cybersecurity education

AN INTERVIEW WITH GENE SPAFFORD ON BALANCING BREADTH AND DEPTH IN CYBERSECURITY EDUCATION

Diana L. Burley

Eugene H. Spafford
Professor of Computer Science
Executive Director, Purdue CERIAS
Purdue University
West Lafayette, Indiana USA

In this critical perspective, Eugene H. Spafford, Purdue University Professor and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS), shares his views on balancing breadth and depth in cybersecurity education. Spafford is one of the most influential leaders in the fields of computing and information security. He serves as a senior advisor and consultant on security and intelligence, education, cybercrime and computing policy to major companies, law enforcement organizations, academic institutions and government agencies. These include Microsoft, Intel, Unisys, the US Air Force, the National Security Agency, the US Government Accountability Office, the US Federal Bureau of Investigation, the National Science Foundation, the US Department of Justice, the US Department of Energy, and two Presidents of the United States. As the founding director of the world's first multi-disciplinary academic center for information assurance (CERIAS), he has led in the development of cybersecurity education efforts for more than three decades [1]. Spafford, or Spaf as he is commonly known, provided these views during a January 2013 interview with Diana Burley, guest editor of this special issue, which he subsequently edited for clarity.

Diana L. Burley: As you know, the theme of this special issue of *ACM Inroads* is holistic cybersecurity education—balancing breadth and depth. So let's start there—how would you describe breadth and depth in cyber security education?

Spaf: I would start by saying that education, as with most other things that involve a process, requires some definition of the intended outcome. Education can have a number of goals. For instance, one purpose of a college education is to prepare individuals for lifelong learning—to provide them with a background in which to become experts about a particular discipline; to be able to enter that discipline, perhaps not as domain experts, but with enough skills that they can be productive and learn as they go. Another purpose of a college education may be to obtain a general awareness of many different skills and cultural items.

Cybersecurity education has a variety of goals. Toward the training end of the spectrum, the goal is to have students come out immediately able to fit into positions where they can exercise certain skills in a production setting. At the other end of the spectrum, we want to provide graduates with a broad, general knowledge of the field sufficient to allow them to adapt and learn new threats and developments over the course of their careers. Programs usually come down somewhere between those two extremes in the overall spectrum.

So to get back to your question—breadth is where we want to ensure that our students understand fundamentals of the various components that are at play in information security. That includes computing, but it also includes issues of social organizations, law, behavior and psychology, ethics, writing skills, and current events. So breadth includes a broad array of topics that are beyond a direct focus on computing and that provide a solid foundation on which graduates can continue to learn and build their skill sets. Depth in

this area is where we sacrifice some of that breadth for additional details, training, and practice in some of the specific tools, skills, and knowledge directly related to the practice of a particular area of information security.

DB: How do we achieve the right balance?

Spaf: There isn't really a single balance. Individuals are different in their capacities and interests, and there are many different applications of the domain. Someone who will work in a government response center needs a different set of skills than someone who will do research on a new product for a start-up. And that is going to be different for someone who will be an educator. So it's misleading to talk about "a cybersecurity education" as if there is a single structured path or focus that should be applied in this arena. That is not to say that there aren't common elements and there aren't some minimum standards, but what we need to do is look at the potential career paths and expectations of graduates to determine what those common elements are and what the common level of mastery is for those elements.

For example, the Common Criteria[1] is something about which every graduate in this area should have at least heard of and know generally what it is. But someone who is going to be involved in a career that is producing to that standard or buying to that standard—which would likely be someone involved in something related to the government—needs to have more depth of knowledge on that subject. Meanwhile, someone working for a social media company will likely never encounter it.

We still have a nascent understanding of what many of the common topics should be for *every* student. As a result, different institutions have different approaches to teaching students—different preparation for different goals. Some places are producing students who are well suited to go into security management positions, others go into law enforcement, and others go into research. Institutions are developing their programs (models, topics) based on interaction with potential employers of their students. In our program, for instance, we have a lot of dialog back and forth with major companies that are involved with the program and with government agencies. Those are the likely future employers of many of our graduates. Another strong program, such as at the University of Tulsa [9] whose graduates tend to go into law enforcement and intelligence agencies, will have a different set of requirements and programs.

DB: What do you think about using the NICE[2] framework of thirty-two cybersecurity job roles to identify different paths and desired skillset and knowledge requirements for those paths?

Spaf: I think that's a reasonable approach. It can certainly help identify opportunities that should be included in a set of introductory or common core classes. But one key element missing from the description of those roles is the background knowledge necessary to perform well in them.

Thinking about the common core, it is even more serious than that.

For example, let's talk about understanding permissions on a file system—people in all those NICE roles, in some way or another, will encounter access control permissions on a file system. To talk about the issues involved in implementing and operating access controls, one needs to have an understanding of file systems and operating systems, either general or specific. This foundational knowledge is generally acquired in computer science or computer engineering, but not necessarily in other programs. But if we are talking about something such as social engineering, deeper understanding of that topic may require some background in psychology, a subject not normally included in a computer science curricula. This is one of the shortcomings with the separation of job roles in the NICE framework. It outlines the positions, but it doesn't really detail the necessary background knowledge that one needs to acquire for them.

At the other end of the spectrum, we want to provide graduates with a broad, general knowledge of the field sufficient to allow them to adapt and learn new threats and developments over the course of their careers.

DB: So the question of balancing breadth and depth is actually more complex than initially thought. With regard to a common core, the question is how do we identify a common core that provides varying levels of depth to encompass the full scope (breadth) of cybersecurity role—using those specified by NICE or not.

[1] The Common Criteria for Information Technology Security Evaluation (referred to as the Common Criteria or CC) is an international standard (ISO/IEC 15408-1:2009) that "establishes general concepts and principles of IT security evaluation and specifies the general model of evaluation [3].

[2] The National Initiative for Cybersecurity Education (NICE) is a collaborative national effort designed to enhance the cybersecurity posture of the United States through improved access to education and training that will better the cyber behavior, skill, and knowledge of every segment of the population [8]. The National Cybersecurity Workforce Framework (the Framework) was developed through the initiative in an effort to describe and provide a common lexicon for cybersecurity work "regardless of organizational structures, job titles, or other potentially idiosyncratic conventions [6]." Released in September 2011, the Framework organizes job roles under seven high-level categories: securely provision, operate and maintain, protect and defend, analyze, oversight and development, investigate, collect and operate; and 32 specialty areas that group similar functions together based on typical job tasks. The Framework provides knowledge, skills, and abilities (KSAs) for each specialty area.

cybersecurity education

An Interview with Gene Spafford on Balancing Breadth and Depth in Cybersecurity Education

Let me touch on something else that you mentioned regarding the training end of the spectrum and the desire to have students ready to hit the ground (and keyboard) running. What do you think of cybersecurity competitions[3] and their role in developing hands-on experience?

Spaf: Competitions are really oriented at demonstrating mastery of highly applied skills. They are, in some sense, equivalent to laboratory experience or experience running a machine press or similar kinds of things in other fields. Various companies and occupations have apprenticeship programs where people learn on the job, but that still appears to be uncommon in some areas of cybersecurity—potential employers expect new graduates to know how to "do it all." Thus, competitions have become popular.

Competitions stress part of the finished skill set in demand by those employers: They're great for finding people who are able to respond quickly with a set of tools to a range of things that are known at the time of the competition, but that is not a measure of creative problem solving in a larger domain. So you will seldom find, through any kind of competition, a set of people who have done in-depth research, who have advanced degrees, or who in fact will be considered for positions as senior managers in this realm. When running competitions to see who can run a drill press the fastest on an assembly line, don't be surprised if few of the winners are mechanical engineers or have MBAs.

I suspect if you were to take somebody who is a director or deputy director in a national agency that is involved with cybersecurity, or the Chief Technology Officers (CTOs) of major corporations, they would do very poorly in one of those competitions. They would probably plummet to near the bottom. I know if you asked me to defend a Windows 7 box against current attacks I would not place highly in a current competition. Does that say that any of us are lacking in skills or does that say that the competitions are directed to a very narrow set of skills? I think it is obvious the correct answer is the second.

DB: Okay, so given the fact, then, that we are seeing an increasing number of competitions and these competitions are supported through a limited pool of public and private funds, do you think that continuing to push toward more competitions is the right approach?

Spaf: I think pushing too far in that direction is a bad idea for a couple of reasons. The first is that currently we have deployed lots of systems that have been poorly designed, poorly tested, have lots of security flaws, and that need constant care and maintenance to be even somewhat safe—and we are under increasing stress. So there is great pressure on companies and government to put people in place to protect those systems. This is, in part, because it will take a while to redesign those systems to build in more fundamental protection even if we made that a priority—those solutions are potentially years off and we need fixes now.

So you will seldom find, through any kind of competition, a set of people who have done in-depth research, who have advanced degrees, or who in fact will be considered for positions as senior managers in this realm.

We also have critical shortages of qualified people, so there is a natural tendency to push lots of resources into quick fixes and patches. Longer term however, quick fixes shortchange investment in more fundamental research, the construction of quality education programs, and the production of people who have a deeper and longer view of the needs—those who are more likely to be able to provide important solutions for us five, ten, and twenty years from now. Too much emphasis on competitions and quick fixes will shortchange the longer view, and prolong our problems.

A second issue is that the competitions are largely focused towards current problems—so they are focused on protecting a current Windows or Linux system. Maybe some of the parties involved can generalize the attacks and the concepts to future systems, but not all of them will be able to do that well. Thus, the people who perform well in the current competitions may find themselves stale in a few years and not able to make a difference because they don't have that deeper background knowledge. That will hurt their employers and hurt them; their technical usefulness may expire long before the expiration of their potential career.

Third, the competitions by their nature may tend to exclude some people—people who think more slowly and deeply about issues, who are not into competitions, and those who are not interested in public exposure—from even going into the field. I haven't seen any numbers, but personal experience (purely anecdotal), has shown

[3] Cybersecurity competitions provide hands-on skill-development opportunities through interactive, scenario-based exercises. A variety of competitions are offered for individuals and teams who range from high-school students to collegiate competitors to advanced participants without academic affiliation. Competitions such as CyberPatriot [2], the National Collegiate Cyber Defense Competition (NCCDC) [4], and the National Cyber League (NCL) [5] have seen considerable growth in the number of participants in recent years. The US Department of Homeland Security National Initiative for Cybersecurity Careers and Studies (NICCS) web portal [8] provides a repository of global cybersecurity competitions. The repository includes information on competitor level (e.g. high school), competition dates, associated costs (if any), and a direct link to the competition websites.

that women don't seem to be excited about these competitions. And we already have a terrible gender disparity in computing in general. Security is a little better, but still it does not exhibit a good representation of the general population. So if promoting these competitions is intended to be a way of encouraging people to get into the field, it may be in fact discouraging some of the very same people we want to attract—including many who can make a difference.

Fourth and last of all, because the competitions do encourage people to win them, it means that curricula and training that these students might go through are likely to reduce emphasis on the more general concepts that are important in favor of the tricks and specific issues needed to score points. The curriculum may even be reduced so that more time and energy can be put into practice for the competitions. Again, this does not serve the students or their potential employers well.

So for all four of those reasons, I don't think it's a good idea to place so much emphasis on competitions.

DB: Like the prevalence of competitions, we are also seeing an increase in the number of cybersecurity degrees. Educators seem to be divided on the value of such degrees? Where do you stand?

Spaf: I think [the increase in cybersecurity degrees] is an overreaction to the push from potential employers who are looking for students with specific backgrounds. In response to the national sentiment that we don't have enough people in this area, colleges and universities are responding with new programs. They are responding to the pull of employers and society's need—as they have for a long time and as they will continue to do for every new area. The problem is that too many institutions have faculty with little or no real background in the field who are offering courses based on the available educational materials they find—some of which are textbooks, some of which are simply online information that anyone can present. They are acting in good faith, but they don't know what is really important and how to present it effectively.

…And here is another danger of the competitions. [Faculty] see [competitions] getting a lot of publicity (especially from companies), so they develop training programs around them. This is not really providing education, but they are able to put together a course of study that they then label with a degree. What employers will find (and have been finding) is that the quality and the preparation of students coming from these many diverse programs are very different. Some institutions are going to get a very bad reputation, and some are going to get a good reputation. Some institutions are going to be in the middle and they may adjust their programs, but there are likely to be quite a few student casualties along the way—where they are going to have a degree but they can't get hired, not realizing that what their degree says doesn't really match what's necessary for them to succeed in the field.

Let me also interject here—this is really the difference between these competitions and training, and a complete education—an analogy to medicine. For someone to become a brain surgeon or a medical researcher or a pediatrician requires a lot of in-depth study and specialization as well as a general core of knowledge. They must go through internships and residencies. It takes a long time for them to get to the point where they really become masters at their craft. Graduates who are right out of medical school have basic knowledge, but until they actually gain the hands-on training through internships and residencies, they are not ready to practice on their own. We also have programs at community colleges and specialized programs to train people to be emergency responders, to train people to be nurses and medical assistants. We need those people too. We need those people who respond to the emergencies—who are able to deal with the very gross level problems to possibly save somebody's life, but if everybody that we produced from the system was an EMT or a nurse, our health system would be in trouble. And it's the lack of balance that worries me in the various places where people are promoting competitions and new curricula.

This is really the difference between these competitions and training, and a complete education—an analogy to medicine. … Graduates who are right out of medical school have basic knowledge, but until they actually gain the hands-on training through internships and residencies, they are not ready to practice on their own.

DB: What do you think the role of industry and government should be in developing faculty and programs?

Spaf: It is obvious that industry has major needs now. They have a bottom line and they tend to think in terms of next quarter's results. So what they demand out of institutions are students who can come in and hit the ground running to solve their problems. That's not necessarily consistent with the goal of most four-year education programs. So one of the responsibilities of industry is to provide feedback and support to institutions. They should also try to understand that what's delivered to them as new hires may require internal training above and beyond what's provided at those institutions, because those institutions who produce the right quality of graduates shouldn't be forced to forego the longer term education in favor of more training.

It's also the case that for many of these companies, they need to realize that education is terribly stretched economically now and institutions can't afford much (if any) of the state-of-the-art equipment, diagnostic tools and software that industry is relying on and

cybersecurity education

An Interview with Gene Spafford on Balancing Breadth and Depth in Cybersecurity Education

is concerned with operating and protecting. So if industry is in a position to help arrange donations, finance access, provide training during summers, offer internships, set up faculty exchanges—anything along those lines—it will help increase the availability and awareness of those technologies and industry needs.

From a government standpoint, the same is true only more so. Government programs should be structured to provide more funding for infrastructure. Recognizing the difference between education and training, another thing government can do is to provide appropriate levels of support for each. It doesn't have to be equal, but right now they tend to be supporting one of the two way out of proportion to the other. Third, government can provide better faculty development opportunities—for instance, exchange opportunities, use of equipment, release of data, release of vulnerability and attack information, and so on.

DB: Given all of the things that we have discussed, where are the priority areas—where should we as educators be focusing our time and attention?

Spaf: This is not an easy answer, unfortunately. I am not sure I can say what the most important thing is. But one of the things we have to do is achieve some understanding of the balance and incentive structure to make sure that we are investing properly in all phases of the challenge. Right now, too many of the policy decisions that are made favor support of frontline protection, incident response, and military objectives. Longer term we should hope that that is not the status quo.

If we have an overall goal of systems that are more secure by design out of the box and don't need as much constant attention by personnel—if this is the vision of where we want to be, we should be investing a sufficient amount to help move us in that direction. I don't currently see that we are doing that. We are not appropriately investing in the whole area of civilian law enforcement, forensics, and cultural issues. We are not investing enough, by far, in the research and development of more secured systems by design.

There are also some things in the area of intellectual property laws and protection that should be revisited to allow us to do better unconstrained research, and in policy-oriented economic incentives for organizations to replace badly vulnerable legacy systems with newer, better protected systems. Those are parts of a class of things that we should focus on rather than responding solely to immediate technical needs.

With people having careers that stretch 30, 40, or even 50 years, we as educators should be thinking about what we want the world to be for our students during the course of their careers. Analogizing again to medicine, our goal shouldn't necessarily be in finding better antibiotics, but in ways to keep people from getting sick in the first place—teach better hygiene, have better water purification, educating people about better nutrition—those kinds of things make a bigger difference than treating people after they get sick. We should be doing the same kind of things in cybersecurity.

DB: We should prioritize prevention then?

Spaf: Yes. We need to focus on prevention rather than simply responding to those threats that we see.

DB: And with regard to balancing breadth and depth—clearly this is not just a question of curricular breadth and depth. Rather, the challenge to balancing curricular depth is very much tied to our ability to manage the tension between addressing immediate needs and thinking more broadly and long-term about how we address the evolving nature of the threat. In other words (and not to diminish the critical importance of developing deep technical skills for some) the breadth vs. depth discussion is, in part, a discussion about quick fixes versus long-term investments.

Spaf: Exactly right. Ir

References

[1] "Center for Education and Research on Information Assurance and Security," http://www.cerias.purdue.edu/ Accessed 2013 June 1.

[2] "CyberPatriot: The National High School Cyber Defense Competition," http://www.uscyberpatriot.org/Pages/default.aspx. Accessed 2012 December 26.

[3] "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model," http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341. Accessed 2013 June 1.

[4] "National Collegiate Cybersecurity Defense Competition," http://www.nationalccdc.org/. Accessed 2013 June 4.

[5] "National Cyber League," http://www.nationalcyberleague.org/index.shtml. Accessed 2013 June 4.

[6] "National Cybersecurity Workforce Framework," http://csrc.nist.gov/nice/framework/. Accessed 2013 June 15.

[7] "National Initiative for Cybersecurity Careers and Studies," http://niccs.us-cert.gov/education/cyber-competitions-repository. Accessed 2013 June 4.

[8] "National Initiative for Cybersecurity Education," http://csrc.nist.gov/nice/. Accessed 2103 June 15.

[9] "University of Tulsa Institute for Information Security," http://isec.utulsa.edu/. Accessed 2013 June 15.

EUGENE H. SPAFFORD
Professor of Computer Science
Executive Director, Purdue CERIAS
Courtesy Affiliations: Professor of Electrical and Computer Engineering, Professor of Communication, Professor of Philosophy, Professor of Political Science
Purdue University
305 North University Avenue, West Lafayette, Indiana 47907-2107 USA
spaf@purdue.edu

DIANA L. BURLEY
Department of Human and Organizational Learning
The George Washington University
44983 Knoll Square, Suite 147
Ashburn, Virginia 20147 USA
dburley@gwu.edu

Categories and Subject Descriptors: K.3.2
General Terms: Security
Keywords: cybersecurity, education, competitions

DOI: 10.1145/2568195.2568211