Comments on:
Growing, Sustaining the Nation's Cybersecurity Workforce

Aug. 1, 2017

General Information

1. My University's Department of Computer Science was founded in 1965 and has offered instruction related to computer security from its inception. I joined the department in 1980 and from the start, my teaching responsibilities have included instruction in operating systems and computer architecture. Computer security is a significant component of these courses, and in 2005, I developed the first undergraduate course we offered that explicitly focused on security.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. I am not familiar with the metrics used to collect and share information about cybersecurity education and training.
2. I do not believe that there is any consensus about workforce categories or specialty areas in the field of cybersecurity. There is poor consensus about the meanings of job titles in the entire field of computing. The term *software engineer* is 40 years old, but to many employers, it just means programmer. A student can have excellent training for work in cybersecurity without ever taking a course with the title security, yet many degree programs that explicitly state cybersecurity as part of their program name are woefully weak. That said, I believe that there are several essentially different categories within the cybersecurity workforce:
   – *System administrators*: Their primary responsibility is configuring systems of off-the-shelf hardware and software to meet end-use requirements. A knowledge of programming is helpful but many think it is secondary for the job of a system administrator, but it is essential that they understand networks, routers, firewalls, network ports, virtual machine monitors, cloud computing, and major application suites such as web servers and mail servers. They must understand client-server relationships, and they must understand major network protocols such as ssh, http, https, and they must understand the division of work loads between client side and server side computation. As far as I can tell, job titles like *security analyst*, *security engineer, security administrator* and *chief information security officer* are all essentially system administrators.
   – *System administration support developers*: Administrators of secure systems rely on antivirus software, intrusion detection software, and a variety of other specialized support tools. Many of these tools exist primarily because of serous design errors in the end applications. Job titles such as *security software developer* and *security architect* are frequently associated with this domain.
   – *Application developers*: Programmers are the primary creators of security vulnerabilities as a side effect of their primary job, creating and maintaining the software that actually meets end user requirements. Failures to understand the security implications of application development is a major source of the problems that we ask system administrators to solve. Patching inherently insecure applications with aftermarket security software is a losing game. Therefore, application developers need much greater security awareness, and they need the support of *security architects* and *security analysts* from the very start of the development cycle.
3. I am not aware that my University has any policies regarding cybersecurity workforce education and training efforts. I am uncertain what kind of policies a university could have in this regard.

4. My contacts with employers suggest a wide range of expectations varying from naïve to solidly grounded. Some seem to think that there will be some kind of magic bullet. They seem to believe that security can be added as an afterthought, patched onto existing systems by inexpensive technicians. At the other end of the spectrum, there are employers who understand that security must be designed into products from the start, and even then, small errors can destroy it. They understand the need for and the cost of the constant vigilance is required to achieve a secure result.

   In general, we face serious problems because a large part of the management pyramid knows remarkably little about computers and less about security. The security consequences of high level executive decisions can be quite serious, and in many organizations, these decisions are made in a near vacuum. Example decisions that have such consequences include such things as what to outsource, for example, into the cloud, what data to gather, what data to sell, and what to put on the Internet.

5. I am not sure that there are any effective cybersecurity education, training, and workforce development programs being conducted in the United States today. To the extent that programs advertise themselves as such, they are addressing the system administration component of the workforce demand. However, I am aware of a very small number of individual teachers at elite universities that teach what I consider to be competent security courses. Students who have come through those courses offer us some hope.

6. The challenge we face is to change the rules of engagement in the cybersecurity field. So long as applications are developed without significant security awareness, the work of the system administrators trying to manage those systems will become progressively more difficult, and major security breaches will become more and more frequent.

   The problem is, as new applications are added to existing systems, the set of vulnerabilities continuously grows. Security is a total system property. If two components that are each, in isolation, judged to be secure, are connected. The act of connecting those components may create new security vulnerabilities. As the number of components increases, the number of interactions that can create vulnerabilities grows explosively.

   Therefore, we need to radically raise the security awareness of all application developers and managers.

7. Security support software, including expert systems and automated administration tools can help, but these tools themselves become parts of the systems they protect, and this contributes to the explosion in the number of interfaces that each introduce potential new security problems.

   Development tools can help. Type-safe programming languages and programming environments that encourage correctness proofs can eliminate many of the more elementary vulnerabilities. Unfortunately, some system components must be developed outside the type-safe universe, notably, key parts of operating systems and the implementations of type-safe languages.

   As such, I do not expect technological advances to reduce the demand for expertise on the part of system developers or administrators.

8. The single biggest step we could make would be to eliminate the ability of software developers to immunize themselves against liability for security flaws in their products. The standard disclaimer that the vendor is “unable to promise nor warrant that there will be absolutely no risk of loss or damage of information, or any other kind of loss” allows vendors to push new features with impunity with no attention to the security consequences. When the software industry was small and struggling in the early decades of the computer era, it made sense to

allow software to be sold free of the kind of implicit warranty that all other products are held to, but the software industry is now huge and on the road to maturity. The time has come to hold vendors responsible for dangerous flaws in their products, including security flaws.

A change to the software liability laws will have to be done gradually. Conventional marketplace models do not deal well with open-source software, and a sudden change in liability rules would lead to significant disruption. Nonetheless, we must find a way to hold system developers liable for the security flaws in their products.

We cannot rely on the top 10 or 20 universities to fill the vacuum in the computer security workforce. There are roughly 200 research-oriented academic computer science departments in North America. Mine is ranked in the top 1/3 of this group, and we have serious difficulty staffing a few undergraduate security courses. For departments in the bottom 2/3, not to mention non-research institutions and junior colleges, the situation is dire. I cannot imagine any short-term fix to the problem of adequately staffing the security classes required to produce a significant change in the current situation.