

Luis M Vicente
Associate Professor, Associate Director,
(ECECS) Electrical, Computer Engineering and Computer Science Department,
Polytechnic University of Puerto Rico (PUPR)
377 Ponce de León Ave, Hato Rey, PR 00918
(787) 622-8000 Ext. (340) / Fax: (787) 281-8342

Personal address:
131 Calle Portugués, San Juan, PR 00926
lvicente@pupr.edu ,1-787-217-4563

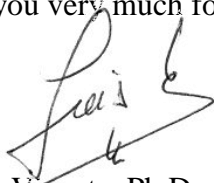
Dear organizers of the 2018 NACE Workshop,

This is Luis Vicente, faculty member of the Polytechnic University of Puerto Rico (PUPR). I am writing you this letter because I would like to participate in the NACE Workshop, on June 9-10, 2018 in New Orleans, LA. PUPR is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and we are devoted to graduate students proficient in Cybersecurity among other fields.

I am part of the PUPR faculty as Associate Professor, Associate Director of the ECECS Department. My main interest attending this workshop is to learn about new Cybersecurity trends, how to efficiently teaching these topics to our students. Also, find about funding, educational, and professional opportunities for our Hispanic students in Puerto Rico. Here at the PUPR most of our faculty and almost 100% of the students are from Hispanic minorities. However, since Puerto Rico is a US territory we all hold US citizenship. This put our students in a very advantageous potential position of being able to work anywhere in the USA, including classified jobs. Last but not least, I would like to increase the underrepresented Hispanic group in the Cybersecurity and National Security fields. The reality is that our minority is not fully represented in those areas yet.

Please find attached a short bio sketch, and a paper intended to inspire thought and discussion about the field of Cybersecurity.

Thank you very much for your attention.



Luis M. Vicente, Ph.D.
Assistant Professor, Assistant Director ,
Electrical, Computer Engineering and Computer Science Department,
Polytechnic University of Puerto Rico,
377 Ponce de León Ave, Hato Rey, PR 00918
(787) 622-8000 ext (340) / Fax: (787) 281-8342 / lvicente@pupr.edu

Dr. Luis M Vicente is the associate director and associate professor of the Electrical & Computer Engineering and Computer Science Department at the Polytechnic University of Puerto Rico. He received Ph.D. in Electrical and Computer Engineering at the University of Missouri-Columbia in May 2009 where he already was author or coauthor of five publications.

From February 1990 to February 2003, Dr. Vicente worked in industry. First, in the Military-Aerospace Division, SENER Group, Spain. In addition, he worked with Voyetra Inc., New York, and with SIEMENS Corp., Madrid.

From February 2003 to June 2009, he became Assistant Professor at the Polytechnic University of Puerto Rico (PUPR). In 2009, Dr. Vicente was promoted to Associate Professor and Mentor of the Master Program in Electrical Engineering at the PUPR. In 2011, he was appointed Sponsor Research Office Coordinator.

In 2012, he was promoted to Associate Director. His research interests include beamforming, array processing, statistical signal processing, adaptive filters, High Performance Computing on Signal processing, and Cybersecurity. As a graduate thesis advisor, he already graduated fifteen students in the digital signal processing area, high performance computing and parallel processing. He is now pursuing a Graduate Certificate in Digital Forensics, expecting to be completed in fall 2018.

Cybersecurity permeates all aspects of our society. It is well known that every electronic equipment connected to the web is susceptible to be hacked, spied on, and the probability of that happening is almost one hundred percent. If that is so, why people are still in negation? What is the reason Cybersecurity is not already part of elementary courses in Engineering? Or even more, why is not taught in every high school in our country, at least at the basic level?. It seems we only pay attention to Cybersecurity after we have been victim of a cyber-crime. We need to change that into a proactive measure!!

The first measure to arm ourselves against cyber-crimes is to be aware of its reality. Learn the basics and at least have a true knowledge of what are the risks we are taking when going online. Getting involved in Cybersecurity is not difficult at all. To have a basic knowledge of how viruses work, how to protect ones computer and smartphones could be learned for people with less than high school academic level. Almost every one of us know what is an anti-virus, a virus, have some ideas of Trojan horses and such. However, all this knowledge usually comes to us from not verifiable sources, like Facebook, personal blogs, unverifiable web pages, gossip. It would not be better to acquire this knowledge from verifiable, academic sources? Why not be learned in schools by adequate teachers in the area? Why not learn all the topics in their correct order and with a strategy in mind? These concepts do not require advanced mathematical skills. These advanced mathematical skill are only needed if you really want to have a deep knowledge of some areas, for example, in cryptography.

Recently, some universities are paying more attention to the importance of Cybersecurity, and not only Engineering universities, but also universities devoted to law. From Chuck Easttom book Computer Security Fundamentals, we read that the University of Dayton School of Law has an entire website dedicated to cyber-crime. The university has extensive links on cyber-crime, cyber stalking, and other web-based crimes. As we all move forward into the twenty-first century, we should expect to see more law schools with courses dedicated to cyber-crime.

I propose to encourage the teaching of some basic topics in Cybersecurity at the very high school level, or even earlier. Starting with the concept of networking layers. To have at least the awareness that all our communications are structured in OSI layers. Then, teaching the students how the

hackers use these layers to infect the network with malware. In addition, a basic knowledge of all kind of malware should be part of the class. The difference between virus, worms, Trojan horses, among other. In addition, chapters on anti-virus, firewalls, anti spyware, would be needed to have a global idea of the basics of Cybersecurity.

None of the above would permeate the mind of our young students without some hands-on laboratories. I propose the creation of some basic laboratories where the students could implement and connect a small network. Both wired and wireless. To acquire the basic knowledge of how it works and how the devices communicate with each other. In addition, some testing, penetration testing, and vulnerability testing. All inside a controlled laboratory network of computers. Create contests where some students would be the defensive barrier of a network and other students to be the cyber attackers.

One of the main difficulties in making reality above ideas is the assumption that all knowledge acquired by our young students could be used for criminal purposes. I am against that idea when referring to our American young students of at least 16 years old. Let's think for a moment what is the minimum age for americans to use and practice with a long shot gun. Just a look at a Washington Post article (By Roberto A. Ferdman and Christopher Ingraham August 27, 2014), we learned that in 30 states there is no minimum age. To me it does not seem a great idea to give a gun to a children, but if we think of young students, around 16 years old. Should we prohibit the knowledge of guns because they could be potential criminals? It is not true that they could learn the topic from the internet, and not precisely by the best people to teach how to use, and the risk of using them? Let's make another analogy. Sex. Why is necessary to teach youngsters about sex? We all know why. However, sex has been a taboo for centuries. Nobody would want to talk or even teach about it. Now, what is the trend today about sex? Why it should be different with Cybersecurity? It is not better to teach all aspects of Cybersecurity in our controlled schools, to young people of at least certain age, than for them to learn from real criminal hackers posting tutorials in the web, and performing penetration testing on the neighbor Wi-fi access point?

We know in conferences and workshops when the speaker ask if your company has been hacked, not everybody wants to disclose that. It seems is shameful to be a victim of cyber-crime. Not

everybody wants to admit they have been victims of a cyber-crime. Cybersecurity is our present time taboo. However, we know by experience in other areas of our life that is better to have good basic knowledge of certain topic than to ignore it or even learn it from the wrong teaching channels. We need a paradigm change in order to place Cybersecurity in its own level of importance. With the fast trend of newer technologies, even faster than ever, we have to admit that the level of importance is rather high. We need to be prepared, armed and ready to know, and defend ourselves against the risks of using technology. We need to prepare our American students to join the good guys.

Regarding the question of how do we get more US citizens, and a more diverse population, into cybersecurity in meaningful ways? I could answer this from our little Caribbean island of Puerto Rico. From centuries, this has been a land of pirates, buccaneers, and smugglers. Even today, the black market, narco-activity, violent crime on our small island streets is rampaging. There is not a single family in the island where that kind of violence did not touch in one or another aspect. On one hand, it is not difficult to convince our young people to join the bad boys, fast money, fast life, short life. However, here in our universities, we are given them sanctuary and teaching them to arm themselves against that kind of life. We teach them how to outsmart the bad people using the latest technology available. We give them power. As I stated in my presentation letter, PUPR is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and we are devoted to graduate students proficient in Cybersecurity among other fields. This is a challenge that any smart student would take, making them truly heroes!! To outsmart the bad people and to contribute the goodness in this island is something not easily understood for people that did not suffer the violence of our streets. For young Puerto Rican students that have seen real suffering, to become proficient in an area where they feel they can contribute to goodness is a true mission. Most of our graduated students are working for security agencies in Washington. They are proud and they make us proud. We have more motives to anyone to help our young students from the beginning of their academic life to learn Cybersecurity. And, we are committed to do so.