R. Brad Morehead

LiveWatch Security, LLC

"The Internet of Things: Exploring the Next Technology Frontier." Tuesday, March 24, 2015, at 11AM

Subcommittee on Commerce, Manufacturing, and Trade

The Internet of Things, or I-O-T, is the technical term we use to describe direct communication between electronic devices. This phenomenon has blossomed into existence over the past several decades. We use the IoT every day when we check traffic or look at the weather forecast. We also see it in the wide variety of smart devices that are popping up everywhere, like "smart" refrigerators, "smart" coffee makers, or "smart" watches that help inform our eating, sleeping, and exercise habits.

But rather than talking about smart coffeemakers and refrigerators, I would prefer to illustrate the potential benefits of a robust internet of things by sharing a brief anecdote about how the security alarm industry works now, and then show you how it could work better with a more developed IoT.

Imagine an emergency at a home or school or work. A burglary or violent crime-in-progress with multiple potential victims on the scene where the intruder or the victim has triggered an alarm. Speed and information are critically important to the first responders. However, when a security alarm goes off at a home, business, or public location, that signal is delayed for over a minute typically to reduce false alarms. Furthermore, the process of notifying the alarm monitoring center is surprisingly manual, as the alarm is transmitted (after the delay) to a person in the alarm center who must then be connected to another person at a 9-1-1 public safety answering point, or PSAP, for emergency dispatch.

Then, after an average 1-3 minute phone conversation between the security station and the safety agency (assuming there was no connection delay because of overwhelmed PSAPs and budget cuts), emergency responders are contacted and dispatched to the site of the alarm with nothing more than basic information about the type of alarm and location of this incident. Furthermore, there are numerous opportunities for additional human error through miscommunication. The average dispatch can take 5-10 minutes. That is valuable time and information that is lost in a true emergency. By some estimates from the Department of Justice, each year more than one million police hours and over $1.5 billion dollars are wasted due to these human error and communication issues.

Adding to the frustration is the fact that there may be additional security cameras or motion sensors and door sensors at the site of the emergency capturing valuable information. Unfortunately, in most cases, those additional sensors and cameras have no way of communicating to the monitoring station, the 9-1-1 PSAP, or the first responders. In other words, there's potential lifesaving data available that no one sees until it's too late. This can cause the first responder to arrive to the wrong place at the wrong time without important information to save lives.

With the Internet of Things, these processes could be seamlessly automated to prevent and mitigate crimes in a more efficient way. In the future, the transmission of emergency alarms and sensor data could occur instantly from machine to machine (or M-2-M), instead of manually. Automated applications could be used to gather and interpret alarm information from various IoT devices to determine the probability of false alarms and help first responders use their time more efficiently. Smart sensors and cameras could be used to automatically transmit images and data from the scene of the crime directly to officers to help them perform their duties in a safer and more efficient manner.

There have already been several successful small-scale implementations of this concept. Several alarm companies and 9-1-1 centers in Richmond and Houston have implemented a system called ASAP,

or the Automated Secure Alarm Protocol. Using ASAP, participating companies and centers were able to cut alarm transmission times down to five seconds, and reduce the volume of calls going between centers by 10 percent. Now imagine how much more productive our police, fire and EMT responders can be with fewer false alarms and better, faster information from IoT connected systems and devices. IoT can help deliver first responders to the scene faster, more efficiently and with more information on the current emergency, if we invest now in the IoT infrastructure that we need so that we go beyond smart coffeemakers and refrigerators.

Unfortunately, there are still a few technological barriers that are currently preventing us from implementing an ideal system.

The IoT consists of several key components. The:

1. Power source
2. Communication method (typically hardwired or radio)
3. Communication protocol and ecosystem
4. Data processing
5. Data security

Let's begin with power, since this is the Energy and Commerce Committee. These connected sensors in the Internet of Things must have a power source. While wired is preferred in some cases, it is typically too expensive to implement for strapped budgets for most new types of devices and sensors. Therefore battery power offers the widest array of uses, but the currently short battery life must be improved to lower the cost of ongoing maintenance and fully tap the potential of IoT.

As an example, recently, a tech startup called Quirky developed an "smart" egg holder that would tell you when you were out of eggs in your refrigerator. This sounds like an interesting and useful

smart device, but due to current battery technology, it unfortunately it needed its batteries replaced more often than it ran out of eggs to replace. When lives are on the line, instead of omelets, we need to make sure that these smart devices don't lose power. This will require investment in better, smaller, and more powerful batteries with longer lifespans.

Research suggests that Moore's law—the theory that explains why the number of transistors in circuits has increased exponentially—does not apply to batteries. To physically power our Internet of Things, we will need additional breakthroughs in the chemistry of batteries to make long-term device life possible.

Secondly, we need to ensure the availability of open wireless spectrum for IoT and specifically IoT for public safety agencies. FirstNet is a government program that is developing new wireless applications to aid first responders, instead of existing radio-dispatch technology first used in the 1960s. We need more funding for projects that involve improving our nation's infrastructure for wireless integration and emergency dispatch. Automated security will be impossible without sufficient wireless spectrum for devices and continued investment in faster wireless networks.

As an example of our outdated emergency infrastructure, currently, only about 200 out of 5,900 9-1-1 PSAP centers can handle text messages. Text messaging has been around for more than 20 years, but approximately 3% of 9-1-1 centers can receive texts. When you consider that 96% of young people text regularly, but only 67% make phone calls regularly, you can see how much emergency information we may be missing from people and devices already on our networks. Only when all emergency call centers can handle texts, tweets, IoT data and other new types of communication will we be fully utilizing IoT to save lives.

Also in our way looms the threat of multiple connection standards for smart devices. Computers generally connect to the Internet using one of two methods: Ethernet or Wi-Fi. However, smart devices

connect using a plethora of standards including Wi-Fi, Bluetooth, Ethernet, z-wave, ZigBee, and Thread, in addition to numerous proprietary protocols.

Currently a Nest thermostat may know the temperature in a home is increasing due to a fire, but it is unable to contact the 911 PSAP through the security system if the homeowner is asleep or unavailable. IoT Standards and interconnectivity would solve this. We must invest resources to develop a reliable system of cross-compatibility so devices from different manufacturers and ecosystems can talk to one another without errors.

Additionally, we must synthesize all of the data made accessible by IoT. Once we understand all the information we're collecting, we must invest in infrastructure for first responders that handle new types of communication.

As an example, my company, LiveWatch Security developed As Soon As Possible Emergency Response, or ASAPer, which is an application that is a step in that direction. It combines the speed of machine-to-machine communication with the latest group chat communication technology to allow people to process information from multiple sensors and other users. This IoT-enabled system has reduced false alarms by up to 30% while also improving response times, in some cases, by 80%. We must continue to invest in entrepreneurs that will develop these new applications that will improve the way we process data from the IoT and turn it into useful information for our first responders.

Lastly, the Internet of Things presents us with issues of privacy and security. We need to continue to develop a better understanding of exactly where our data goes, and make sure that smart devices remain hard to hack. Unfortunately, un-hackable will be impossible to achieve. This is a moving target. While systems like ours use 256-bit encryption, which is typically found in online bank security, we need to continue to push the envelope of information security.

These are all issues that can be solved with additional “smart” investment in the Internet of Things.

We can obtain the most progress towards eliminating these obstacles and automating and improving security of Americans by investing time and money in three major areas:

1. First, we should focus on engineering advances in Battery efficacy and low-power Radio range.
2. Second, we must find ways to better utilize wireless spectrum for first responders and create standards for communication between IoT ecosystems, so that IoT devices can communicate across platforms.
3. And finally, we should invest in better first responder infrastructure that can handle new types of communication to, and from, IoT devices and users.

We are at the beginning of the next big shift in technology, where machines and devices can “talk" to each other and instantly share data in ways that change lives. Clearly, the internet of things is a growing trend, but if we invest in the right places now, we can make it more than “smart” coffee makers and “smart” refrigerators that re-order eggs…We can use IoT to enhance the security of Americans and the safety of our first responders. To me, these are compelling reasons to invest in this new frontier of technology.