DOI:10.1145/3102112

Vinton G. Cerf

A Brittle and Fragile Future

While this is not intended to be a dystopian rant, I feel strongly motivated to draw attention to the fragile and interdependent future we are creating through the use of

programmable devices and systems. Some of you are, no doubt, rather tired of this theme, but as we equip cyber-physical and virtual systems with programs that animate their functions, it seems inescapable that over time they will become increasingly interdependent and that may produce vulnerabilities and fragilities that will be exploited by inimical parties or will simply create difficult and even unrecoverable failures.

Consider systems that use passwords and two-factor authentication to identify users. It is often advised to have alternative means for authentication: a mobile device, a distinct email account, a phone number, or an alternative means of identification. These kinds of interdependencies can lead to cascade failures where loss of access to one system initiates failures in others until a complex of authentication failures render a user unable to use any of them. Loss or cancellation of an email account or a mobile phone number may have later consequences if users do not remember to revise all accounts dependent on these alternative means of identification. They may discover the oversight just when the alternatives are vitally needed.

Multiple platforms that support common services such as Alexa or Google Assistant may be concurrently invoked, leading to confusion as to which is “in charge” at the moment. The situation is exacerbated when multiple users are interacting with the same set of platforms or when the platforms are distant from one another.

Conflicting commands from authorized but uncoordinated parties could easily lead to instability or even damage physical and virtual systems.

An analogy might be apt. Personal computers were designed initially to be exactly that: isolated computers for personal use. But before long, they became valuable avenues to access and use of the Internet. Not much thought had been put into the security of these systems when they were stand-alone devices and viruses and worms were already propagating by Sneakernet via floppy-disk drives. The Internet and its predecessors including bulletin board systems were new vectors through which malware could travel and various attacks could be executed. A great deal of effort had to be expended to improve the resistance of personal computers to various forms of attack and failure.

Concerns for safety, security, privacy, and control must be assuaged by systematic analysis of increasingly complex use scenarios.

Many of the devices that are considered cyber-physical systems may suffer from a similar oversight. Often the designers see them as a single-user device controlled from an application running, for example, in the user's mobile smartphone. What is emerging, however, is a highly connected ecosystem of devices and networks with emergent properties derived from the rich, diverse, and distributed connectivity they exhibit. Concerns for safety, security, privacy, and control must be assuaged by systematic analysis of increasingly complex use scenarios. It might even be argued that these analyses will need to be carried out automatically just to keep up with the non-linear growth in potential use cases and device interactions as the devices proliferate.

The designers of devices that populate the Internet of Things have an ethical responsibility to be attentive to the hazards their interactions may create and the companies that market the devices and their services may ultimately be charged by society with liability for their failures or the abuses they invite. It is not too early to begin thinking about these kinds of problems and how they might be addressed technically, legally, and ethically by the engineers and scientists whose advances make new capabilities possible, but which may have unknown consequences as their use proliferates.

Vinton G. Cerf is vice president and Chief Internet Evangelist at Google. He served as ACM president from 2012–2014.

Copyright held by author.