SOFTWARE INDUSTRY STANDARDS

I agree with the observations that Simone Santini shares in “Standards: What Are They Good For?” (The Profession, Dec. 2006, pp. 140, 139).

The mantra-like opinion that academia should serve industry’s purpose is not only wrong but dangerous to the health of industry and society at large. Academia should serve society as a whole, including the part of academia that works with engineering and industrially applicable topics.

During my 15 years as a programmer, I have been alarmed by the way the fanaticism for standards extends to various aspects of the software industry such as the choice of processes, programming languages, and software products.

For example, a standard choice in the software industry for the past five to 10 years has been that “we must use standard processes and tools like RUP, Java, and XML.” Unfortunately, that choice often is made before achieving a thorough understanding of the problem to be solved. Doing so automatically gives up a possible and important competitive edge—namely, trying to find the best technical and cost-efficient process and tools for the problem at hand, even if that means inventing new ones or developing new protocols or formats, for that matter.

This is apart from the fact that RUP is basically useless, Java is a mediocre high-level language, and 95 percent of the XML-related standards solve only 5 percent of the actual data representation and storage challenges in a typical business software system. I even have to put up with people who use XML to design system configuration file syntaxes.

It’s all just plain stupid and incredibly short sighted. But then again, they are “standards.” Sigh!

Paul Cohen
pacoispaco@gmail.com

The author replies:

I had similar experiences during my stint in industry. The frustration deriving from seeing ersatz solutions being imposed on us just because they were standard was one reason why I decided that stint had better come to an end.

Part of the problem is that the people who make the decisions don’t really understand the techniques and standards they’re forcing the engineers to use. I remember a product in which one of the requirements was to use XML. Just that, regardless of whether we needed XML or not. The problem was that at the time (1999), XML was the new thing in town, and our marketing people wanted to be able to say to equally ignorant marketing people at other companies that we were up to date, that we were using the latest thing.

Another serious problem is that computing professionals are being educated to fit into this state of affairs. When faced with a problem, students are no longer being educated to think about it in the abstract, look for an efficient solution, and then, if necessary, look for existing products and standards that can be helpful. The new methodology—often the one that is being taught—comes straight from the bizarro world: When faced with a problem, find all possible programs and standards that have an even remote connection with it, and build your solution around them.

Allegedly, this is a cheaper and faster way to build things. The delays and poor quality of Internet software—the software that most heavily relies on standards—seems to say otherwise.

INTERNET SECURITY

In “Reengineering the Internet for Better Security” (M. Parameswaran et al., Jan. 2007, pp. 40-44), the authors address a grave situation regarding the Internet as we know it, due to improper usage by crackers and related concerns such as data clogging with e-mail spam. The article discusses the notion that these issues can be solved by creating “an institutional structure that strongly motivates ISPs, network service providers, equipment vendors, and users themselves to control attacks at their origin as well as to maintain security on a dynamic basis,” which in my opinion has a fundamental flaw.

The Internet today is made up of interconnects from most developed and developing countries, who all want their say in how the Internet should be operated and controlled. Some countries appear to have a hands-off approach, while others directly control all aspects of its operation.

Given these different approaches, no single institutional body would be able to unite all ISPs, network service providers, and so on toward a common goal of achieving “better security.” The United Nations was created largely to police the world, and the challenges that it faces are obvious and well understood. It seems likely that any single governing body for the Internet would face similar difficulties.

Outbound traffic control and ISP certification are only effective if the rules and “certifying authority” covering these controls have teeth. This might be an obvious solution if the offending ISP and the impacted ISPs are located in the same country or in countries that have trade agreements. But what happens when the offending ISP is located in a country where a trade embargo has been imposed and its actions are impacting ISPs outside its borders? Imposing financial retribution would be difficult if not impossible, and the attacks on the impacted ISPs most likely would continue.

In my opinion, what the authors propose for addressing the current situation will help create a better security mechanism between the larger Internet backbone providers, but, due to today’s world politics, it is by no means the silver bullet addressing all aspects of Internet security.

Todd Kolb
toddkolb ieee.org

The authors respond:

We agree that the decentralized interconnection structure and global scope make it impossible to have a centralized authority unify and con-
trol providers. That is precisely why a feasible mechanism must be decentralized and dependent upon self-interest rather than administrative control as the motivating factor for providers to participate.

In our mechanism, a provider joins only if it finds that its net gains after accounting for financial payments justify certification. Voluntary participation also signals the provider’s reputation, thus helping users screen out inferior, uncertified providers. The choice to participate implies willingness to pay compensation; default of payments can affect both reputation and certification status itself.

The role of the certification authority is to serve as the body that issues certificates and disseminates certification and reputation information to the public. In turn, reputation impacts customer preferences and acts as incentive for providers.

While it would be ideal to have all providers certified, in a world of divergent security profiles, the mechanism is designed to screen the “better” providers into a certified group that users can clearly identify. The providers that remain uncertified are in effect signaling poor security, and they attract a corresponding customer base; further, their customers lose the ability to send traffic to the certified providers. The certified providers thus have a clear idea of which providers to block; such a separation is the focus of the mechanism, not bringing all the providers into a financial settlement structure.

Over time, loss of value to customers and erosion of the customer base can shrink the revenue of uncertified providers and push them to seek certification. But they can sign up only after making necessary investments in security to ensure that joining the scheme is viable.