For a long time, I had the idea that configuration of a suite (ensemble) of Internet of Things (IoT) devices would be an infrequent process — for example, when you bought a new device, sold, transferred, or superannuated an older one. However, my thinking has evolved. Sticking with the residential paradigm for a moment, although the ideas seem equally applicable to industrial settings, it’s becoming clearer that many devices will come and go with the residents, guests, workmen, emergency services personnel, and others who might have reason to enter the premises and have need to “control” at least a part of it while present.

This leads me to believe that an IoT ensemble must actually be in a kind of continuous configuration mode, anticipating the arrival and departure of all manner of Internet-enabled devices. Among the implications is the notion that the local IoT management system needs to expect that new devices will need to be configured into the system and others to depart — it needs to sense their arrivals and departures and to react accordingly.

Not every device that arrives must be configured into the system, nor must every device that leaves be deconfigured. Indeed, some devices must be recognized when in remote locations, to be authoritative with regard to access to data and ability to exert controls. Others should be ignored even when on the premises. This implies that there must be a highly active process for discovering and qualifying devices to become part of the local IoT ecosystem and to be recognized as authoritative even when not local.

By extension, these devices must be able to present bona fides to the residential IoT control system when called upon to do so. The process must be painless for users, but assure household authorities that only devices (and people) that should be granted access are properly identified. This strikes me as a nontrivial design challenge; the ecosystem will need some serious thinking about standards to achieve interoperability across a multitude of potential “players” that might be encountered.

The Bluetooth technology-pairing mechanism offers an example of device discovery and a means of confirming that a selected device should become associated with another. For example, cars equipped with Bluetooth technology can detect the presence of another Bluetooth device if the latter is put into a beaconing mode. The car typically serves as the master and discovers a beaconing slave. The master sends the slave a locally generated random number, typically displayed on the slave device. Users are asked to verify that both the master and slave are displaying the same random number before the master adopts the slave. Protocols like this are already in use to allow controllers to incorporate new IoT devices into an ensemble. In a residential setting, we can easily imagine a home controller that detects and configures new devices into its universe, and that can be told to forget an adopted slave when it should be deconfigured (upon the departure of a visitor, for example) or to remember the device and to have a means to recognize it again even when it’s remote and communicating — for example, via the Internet.

Here’s a scary thought: what if a device is adopted that’s corrupted, and it has a backdoor allowing remote access to a residential network of devices?

Vinton G. Cerf is vice president and chief Internet evangelist at Google, and past president of ACM. He’s widely known as one of the “fathers of the Internet.” He’s a Fellow of IEEE and ACM. Contact him at vgcerf@gmail.com.