New Approaches to Cybersecurity Education Workshop

June 9-10, 2018, in New Orleans, LA

Proposal Submitted for the Steering Committee's Consideration

From Seth Hamman, Ph.D.

Author Academic Bio

Seth Hamman received the B.A. degree in religion from Duke University in 2002, the M.S. degree in computer science from Yale University in 2011, and the Ph.D. degree in computer science from the Air Force Institute of Technology in 2016. He is an Assistant Professor of computer science with the School of Engineering and Computer Science at Cedarville University. His research interests include improving cybersecurity education, and he has written journal articles and presented at national cybersecurity education conferences on the importance and practice of teaching adversarial thinking for cybersecurity. He has also been the recipient of two NSA National Cybersecurity Curriculum Program grants to develop curriculum for teaching adversarial thinking for cybersecurity and for teaching the legal and ethical aspects of cybersecurity.

Cybersecurity for All CS

The discipline of computer science is no longer in its infancy, but at only around 50 years of age, it is still in some ways in its adolescence. One of the next steps in its maturation must be for it to fully embrace security as a core part of its identity.

Because the benefits of "technology" (hereafter a catch-all term for the products of computer scientists) increase when they are networked together, the coming era of the Internet of Things is an inevitability. As this era comes about over the next decade, the distinction between technology and cyberspace will practically disappear. Therefore, securing cyberspace (i.e., cybersecurity) will be a concern of the vast majority of the next generation of computer scientists.

The movement of all technology into cyberspace is somewhat disconcerting because many of the properties intrinsic to cyberspace make it a fundamentally vulnerable domain. For example, cyberspace is *distanceless*, meaning that bad actors can operate at anytime from anywhere in the world, making the number of potential threat actors virtually limitless. Also, the world of cyberspace is *digital*, making it possible to perfectly impersonate others and trivial to steal, modify, and destroy cyberspace assets. Cyberspace is also *invisible*, cloaking nefarious activities in darkness. This makes it difficult to detect and to identify bad actors, enabling them to act with near impunity. These attributes (among others) combine to make cyberspace particularly susceptible to criminal wrongdoing, and history has shown that criminal bad actors are ready and willing to take advantage of these dynamics. These attributes also make cybersecurity, which is about protecting the rights of individuals and organizations in cyberspace, an enormously difficult undertaking.

Therefore, as cyberspace more and more becomes part of the core infrastructure of our society, all those involved in producing and deploying technology must be thoroughly security-conscious. Cybersecurity should be seen as a shared responsibility among all those involved in creating its artifacts and infrastructure. However, it is not clear that today's computer science programs are sufficiently emphasizing security to the extent that every graduate is security-minded. From my experience as a computer science faculty member and as a computer science graduate student over the past 10 years, security within the discipline of computer science is

still seen as something of a sub-discipline that some will focus on, while others are free to ignore. Again, this is especially disconcerting because increasingly, the proper functioning of our economy, the well-being of our citizenry, and the safe-guarding of our freedoms are all dependent on a secure cyberspace.

It is true that much progress has been made to raise awareness of this need within the discipline of computer science. For example, the CS Curricula 2013 guidelines made headlines for highlighting security as both a stand-alone and a cross-cutting concern. This was the first time in the history of the guidelines where security was specifically called out and represents a major step forward. However, the guidelines did not go far enough in emphasizing the importance of security. For example, the only time the word "security" is mentioned in the *Characteristics of Graduates* section, is under the *Familiarity with common themes and principles* sub-heading. The sub-section states, "Graduates need understanding of a number of recurring themes, such as abstraction, complexity, and evolutionary change, and a set of general principles, such as sharing a common resource, security, and concurrency." Again, it is good that security is mentioned in the context of characteristics of graduates, but the level of prominence assigned to it does not match its importance. In order to help create a more secure technological infrastructure, "security-minded" must be one of the foremost "characteristics of graduates."

Today we lament the fact that security concerns have frequently been an afterthought in the design, production, and deployment of technology, which has helped to lead us into an entrenched dependence on a vulnerable infrastructure. But with the current state of computer science education, these mistakes are likely to be reproduced by the creators of tomorrow's technology.

I recognize that this idea is not new. In fact, Eugene Spafford wrote about how computer security issues pervade every aspect of computing in the 90's in his testimony that in part inspired this upcoming NACE workshop. But I am arguing that to date, we (the cybersecurity education community) have not sufficiently prevailed upon our computer science colleagues to accept responsibility for incorporating security into their courses. This negligence has helped lead us into the present situation in the workforce where cybersecurity specialists

are continuously putting their fingers in a dike with new leaks sprouting around them all of the time. A continued push to raise awareness and ultimately to reorient the discipline of computer science around security is for me one of the most effective ways to deal the acute cybersecurity labor shortage.

Practical Next Steps

In order for computer science education to properly prepare the next generation of computing professionals, who are increasingly laying the groundwork for a technology-based society, the next stage in the maturation of computer science must focus on nurturing a security mindset in students. Producing a computer science graduate who is unconcerned with potential adversarial actions is like producing an accountant who does not appreciate the potential for an audit, or like producing a mechanical engineer who is not preoccupied with safety concerns. In short, it is irresponsible. Cyberspace is rife with threats, and no computer scientist should be enabled to remain ignorant of this fact.

I am not suggesting that cybersecurity should not be a specialized sub-discipline of computer science – it definitely needs to be, and I am sure that the NACE workshop will find ways to promote this from K-12 through graduate school education. I am also not arguing that every computer science graduate must be a cybersecurity specialist. But what I am suggesting is that every computer science graduate must be exposed to security concerns early in their course of study and throughout their program. It must be impressed upon every student that in addition to their expected user base, nefarious people exist with impure motives, and the threat they pose must be mitigated at every opportunity. We have done well at emphasizing reliability testing and the necessity for handling random natural events and unintentional human mistakes (which ported naturally from the discipline of engineering), but computer scientists must always consider potential adversarial actions as well (which is not a vital concern of most engineers).

We must work to promote cybersecurity among broad audiences of computer science educators. Already existing curricular guidelines like CS Curricula 2013 and CSEC2017 provide the specifics; our task must be making sure guidelines like these rise in prominence. One practical idea would be to push for security-related keynote addresses at future SIGCSE

conferences. Another idea is to work with ABET's Computing Accreditation Commission to better highlight and enforce security-mindedness as a student outcome. Teachers and faculty members reproduce what they are, and many of them are not security-minded, so another idea would be a to offer continuing education in the areas of cybersecurity for computer science teachers and faculty. Offering a free cyber workshop at major computer science conferences might be a great investment for equipping computer science faculty.