Introducing the Principles of Cyber Security at an Undergraduate Level
Poster Abstract

Brian-Thomas Rogers, Aliena Rogers, Colin Kautz, Lucinda M. Caughey & Joshua L. Smith

Conference: Midwest Instruction and Computing Symposium
April 19th – 20th, 2013

With growing awareness to the vulnerabilities of computer systems and architectures, software engineers are tasked to change their approach to programming. Many major companies have recently been victims of cyber warfare attacks that have garnered public attention [1], [2]. The goal at the University of Illinois Springfield (UIS) is to augment the current undergraduate curriculum to encourage a more prominent security-centric approach to software development. At UIS, we believe that cyber security should not be a course that our students take, rather it should be an intrinsic attribute of many, (if not all) undergraduate computer science classes.

The UIS computer science program focuses on teaching programming using Java as an introductory language. This involves nine courses that cover the major principles in Java programming. At the undergraduate level UIS also offers between six and 10 networking courses each semester. Current economic realities encourage degree programs to do more with less, and in this spirit, we have decided that it is preferable to include security topics within our current course offering rather than to create new courses (which would require increased faculty and resources).

This poster will focus on the approach, cause, and effects of introducing a cyber security centric paradigm throughout the core courses of our degree requirements rather than having a single elective course. We believe that cyber security should be introduced at the first level of programming and should be encouraged throughout degree course progression.

Introductory programming courses should focus on secure programming, i.e., that which enforces properly handled user input, data type, and scope. This will alleviate many of the major problems currently being faced with software vulnerabilities of buffer overflow and SQL injection. Higher levels of programming should focus on data encapsulation and obscurity. By enforcing simple standards of data protection we will find ourselves creating more secure programs in a timely manner.

Courses pertaining to the use of data structures and algorithms should encourage the use of efficient and safe practices when transporting and manipulating data. We will explain that complex algorithms should have access to and be able to manipulate only the data needed to perform the calculations. Enforcing a well-planned class in data structures and algorithms will provide a more secure application and also increase modularity.

In Operating System and Computer Organization classes students typically learn the fundamentals of memory and process management. An emphasis on computer security at this level is important; the result of unsecure programming in kernel-level functions frequently lead to flaws that result in Zero-Day

exploits and attacks [3]. This is particularly important due to the nature of the now open sourced operating systems such as Ubuntu, Debian, and Android. An understanding of the types of vulnerabilities that such platforms have will lead to conscience decisions and good secure thinking when developing for a certain OS.

As a laboratory enhancement, we have recently built a Cyber Warfare Arena astutely named 'The Jungle'. This is a closed network containing multiple machines using many different operating systems. The idea behind The Jungle is to enable students to be both “black hat” -hack other machines and “white hat” -defend the systems against other hackers. A strongly competitive environment like this will encourage the students to work harder and longer on problems and solutions to real world cyber threat scenarios. When The Jungle has maintained an acceptable level of up-time we will encourage other universities to send their students and faculty to UIS to experience an environment built for threat activity and anlysis.

In conclusion, introducing the principles of cyber security at an undergraduate level will not only produce a higher quality software developer but also increase the awareness of insecure applications. At UIS we believe that this is a priority and are actively encouraging other universities to consider our approach to make our computer system landscape more secure.

References:

[1] Skidmore, Micah, “U.S. Companies Face Increasing Cyber Attacks from China” http://www.businessinsurance.com/article/20130227/NEWS09/130229841 retrieved February 28, 2013

[2] Chakraborty, Barnini, “US officials addressing cyber threat at 'highest levels' with China, on heels of hacker report” http://www.foxnews.com/politics/2013/02/19/us-raising-highest-levels-cyber/#ixzz2OKWdjMGj” retrieved February 28, 2013

[3] “Zero-Day Vulnerabilites” http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities retrieved February 24, 2013