An Intelligent Vision? Autonomous Systems in Computing Education

Daniel E. Krutz

Qi Vu

From self-driving cars, UAVs, and even the cloud infrascturcure that hosts Facebook, autonomous systems are changing the world we live in. This next generation of computing engineers and scientists are not only going to drive the innovation of these systems, but of the world itself. In order to develop these engineers, we are going to need to both train and enourage students to pursue this area of innovation. K-12 institutions are likely to be faced with the question of if and how they should include this area in their curiculum. Three primary questions will need to be addressed. Dsfsfasrewrfs

**Should we teach it?**

The first question is should we include it in our curiulum. While most would agree that this is an important topic; the our curiclum is already jam packed with important topics and including autonomous systems will mean taking away another topic. It is a zero-sum game. If we do include it, then what do we take away? A likely candidate could be an upper level math or science activity. However, one could argue that such activities are themselves necessary for building students who are motivated and capable of careers in intelligent systems.

**What should they be taught?**

For institutions that decide to include intelligent/autonomous education in their curiclum, the first question will be what they should include. Some potential areas covered could include basic decision-making, or integration of intelligent/autonomous concepts into physical devices. Schools will next need to determine what level of students they should begin targeting. Is K-6 an appropriate age group for foundational concepts, or should middle or high-school aged students be targeted.

**How should they be taught it?**

Most K-12 instittutions are not equipped to include this potentially difficult topic in their courses. This is to no fault of the teachers, since intelligent/autonomous is a new and often complicated concept. This is from both an educational materials perspective and from an the knowledge most teachers have in this area. There is a general lack of easily adoptable intelligent/autonomous activites in computing education. If we want to include this topic in our courses, we will need to develop reusable materials that are easily adoptable by a large number of organizations, especially those that typically have limited resources.

**References**

[1

Author Information

Daniel E. Krutz

GOL-70-1575

[Department of Software Engineering](http://www.se.rit.edu/)

[Rochester Institute of Technology](http://www.rit.edu/)

Rochester, NY 14623

[dxkvse@rit.edu](mailto:dxkvse@rit.edu)

Qi Vu

GOL-70-2113

Department of Information Sciences and Technologies [Rochester Institute of Technology](http://www.rit.edu/)

Rochester, NY 14623

[qyuvks@rit.edu](mailto:qyuvks@rit.edu)

The vast majority of today’s car accidents are caused by human error. They are preventable. Whether it is running a stop sign or failing to stay in their lane, most accidents could have been avoided. Very rarely do accidents occur due to hardware failure in the vehicle. Long ago, we learned to create cars where the wheels typically do not fall off while driving and lead to a catastrophic accident. Cybersecurity is much the same. Nearly all vulnerabilities are due to human error, by either the user or the developer and could have been prevented. We’ve long ago created practices and technologies that should prevent nearly every vulnerability. So why do they still occur? Why are cyber attacks still a regular topic on the nightly news?

It starts with including this important topic in our curriculums, by showing students that security is by and for everyone, and shouldn’t be left to the “experts”. Nearly every instructor will tell you that security is an important topic, but only one out of the top 36 Computer Science programs in the US require a course in cybersecurity [1]. So why are we so behind the times? Why are we not achieving this quintessential objective of the creation of software systems? Will it take a cyber attack that cripples our nation’s infrastructure? Will it take World War III (The Cyber War)

It is no secret that industry highly values not only trained cybersecurity experts, but even those who are at least somewhat reasonably well-versed in the topic of cybersecurity.

Thomas Richards, a Senior Security Consultant at Synopsys stated:

”Students that can demonstrate the basic concepts of cybersecurity will have an advantage over their peers as security is increasingly being integrated into industry job roles. Developers at major software development companies and other firms are required to follow security guidelines when developing software.”

Instructors need to finally take it upon themselves to include more cybersecurity courses in their curium. Secure systems need trained developers and maintainers that not only understand how to create these secure systems, but truly understand their importance. It all begins with education and awareness. Secure systems are no accident.

**References**

[1]”CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education”<https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/> Accessed 2017, August 9

Author Information

Daniel E. Krutz

GOL-70-1575

[Department of Software Engineering](http://www.se.rit.edu/)

[Rochester Institute of Technology](http://www.rit.edu/)

Rochester, NY 14623

[dxkvse@rit.edu](mailto:dxkvse@rit.edu)

Thomas RIchards

21351 Ridgetop Circle

Suite 400

Dulles, VA

[Thomas.Richards@synopsys.com](mailto:Thomas.Richards@synopsys.com)

Cyber Security Education: Why Don’t we do anything about it**?**

Daniel E. Krutz

Thomas Richards

The vast majority of today’s car accidents are caused by human error. They are preventable. Whether it is running a stop sign or failing to stay in their lane, most accidents could have been avoided. Very rarely do accidents occur due to hardware failure in the vehicle. Long ago, we learned to create cars where the wheels typically do not fall off while driving and lead to a catastrophic accident. Cybersecurity is much the same. Nearly all vulnerabilities are due to human error, by either the user or the developer and could have been prevented. We’ve long ago created practices and technologies that should prevent nearly every vulnerability. So why do they still occur? Why are cyber attacks still a regular topic on the nightly news?

It starts with including this important topic in our curriculums, by showing students that security is by and for everyone, and shouldn’t be left to the “experts”. Nearly every instructor will tell you that security is an important topic, but only one out of the top 36 Computer Science programs in the US require a course in cybersecurity [1]. So why are we so behind the times? Why are we not achieving this quintessential objective of the creation of software systems? Will it take a cyber attack that cripples our nation’s infrastructure? Will it take World War III (The Cyber War)

It is no secret that industry highly values not only trained cybersecurity experts, but even those who are at least somewhat reasonably well-versed in the topic of cybersecurity.

Thomas Richards, a Senior Security Consultant at Synopsys stated:

”Students that can demonstrate the basic concepts of cybersecurity will have an advantage over their peers as security is increasingly being integrated into industry job roles. Developers at major software development companies and other firms are required to follow security guidelines when developing software.”

Instructors need to finally take it upon themselves to include more cybersecurity courses in their curium. Secure systems need trained developers and maintainers that not only understand how to create these secure systems, but truly understand their importance. It all begins with education and awareness. Secure systems are no accident.

**References**

[1]”CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education”<https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/> Accessed 2017, August 9

Author Information

Daniel E. Krutz

GOL-70-1575

[Department of Software Engineering](http://www.se.rit.edu/)

[Rochester Institute of Technology](http://www.rit.edu/)

Rochester, NY 14623

[dxkvse@rit.edu](mailto:dxkvse@rit.edu)

Thomas RIchards

21351 Ridgetop Circle

Suite 400

Dulles, VA

[Thomas.Richards@synopsys.com](mailto:Thomas.Richards@synopsys.com)