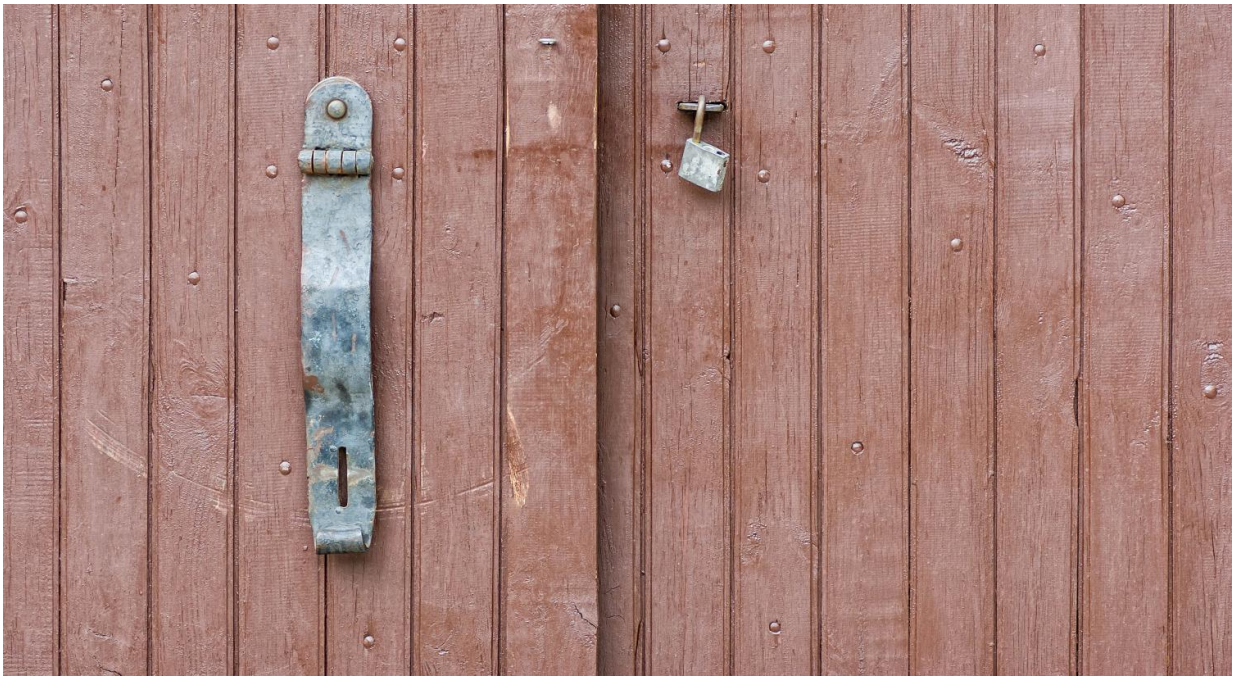
Can cybersecurity crack the undergraduate curriculum?

May 16 2016



Credit: Morgridge Institute for Research

In a time when million-dollar security breaches of major corporations regularly make headlines and complicate lives, computer science undergraduates at America's universities remain surprisingly underexposed to basic cybersecurity tactics.

The Software Assurance Marketplace (SWAMP), a national

cybersecurity facility housed at the Morgridge Institute for Research at the University of Wisconsin-Madison, has been working to address this skills gap through a unique partnership with Bowie State University in Maryland. The SWAMP offers a rich and accessible suite of software security tools that Bowie State has been integrating into undergraduate coding courses, giving students an efficient way to examine and rid their code of security weaknesses.

The partnership offers a national model for integrating cybersecurity into the curriculum.

Funded by the Science and Technology Directorate of the Department of Homeland Security (DHS), the SWAMP is designed to give software code developers a simple, one-stop resource to examine code with a multitude of both open-source and commercial assessment tools. Now in its second year, the SWAMP plans to expand its current suite of 19 assurance tools covering five common software languages to 30 tools covering 11 languages by the end of 2016.

The academic benefits of this resource have been transformational for students of Dr. Lethia Jackson, a Bowie State associate professor of computer science who is implementing the assurance testing in four of the school's sophomore- and junior-level coding courses that attract 50-75 students per semester.

Jackson established a code review process in the classes, where graduate and undergraduate researchers submit student-produced code into the SWAMP continuous assurance pipeline. The team, called the Forensic Technology Information Cyber Squad, works with students to identify where and why code is vulnerable, and determines a path to correction. This process is repeated until the team is reasonably assured the code is free of weaknesses.

"My research students are becoming what I consider to be prolific programmers by using the SWAMP," Jackson says. "Now they not only write code, but they can read and interpret other people's code for errors, which will be necessary for any job in this field."

Security company CloudPassage conducted a 2016 analysis of the top 121 U.S. computer science programs, and found that only three programs require at least one cybersecurity course for a degree. It found many programs offer no cybersecurity curriculum at all. Given the high-stakes nature of cyber-threats, why would universities not already be arming students with a curriculum to help thwart malicious activity?

The answer is based on the rapid-fire evolution of computing in everyday life along with the ubiquitous rise of the Internet, says SWAMP Chief Scientist Barton Miller, a UW-Madison professor of computer science.

"Two decades ago, big software systems for things like payroll and inventory ran on a mainframe that was not connected to anything else," says Miller. "There was no, what we call in security, 'attack surface,' or that part of your software that can be touched by an outsider."

Today, all things digital have some kind of attack surface, from phones to cars to homes, to all transaction tools involving customers. This shift has given rise to an underground industry that generates 4,000 cyber-attacks daily and produced $18 billion in credit card fraud in 2015 alone, according to estimates by IBM.

Bugs in software used to be primarily a reliability concern, causing the nuisance of systems crashing and time and data being lost, Miller says. Now that they are matters of great economic and national security risk, universities face an urgent challenge to address cybersecurity not just in separate courses or specialties, but within the code development culture

itself.

Computer science programs nationwide are under tremendous pressure to increase enrollments and graduate more talent to meet shortages, Miller says. As enrollments and class sizes increase, programs also need to scale these labor-intensive cybersecurity practices into larger classes without taking valuable learning time away from students.

Miller says that's a big advantage of the SWAMP. The resource is designed to eliminate overhead and time-consuming downloads and continual updates, making it easy to plug-and-play in the classroom environment and scale to a growing community of users.

"As part of normal code hygiene in computer science classes, I'd like to see faculty say, 'Your assignment can be turned in after it's run through the SWAMP and gets a clean bill of health,'" Miller adds. "This would be fast and efficient, with little time sink for the student."

Jackson says these skills not only will improve future code, they must be applied to the current infrastructure of installed software. "When many of our students return from summer internships, they say their main job was to convert already existing code into secure code. That was our first wake-up call."

Bowie State's computer science department is documenting this daily activity of code review and error detection, and compiling it into a comprehensive secure coding book that defines common errors and possible fixes. Jackson says the goal is to share this book with other universities, beginning with Bowie State's own network of 12 historically black colleges in the United States.

Miller says cybersecurity has been a game of catch-up in industry as well as academia, and remains a hard sell in some environments. But students

trained in security will bring that mindset and expectation set to employers, he says.

Major companies like Microsoft and Google already have strong security cultures, but companies where software is just a portion of their business may not respond "until they actually get hit by something really bad."

"We see a lot of closing of the barn doors after the horses get out," he says.

SWAMP Director Miron Livny, a UW-Madison computer science professor and Chief Technology Officer of the Morgridge Institute, says supporting educational customers is a cornerstone of the project. "We hope the success seen by Bowie State of translating SWAMP capabilities into a powerful classroom tool will soon be followed by others," he says.

Provided by Morgridge Institute for Research

Citation: Can cybersecurity crack the undergraduate curriculum? (2016, May 16) retrieved 28 June 2024 from https://phys.org/news/2016-05-cybersecurity-undergraduate-curriculum.html