DATAART

LinuxInsider
Linux News & Information From Around the World

The Importance of Openness to the Internet of Things

September 10, 2014

By Jack M. Germain

The IoT has the potential to transform peoples' lives. However, IoT equipment and software have to be designed from the start with security in mind, said NCP Engineering CTO Joerg Hirschmann. That transformation will not occur if security is left to individual product makers. Securing the IoT will require a commitment to openness among manufacturers.

Consumers today are in an awkward position. Personal privacy is being wiped out by the Internet. At the same time, new technologies that interconnect our devices with our homes and office environments are offering stupendous advantages.

Welcome to the Internet of Things' new world of openness. "Openness" means something different depending on whether you're basking in the convenience of all things connected or contributing to the monetized cash flow that connected-product purveyors get from your personal information.

In this world, openness is pitted against privacy. That is the price consumers pay for the convenience of life with the Internet of Things.

Let's set aside the reality that consumer privacy must give way to controlled openness for IoT technology 🛒 to work. From a technology standpoint, let's shift the focus from consumer privacy to the need to share protocols among product makers in the interest of IoT interconnectivity.

That is the agreement not quite worked out yet among manufacturers. Perhaps there is a double standard involved. Product makers have little worry about monetizing the personal details of users of their connected products. However, those same manufacturers are not yet fully committed to the level of openness the IoT needs in order to allow products to get along.

"I am seeing a lot of need in the industry for agreeing to a system of openness -- but I do not see much cooperation setting in," said Riccardo Mazzurco, head of strategy and business development for Link Your Things.

"Much of this proprietary infighting is the result of industrial politics," he told LinuxInsider.

No Age of Cooperation

For the IoT to advance to the next level, product makers must accept the need for interoperability to take dominance over protecting proprietary information. Otherwise, one manufacturer's black box will not interconnect with some other's white or gray box.

Take product inventory for home automation. Consumers want to remotely control lights, interior climate settings, entertainment controls, and household alarms and sensors. If consumers must deal with manufacturer lock-in, how likely is it that products will move off shelves?

Just to turn a device on and off, you need access to the application programming interface and the cloud. That involves machine-to-machine protocols.

"The process of switching a light on or off remotely becomes a crazy problem. The number of combinations is almost infinite. The process of turning on an IP camera involves replacing a simple cable connection with hundreds of Ethernet protocols. This creates a mess," Mazzurco said.

Growing Market

Home automation products might be one of the most consumer-sought product lines today for use over the Internet. Consumers already are sold on the concept of using an app to control their living environments over the Internet via a smartphone, tablet or laptop.

Smart homes are not the only area plugging into the Internet for remote access and interconnectability. Smart grids, smart meters and connected cars are becoming synonymous with the Internet of Things. Consumers' appetites for all things IoT are becoming insatiable.

There are more than 2.5 billion connected devices today, Gartner estimated. By 2020, there will be some 28 billion more. If manufacturers do not agree to sharing their secrets, consumers will feed elsewhere.

"Markets decide the standards. When the manufacturers play too many games, the market decides," said Mazzurco.

Smart Stuff

The smart home product line is not a new market. Automation has been a thriving market for 25 years for those who could afford it.

Link Your Things has what could become a solution for proprietary infighting on the IoT highway. The company recently launched ALYT, a new smart home management device, through Indiegogo. The platform is built on the open Android operating system.

The product's developers see this new line as an opportunity for the whole developer market. Their plan is to build an ALYT store -- similar to the Apple store concept -- so that developers can create and sell apps for the platform.

Being open makes it easy for developers to take advantage of the concept. Ease of integration with this Android-based system also just led to a new partnership with E-Glas, which offers a voice-command system so that disabled people can live safely and independently in their homes, according to Mazzurco.

The system, integrated with ALYT, also will be offered to retirement facilities to keep people as independent as possible there too. ALYT is the first Android-based, do-it-yourself smart home management platform.

The Openness Overture

Another manufacturer buying into the openness movement is DataArt. The company develops custom software for select industries. It recently announced its open source M2M framework DeviceHive.

The framework, which is an IoT comms platform, is designed to allow developers to focus on building IoT apps without having to focus on the foundation layer technology. That will encourage innovation, enabling the IoT to move forward at a faster clip.

"DeviceHive will be able to energize the IoT by decreasing prototyping and development costs for new devices," Artyom Astafurov, chief innovation officer at DataArt, told LinuxInsider.

Helping the Cause

Essentially, developers will not have to re-do any plumbing. For the users of this solution, this is making the development process more agile, Astafurov said.

The process allows them to put together different pieces of technology that solve specific problems in less time. This lowers the barriers to entry for new players in the market, he explained.

"For example, if you want to borrow an idea from the next big thing in wearables and switch it over to chasing the success of Nest Thermostat using DeviceHive, the underlying communications and protocols would essentially be the same," noted Astafurov.

Securing an Open IoT

Such business ventures could go a long way toward bringing about openness in the IoT. That adds to the IoT's potential to create new business, as well as boost productivity and convenience.

That said, openness also is needed to help IT professionals keep the IoT secure. Another reality is that once a device is connected to the Internet, someone will try to hack it.

With new devices proliferating, it is time to take a different approach. Defense in depth is the only way to fully secure the IoT, Joerg Hirschmann, CTO of NCP Engineering, told LinuxInsider.

"Defense in depth for the IoT includes implementing technologies such as VPNs -- virtual private networks, which have been instrumental in securing M2M communications for some time now -- encryption, key management [and] access control."

Not Wide Open

The IoT has the potential to transform peoples' lives. However, IoT equipment and software have to be designed from the start with security in mind, Hirschmann said.

That transformation will not occur if security is left to individual product makers. That approach has not worked well so far, with current mobile device and Internet security efforts. Securing the IoT will require a commitment to openness among manufacturers.

Product makers have to consider how each component is being used. They also must consider the type of data that will be communicated and which connections will be made. Lastly, manufacturers must take into account who will have access to the data, said Hirschmann.

Open but Apart

Obviously, every manufacturer is pushing for proprietary standards -- but there is no reason for having your home controls different from your phone, Mazzurco said.

For example, on your phone you need an app to do some task. You visit the app store and make a selection. You choose from some 20 possibilities that are user-rated. You know how many people downloaded it. You can read the reviews.

"The process should not be different for a smart home," suggested Mazzurco. "It should not be based on having a particular phone. The problem is the market mentality. It needs to catch up."

Ripe for Non-Cooperation

The home automation market is a good example of how openness quickly can be shut out, warned Mazzurco. For example, Google and Apple probably are looking at the IoT market and discovering that maybe 90 percent have no automation.

They are realizing that it is a huge market, and they want to be there -- even if they are not wanted, he observed.

Google had voiced some interest in an Android device for the home, but that did not materialize. Apple has what is basically a black box that is not open, Mazzurco noted.

"Too many companies trying to open the market are pushing their own platforms. It is not open technology to everyone. The products are still in the proprietary realm," he said.

A Better Way

Creating an ecosystem that will allow all consumers to connect to any home automation product is the concept Link Your Things is promoting. Users of any smartphone platform can access an app that will connect to whichever black box is installed in their home automation product.

"It is a little bit complicated. It looks like we are selling a box," said Mazzurco. "We needed an Android device and an Android app, but it was not available on the market."

Within one year, Link Your Things' application will be copied five or 10 times, he predicted. It is built on Android and will have a normalization layer or API at the level of the app. That is what the company will sell as a service whenever manufacturers make an Android-compatible device.

"This means that you will not have one remote box for each house automation task: heat, lights, A/C, alarms, etc. You will have one single device. You will download the control apps from the app store for what you need. This will enable people to create any number of home control services," Mazzurco explained.

Breaking the Mold

Where the industry is right now only allows consumers to buy all of these proprietary islands of products for all of the different automation products. Changing that is essentially the mission of the various alliances that are trying to get cooperation among the proprietary product makers to use common standards, said Hirschmann.

"Otherwise, products will only work on certain platforms. We need a common system using the same ground-level protocols. Otherwise, you can not have one control console that will hook up all of the disparate automation systems," he said.

Manufacturers must forge openness that will allow consumers to securely connect to the Internet of Things, Hirschmann maintained, but "I think we still have some distance to go there."