Security in an Internet of Things [IoT] World

--- Point of View: Denison's CTO Vishy Narayan discusses the increased exposure to new security threats and issues created by our all-connected world and uncovers how to look at security solutions across systems, platforms and devices.

Unprecedented levels of automation and efficiency.

Today, industries are seeing unprecedented levels of automation and supply chain efficiencies as industrial control systems connect to the Internet. In the era of IoT, more and more devices connected to the network will impact our life and continuously change the way we interact with these devices. While there are many benefits in an all-connected world, we simultaneously create and are part of increased exposure to new security threats and issues created by these devices a.k.a 'things'.

How did we get here?

In the pre-IoT days, we probably had much well understood security issues – e.g.: loss of connectivity, denial of service, information theft to name a few. In a network coupled with an overlay of millions of intelligent sensors, software & applications that drive these sensors and aggregate continuous data streams and a platform to crunch data to make sense out of this – we now have created a "connected enterprise". Each of these sensors is a security threat, vulnerable to hacking and other malicious activities. Thereby these devices have just exponentially increased the probability of an attack and resultant security incidents.

When these devices become closely related to our lives in a physical world, then there is an impact on risks to our physical security. A real-life example is the 'connected car', a car with a

sophisticated sensor network, controlling and monitoring most components in the car -- from fuel mixture to engine operation' to tyre pressure – which is susceptible to hackers who can gain control of the car. From power grids to a connected healthcare devices, danger lurks. And not the least of all, every user must be concerned about the threat to their privacy as their life seems to be very much interconnected.

Now consider the fact that almost every 'thing' in our life can be connected to the internet to allow visibility and control – thermostats, air conditioners, security systems and cameras – and the list is growing. Even a conservative estimate puts the number of such interconnected things to touch 50 billion by the year 2020.

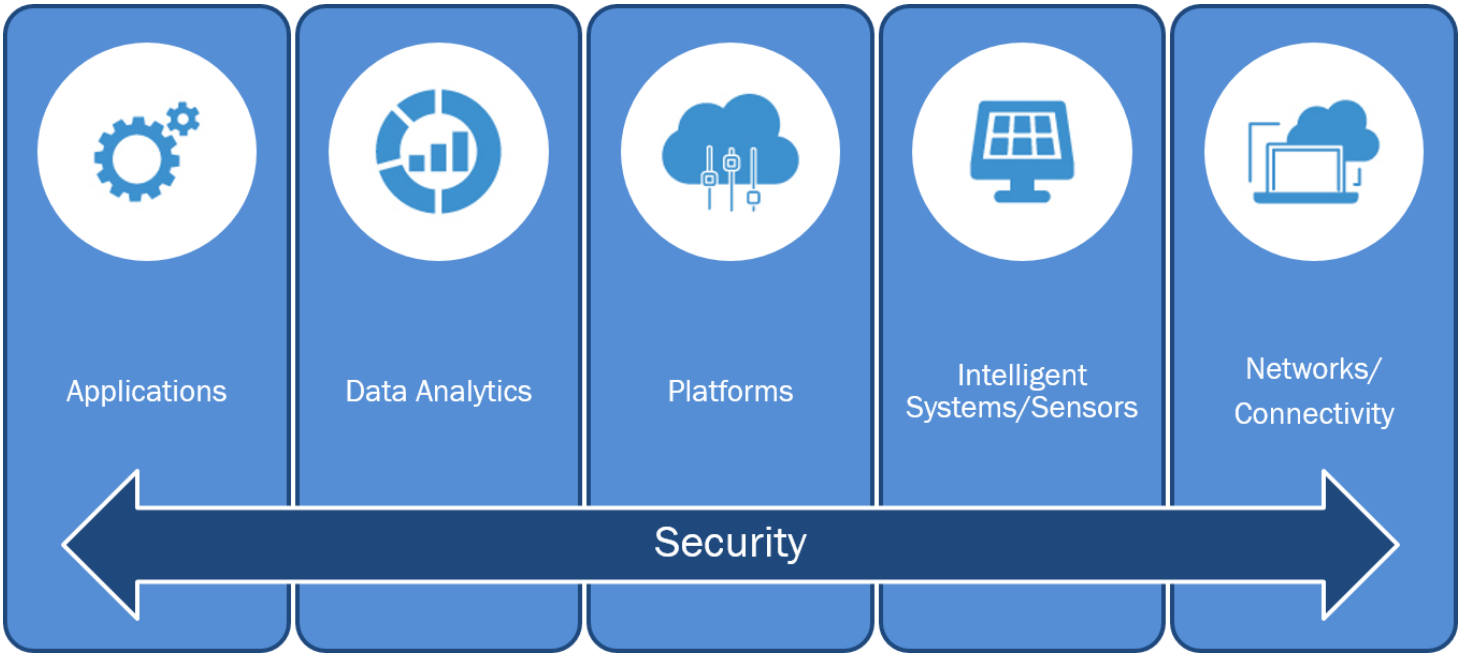
This brings us to 'security of things' and 'identity of things'.

IoT Security

The Internet of Things consists of various platforms and devices with different capabilities. Each system component will need security solutions depending on its characteristics and each element has its own security requirements and will need appropriate solutions depending on its characteristics.

Usually manufacturers of IoT devices, especially the edge devices do not focus on device security thereby causing a potential threat. The IoT applications and device ecosystem is fragmented and with the lack of security standards, there seems to be no quick and easy way to solve the security issue. However, several security standard consortiums are working to set this right.

Below is a graphic representation of what makes up the end-to-end IoT stack.



Experts do agree that the core of the IoT security is in authentication and authorization of the device. Applications with secure layers can be built upon this and it's a good practice to tie application security to network security, with additional authentication mechanisms built in at the network level.

For now, the immediate technique to resolve IoT security issues is based on authenticated security, by providing connectivity to the internet and maintaining known segregation boundaries at all times. Careful risk analysis to balance the limitations of IoT but preserving individual privacy protections in the long run is the most appropriate way to secure the emerging world which is here to stay.