BPTrends COLUMN

December 6, 2016

Process Solutions Tom Bellinson

In my prior column for BPTrends, I wrote about scaling applications to handle Internet sized crowds. In my fourth and final entry for 2016, I'd like to elaborate on another Internet evolution that is changing both the scale and scope of what we can do with it. This evolution is often referred to as the "Internet of Things" or IoT.

What is the Internet of Things?

As the name implies, IoT refers to "things" connected to the Internet. This essentially includes anything which does not have as its sole purpose, being just a computing device (e.g. a desktop, laptop or server computer). Some devices may be hard to classify. Is a smartphone a computing device? It has a camera, but now so do laptop and desktop computers. Other devices are clearly IoT type devices. These include vending machines, smart grids and home security systems.

The list of devices that are now "on the net" is growing at a phenomenal rate. Some devices are only indirectly on the Internet, but they still have implications. For example, the other day I saw a promotional video for a wallet that can attach wirelessly to a smartphone or wifi hotspot. If it gets too far from your phone, you are alerted. If you leave it somewhere, you can use GPS location service to find it.

Security

Of course, this means that others can find your wallet as well. The IoT presents a huge security risk that most of us don't understand very well. Allow me to provide a brief tutorial that will help explain why all these new Internet devices are such a risk.

Inside every smart device is a low powered, inexpensive computer. It doesn't matter whether it is a coffee maker or a door lock, if you can talk to it via the Internet, it has some basic components of a computer - a CPU, memory, and network card. Most of these devices use the Linux operating system because it is free, well understood and widely supported.

These benefits are also a weakness. Because Linux is well understood, hackers can find ways to commandeer devices that use it. Besides the obvious ability to control the functions of the device being hacked, there is another, much more insidious usage. One of the most threatening cyberattacks is known as distributed denial of service (DDOS). The way this works is really quite simple, a particular website or other endpoint (like a power plant), is bombarded with requests to communicate. The hardware essentially becomes overwhelmed with requests and cannot process any of them fast enough to remain functional.

If all the DDOS traffic comes from one computer, it is easy for security measures to just ignore that traffic. However, clever hackers create something called a botnet. This is a large number of computers, which are distributed across the Internet and

are coordinated to simultaneously make requests of a single point on the Internet. State actors, such as China and Iran have been detected setting up such botnets. They have the resources to do it. However, with IoT, we now have millions of new computers in devices that have minimal security and monitoring that can be commandeered for an ad hoc botnet.

Last month, the maker of software called Murai that helps hackers assemble botnets, released the code to anyone who wants to download it. Since then, system administrators have been working to close holes in their security. However, your new coffee maker could be attacking the CIA!

Implications for Business

If you are a manufacturer of "things," you may already be building Internet features into your products. If you don't make these things, you may be using them. In either case, security should be concern #1. Nobody questions the value of having remote access to devices across the Internet. Surveillance systems can provide real-time alerts, vending machines can notify operators when they are low on product, and working parents can monitor how their children are being cared for from their smartphones.

Manufacturers of IoT devices should take measures to ensure that there is sufficient security to thwart attacks that can easily compromise the default security typically built into many devices. If you use these devices, there are steps you can take to reduce the attack surface and make it more difficult for hackers to gain and utilize access.

Gartner projects that in 2016 there will be 6.4 billion devices connected to the Internet; up 30% from 2015. Using current data to project, they expect 20 billion devices by 2020. This unprecedented level of connectivity means that your business will be able to make many more decisions in real-time and based on actual data. Because of this, some of those decisions will be able to be turned over to computer algorithms.

Some of these algorithms may be hard coded with rules predefined by the humans who designed them. Other decisions may be made by deep learning algorithms that are designed to spot patterns in the data streaming from these devices. The human users of these systems may offer a nudge in a certain direction, but the actual decisions are a mystery to the humans that launched the software doing the analysis. Whether computers enable decisions or actually make them, the big data coming from IoT devices are already greatly improving the choices businesses make. Amazon's Echo product is an example of an IoT device that is gathering lots of customer data. Not surprisingly, there's a rumor that these are being sold at a loss.

Increasingly, the devices we deploy are gathering data. A quick read of many privacy policies will reveal that the producers of these devices may collect data for purposes of improving future generations. That means there will be vast amounts of data coming from these new devices that can be correlated to determine how users of the devices will behave. This information can subsequently be used to either design improvements into the products or in some cases, sold to other firms that use the data to take advantage of a deeper understanding of human behavior.
Never before have we had so much access to massive amounts of data describing human behavior in such a large number of situations. Coffee makers can tell companies what time most people drink coffee and how many times a day. Door

locks can tell makers how often people come and go from their homes each day and if they remember to lock the door. Vehicle telemetry systems already keep track of location, average speed, even tire pressure.

As people come up with new ideas for devices that collect data, more information will be available to businesses to understand consumer behavior. Businesses that use available data to improve product design and better target consumers will naturally have a distinct advantage over those that don't.

So...

The Internet of Things provides users and businesses a vast opportunity to make life a little easier and more connected. It also can help businesses better serve customers while providing many new revenue opportunities by wrapping services around products (how about a refrigerator that can build an order and place it for home delivery...for a fee?).

However, left unattended, these devices have the potential to do great harm. Our electrical grid and the Internet itself is vulnerable to DDOS attacks and these devices could be turned against us in a massive assault if we don't take steps to secure them. This is the job of device manufacturers and users alike. Education is key.

Author

Tom Bellinson

Mr. Bellinson has been working in information technology positions for 30 years. His diverse background has allowed him to gain intimate working knowledge in technical, marketing, sales and executive roles. Most recently, Mr. Bellinson finds himself serving as President of a BPM related software start-up company called UnaPage that provides solutions based on Microsoft SharePoint. From 2008 to 2011 Bellinson worked with at risk businesses in Michigan through a State funded program which was administered by the University of Michigan. Prior to working for the University of Michigan, Mr. Bellinson served as Vice President of an ERP software company, an independent business and IT consultant, as chief information officer of an automotive engineering services company and as founder and President of a systems integration firm that was a pioneer in Internet services marketplace. Bellinson holds a degree in Communications with a Minor in Management from Oakland University in Rochester, MI and has a variety of technical certifications including APICS CPIM and CSCP