENTER *for* CYBER SECURITY *and* INTELLIGENCE STUDIES

Thank You for Your Attention

Dan Shoemaker - shoemadp@udmercy.edu

Professor

Computer and Information Systems

Senior Research Scientist, Center for Cybersecurity and Intelligence Studies

University of Detroit Mercy