Labeling-in Security

Fred B. Schneider

A chain of "off price" apparel stores in the US advertises "an educated consumer is our best customer." Education is indeed a powerful tool for incentivizing action, and educated users would undoubtedly view trustworthiness as an important criterion when purchasing a computing system. But I doubt there actually would be trustworthy computing systems available for purchase. To get these, we're clearly better off focusing on creating "educated producers."

With this in mind, some have argued that we should compel all computer science and information science undergraduate majors to take courses that discuss the design and implementation of trustworthy systems. However, only a small fraction of these students are destined for system-building careers, and most software doesn't have to be very trustworthy anyway. So only a small population of our undergraduates really need to learn about trustworthy systems. Also, not all system developers are computer or information science majors as undergraduates, and thus we would not be educating a significant population that need to become "educated producers."

What we really need are incentives for companies to hire and use "educated producers" for producing systems that ought to be trustworthy. The job market then provides the incentives for undergraduates to take courses to become "educated producers." This kind of reasoning invariably leads to proposals for credentialing—assigning labels to workers, indicating whether these workers are deemed qualified to engage in building trustworthy systems. Legislation currently being discussed in the US Senate, for example, advocates something along these lines.

Credentials by themselves are not the solution. At best, they are a symptom of a solution.

You might hope that a credentialed individual would engage in best practices. But hope is all you can do. Possession of a credential does not by itself compel the use of best practices, and it's easy to imagine credentialed system builders cutting corners by choice (such as out of laziness) or by mandate (such as from management trying to cut costs). Also, the value of a credential depends on the institutions that define what content must be mastered to obtain the label. To whom should society be willing to vest that responsibility? How do we ensure that the content and standards enshrined by the credential have been selected based entirely on society's best interests rather than financial gain or commercial advantage?

In a fast moving field, content will change rapidly. The credentialing process must keep up, as must credential holders. Otherwise, credentials impede the spread of innovation because people who employ practices learned for a credential are soon engaging in outdated methods.

We are not the first group of professionals to face these problems. Credentialing schemes that the legal and medical professions use, for example, seem to serve society well. Therefore, we would be wise to understand the particulars of their credentialing processes before endeavoring to create our own. I see three elements as having been crucial to their success:

- Obtaining a credential requires years of post-bachelors education, in which the curriculum has been set by the most respected thinkers and practitioners in the field.
- Credential holders are required to stay current with the latest developments in the field by continuing their education through courses sanctioned by the institution that issues credentials.
- The threat of legal action to individuals (including malpractice litigation) incentivizes professionals to engage in best practices.

In sum, using exams to create labels for our workforce might sound like a way to get more trustworthy systems, but it's not. You can't label-in security. To have the desired effect, a credential must bestow obligations and responsibilities on practitioners. Moreover, curriculum and educational programs—not an exam—are central to the enterprise. □