– Short Topic Submission –
SEED: 25 Hands-on Labs for Information Assurance Education

Wenliang Du
Department of Electrical Engineering & Computer Science
Syracuse University, Syracuse, New York 13244
Email: wedu@syr.edu. Tel: 315-443-9180

Intended Audience: The topic is intended for the educators who teach information assurance courses at the undergraduate and graduate levels. It is also intended for the educators who provide professional training in the information assurance field.

Intended Outcome: The audience will learn 25 well-developed hands-on labs for information assurance education. These labs cover a wide spectrum of topics in security, so most audience should be able to find several labs that they can use in their classes.

Topic Description: It has been widely known that learning-by-doing can significantly enhance student's learning in many disciplines, including information assurance (IA) education. Eight years ago, due to the lack of well-design hands-on projects for IA education, we started to develop our own projects. The effort was initially funded by an NSF CCLI Phase I grant in 2003, and was later continuously funded by a Phase II grant in 2006. The objective of the effort is to develop a suite of labs that cover a wide spectrum of principles, ideas, and technologies that are essential for information assurance. We call these labs the SEED labs (SEED stands for SEcurity EDucation).

After 8 years' working on the project, we have developed 25 labs, covering topics ranging from software security, operating system security, network security, and web security. Each lab provides students with a list of well structured activities that focus on one or few particular security attacks, principles, concepts, and techniques. The labs are divided into three categories: (1) The first category consists of vulnerability and attacks labs. The objective is to give students first-hand experiences in attacking vulnerable programs, systems, or networks (all in a contained environment). (2) The second category consists of exploration labs. The objective of these exercises is to coerce the students to explore or play with an existing security functionality. Exploration labs are like a "guided tour" of a system, in which, students can "touch" and "interact with" the key components of a security system to either learn or question the underlying security principles that the system is based on. (3) The third category consists of design and implementation labs. Their objective is to help the student understand the concepts of secure system development. For this type of labs, students are expected to design a system that provides a specific security functionality.

Over the last 7 years, we have used the SEED labs in two graduate and one undergraduate security courses. We have been revising those labs based on student feedbacks. Now, most of the labs are quite stabilized, and are ready for use by other instructors. So far, 15 other universities have informed us that they have used some of our SEED labs in their courses. Since 2007, the labs have been downloaded for over $40,000$ times from the computers outside of our university network.

In this short topic session, I plan to do the followings: (1) Introduce the lab environment used by the SEED labs. (2) Present a subset of the SEED labs, so the audience can get an idea of what these labs look like. All the labs can be downloaded from our URL `http://www.cis.syr.edu/~wedu/seed`. (3) Share with the audience our own experience of using these labs in the classroom. Rigorous evaluation has been conducted for each SEED lab, and the evaluation results will be presented as well.