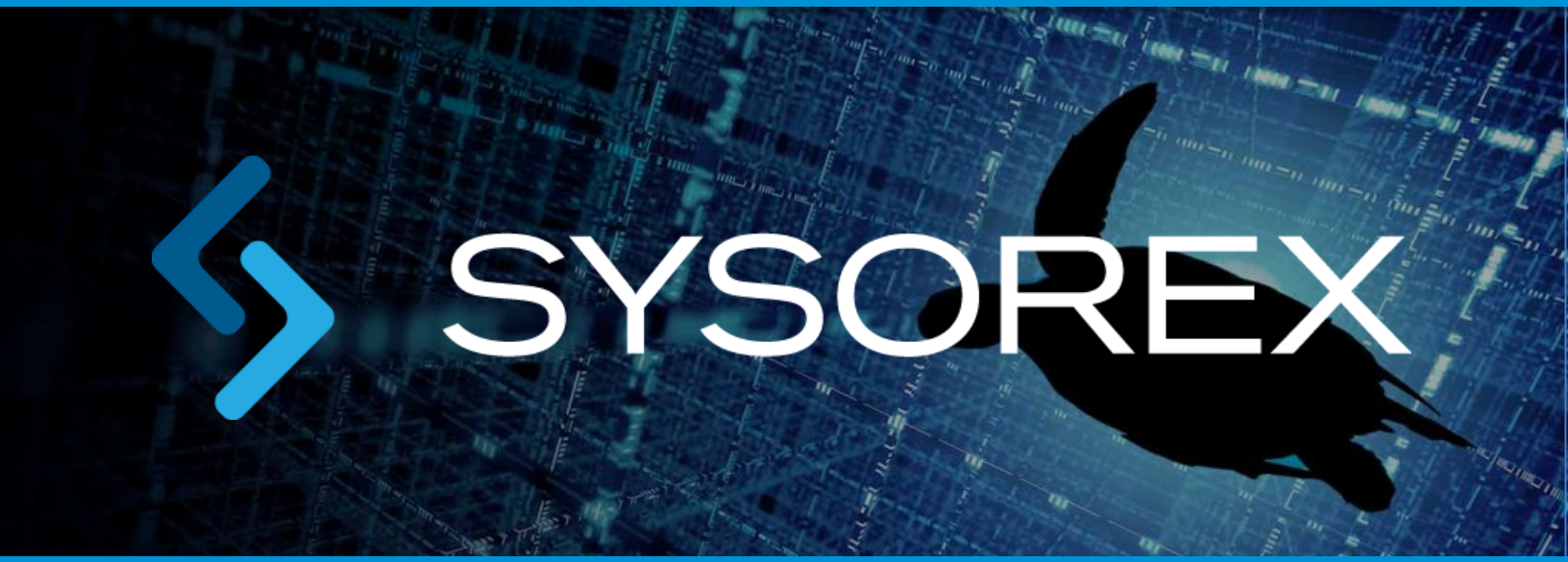
Response to Request for Public Comment

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

May 23, 2016



Submitted by:
Bret Osborn
Chief Sales Officer
bret@sysorex.com
415-299-9497

Submitted to:
Lawrence E. Strickling
Asst. Secretary for Communications and Information
National Telecommunications and Information Administration
iotrfc2016@ntia.doc.gov

1 Introduction

Sysorex USA (Sysorex), a developer of high-performance analytics solutions and leading real-time locationing and positioning sensors and systems, offers a variety of products and services that have tremendous potential to help the Department of Commerce and its subsidiary organizations implement Internet of Things (IoT)-based technologies into various levels of operation.

Our experts possess decades of cumulative experience developing and managing the most cutting-edge solutions in the field, and would be able to offer extensive consulting regarding opportunities and risks of implementation of IoT solutions. This response will serve to inform the Department of Commerce in both of these areas – potential upsides of IoT, and risk factors that the Department should consider in making IoT procurements.

We would be happy to schedule a meeting between our technical and management personnel and Department of Commerce stakeholders at your earliest convenience to discuss the possibilities and risks posed by the implementation of IoT-based technologies.

2 How can Sysorex help the Department of Commerce benefit from advancements in IoT?

The Department of Commerce stands to benefit greatly as a whole by intelligently leveraging IoT-based solutions across all levels of activity. The ability to pre-process, filter, and reduce data, and subsequently perform distributed analytics, can allow the Department to carry out rapid and reliable collection and analysis of information. Our organization is eager to help the Department realize new efficiencies and advantages on functional, cost, and schedule fronts. We know this is possible through the incorporation of real-time data collection and analytics capabilities – ideally without the need to reach back to a data center – across the spectrum of all of the Department's efforts.

Sysorex will soon release its AirPatrol 4000SE line, which will have the ability to detect programmable frequency ranges from 300 – 2600MHz. These sensors are able to detect the presence of authorized and unauthorized mobile communication devices of all kinds. Data gathered from these sensors could be combined with the spectrum analytics capabilities from our LightMiner High-Performance Analytics Platform, giving Department of Commerce the ability to perform supercomputer-level data analytics in real time. We would bring the Department of Commerce / National Institute of Standards and Technology (NIST) and its reference architecture over a decade of experience deploying radio frequency (RF) intrusion detection systems, also known as wireless IDS, along with our high-powered data analytics capabilities.

Our solution is unique in the marketplace because it detects and monitors intrusions based on the RF spectrum, as opposed to most other solutions which are based on wire. Our products passively detect intrusion while other systems rely on access to connection or connection to access. Sysorex's passive sensor systems detect and display an intrusion in real time.

Sysorex's AirPatrol IoT solutions may also be utilized by Department of Commerce and its sub-agencies for purposes beyond the detection of wanted and unwanted devices and frequencies. With regards to the Department's economic development administrations, our product is being used in commercial deployments to help companies understand everything from logistics to employee optimization to customer journey.

For example, in hospitals, our systems are used to automatically track RF-emitting electronic devices throughout the entire facility – devices of all makes and models. In hospitals, our unified, real-time tracking system monitors tens of millions of devices from crash carts to pulse oximeters providing instant logistical analysis of the location and activity of any object at any time.

For customer journeys, malls and airports have begun to deploy our product to understand all kinds of statistics, such as dwelling figures, football statistics, the amount of time people have to wait in line, or whether or not their journey takes them in and out of restricted areas. Companies of all kinds implement AirPatrol as self-insured products to ensure that visitors are not in sensitive spaces without proper escort.

In every office building, airport, or mall where Sysorex's AirPatrol solution has been deployed, it has been used in optimizing logistics and protecting intellectual property. With reference to optimizing logistics, building owners can make determinations about all kinds of information that have a direct effect on quality of services – for example:

- Did a janitor make it to a rest room, and how much time did he or she spend there?
- Is a security guard properly walking his or her routes?

Our product can be harnessed to direct security personnel straight to the point of an intrusion when a breach is detected, or to produce monthly reports on how long employees spend performing their responsibilities. AirPatrol can be deployed in conjunction with mobile device management technologies to automatically enable or disable services on end-point devices that could be used to circumvent physical security measures.

A large shoe manufacturer can serve as an effective example of a case in which Sysorex's AirPatrol product could be implemented to potentially save an organization hundreds of millions of dollars on return on investment. When a famous basketball player has a shoe designed under his name, the estimated value of the line could be anywhere from $500 million to $1 billion. If pictures of the shoe leak on the internet prior to its official release, the value of the line could top out at $100-150 million.

Sysorex's AirPatrol product can disable cameras on end point devices in sensitive facilities such as a shoe manufacturer to stop the leaking of intellectual property. Our product can disable any service on any end point device. Sysorex would be happy to meet with Department of Commerce to discuss these capabilities in greater detail.

Sysorex's AirPatrol product is the only solution in the world that can track encrypted packets across spectrum and through a physical space. While we have not yet filed any patents for these algorithms, we have over 50 pending, unique items that we would consider filing and would be interested in discussing with the U.S. Patent and Trade Office (PTO).

3 Risks presented by IoT

The single most significant security risk that IoT poses to organizations like Department of Commerce and its divisions is the presence of latent capabilities built into devices. IoT-enabled devices often run off of complex operating systems such as LINUX, but only utilize a small handful of the many capabilities that such an operating system has within it.

Latent features – inactive, dormant capabilities of a system that are never used in the primary given application of the end product – can be taken advantage of by a nefarious party to wreak havoc on a dangerously wide scale. Many vendors of IoT products offer solutions without notifying customers of the potential for latent features to be exploited by hackers. The average customer is rarely given the opportunity to understand the breadth of damage that can be done on this front.

The risks associated with latent capabilities in IoT products can be demonstrated using the example of street lights in a city. A city may wish to install adjustable LED lights within lamp poles and street lights that automatically brighten and dim according to surrounding activity. A company responding to a request for such a service will market their product by pointing out that their solution is run off of high-powered LINUX-based microprocessors that can perform edge analytics and determine day/night cycles to reduce light and noise pollution or change calibration based on activity surrounding the light posts.

If a nefarious party discovers that the embedded version of LINUX is several generations – or even a single generation – behind patch, it may very well easily be able to exploit resulting security vulnerabilities and take out an entire city lighting system with the push of a single button. While the customer was initially led to believe that the powerful and highly capable LINUX-based system was the core feature responsible for saving some funds on the energy efficiency front, it might very well be the presence of that embedded LINUX system that could lead to catastrophic results.

This example can also be applied to devices such as traffic sensors that run 24x7x365 to gather traffic statistics or issue speeding / stoplight tickets. These ever-present, always-on IoT devices inevitably contain a wide array of latent capabilities within them that can be easily taken advantage of by a nefarious actor. Sysorex's thought leaders and technical experts have decades of experience developing solutions that address these kinds of risks. We fully recognize the crucial importance of either removing exploitable latent features, or hardening such potentially vulnerable features to the point that they cannot be taken advantage of by hackers.

Another risk presented by IoT-based systems is the fact that they are widely distributed, and therefore offer many nodes of opportunity for potential attacks. If a traditional, non-IoT-based IT system is centralized to a single, secured space, it is likely extremely difficult for hackers to infiltrate the system because there would only be one or a very small number of potential vectors of infiltration. IoT inherently, exponentially increases the vectors of attack that may be exploited by a hacker that wants to inflict damage on a system.

When you combine: 1. large numbers of potential vectors for attack, 2. the aforementioned potential for latent features of a system to be exploited, and 3. the fact that many IoT devices are currently being rushed to market without considering or notifying customers of these potential dangers, the result is a perfect storm of vulnerability for companies and organizations that wish to harness the power of IoT.