The Internet of Things

Connect the Unconnected[1]

Author: Jack Fletcher, Risk Control Specialist

Published: November 2013

Executive Summary

Farmer Brown can now sit in front of his computer and determine whether his cow Bessie needs to be milked. He even knows if Flossie is about to give birth. Yes, cows are becoming wired! Through a sensor attached to the ear, farmers can monitor critical data for each of their farm animals.

The days of the meter reader being chased by the family dog are becoming a distant memory. Smart water meters can now more accurately monitor water usage, enhance water management and identify wasteful usage. Customers not only receive their monthly water bills, but sometimes even graphic analyses of their water usage as compared to their neighbors, and the utility company doesn't even have to visit.

How about a house with a Twitter account? The "House of Coates" gives a visual representation of the goings-on in San Francisco designer, Tom Coates' home. By using various hardware, software programs and interfaces, he can monitor temperature, vibrations and even the soil moisture in the Fichus pot! This is then translated into a running discussion of the events occurring in his home.[2]

Fast-forward five years and you may be using augmented reality glasses to provide overlay graphics to assist in repairing your car, fixing plumbing problems and even performing minor surgery.[3]

Are these developments intrusive or a boon to society? What are the payoffs? What's the downside?

This article will discuss the current state of the Internet of Things (IoT), including its definition and how it works. Additionally we will discuss the scope of current and future technology and its benefits and downsides.

Definition

IoT encompasses machine-to-machine communications, although definitions vary greatly. Essentially, IoT means, "Uniquely identifiable physical and virtual objects, which can be manipulated, monitored, measured, and controlled, that interact through a defined network with some form of control systems. Each object is identified via bar code, RFID (radio frequency identification), software, sensors, microchips, and other tags."[4] [5] Cisco defines the Internet of Everything (a variation on IoT) as "the networked connection of people, process, data, and things."[6]

The term "Internet of Things" was first coined by Kevin Ashton to describe a system where the Internet is connected to the physical world via ubiquitous sensors.[7]

Connect the Unconnected

Closely related to IoT is the term "Machine to Machine (M2M) communications." Wikipedia defines M2M as "a device (such as a sensor or meter) to capture an event (such as temperature, inventory level, etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information (for example, items need to be restocked)." [8]

Examples of this technology include:

- Google prototype self-guided cars
- Remote monitoring of environmental conditions in buildings, server systems and manufacturing processes
- Heads-up display systems and body monitoring systems for soldiers on the battlefield
- Facial recognition systems used in casinos to identify blacklisted gamblers

How does it work?

Each system has a sensor or actuating device, a conduit (wired or wireless connection, primarily the internet or a private network) and a controlling or reactive device. Of course, at some point, there is a human interface. Whether the human interface actually controls the system, interacts with it or simply monitors it depends on the system.

Systems can generally be divided into two primary categories [9]

- Information and Analysis - track user or device behavior (i.e., GPS vehicle tracking), provide situational awareness (i.e., soil moisture on farmland) and provide sensor driven analytics (i.e., interactive displays in retail stores).
- Automation and Control - provide process optimization (i.e., sensors that measure out ingredient mixtures), resource consumption control (i.e., use of smart meters) and complex systems controls (i.e., vehicle collision control systems).

State of Industry

Jean Baptiste Waldner, one of the early proponents of the concept of "Internet of Objects," estimated that our world is comprised of 50 to 100 trillion objects in which humans are surrounded by 1,000 to 5,000 traceable objects.[10] A more conservative estimate is that there are currently 10 billion connected devices, managing information and communications. By 2020, there will be 50 billion connections.

Cisco's IoE Value Index study estimates that IoE related activities currently generate at least $613 billion in global corporate profits.[11]

Benefits

Through the use of IoT, there is huge potential for companies to profit from savings in time, cost and labor. Sensors can streamline provisioning needs and anticipate future usage.[12] The energy, manufacturing and retail industries stand to benefit significantly by incorporating IoT into their processes, products and operations. Examples of other benefits include:

- Utility companies can monitor electrical grids on a real-time basis to anticipate load requirements.
- Service call planning can be made more efficient through better route planning.
- Companies can track package pick-up and delivery immediately.

Connect the Unconnected

- Patients can be monitored remotely for critical medical conditions.
- Construction equipment at remote sites can be monitored for needed maintenance and repairs.
- Warehouse operations such as shipping, receiving and storage can be streamlined.

Insurance companies are also taking advantage of this innovation. A recent example is the use of M2M technology, which allows the carrier to monitor the policyholder's driving behavior. A monitoring sensor is installed in a vehicle to track the driver's performance. This information is then provided to the policyholder. It can also be used to help determine the renewal premium, based upon factors including driving behavior, driving distance and trip frequency. Insurance companies view this as an especially useful tool in monitoring the behavior of younger drivers.

Challenges

IoT is an emerging technology. As such, industry standards and government oversight are still evolving, along with privacy issues and security concerns. Many devices require little or no authentication, which may be fine if the device is a volume control for your home speaker system. But what happens if the device can remotely manipulate the locks on your doors, or affect the performance of a connected medical device?

There is, understandably, some pushback from the public. Take smart meters, as an example. Within the next three years, it is expected that nearly 65 million homes in the U.S. will have wireless smart meters measuring water and electrical consumption. But some California environmentalists, liberals, Tea Party supporters and other activists have expressed concern. At the heart of the debate is whether smart meters can cause illness from the exposure to electromagnetic fields or present an intrusion on the privacy of the subscribers. In 2011, the Marin County Board of Supervisors even went so far as to ban the installation of the devices in unincorporated areas of the county.

Furthermore, industry groups and government regulators have not reached consensus regarding data privacy and data security matters. Many devices and subsystems, both critical and noncritical, connect to the internet with only minimal safeguards. The belief is that they are not considered as lucrative targets, so security is an afterthought. However, these devices can be easily circumvented by unauthorized parties and can provide a wealth of otherwise private information.

There are even websites that are designed to locate internet-connected devices. Just take a look at Shodan – http://shodanhq.com – a search engine used by academics and others to locate internet-connected devices such as routers, modems, webcams, printer servers and others. Many of these devices can be accessed with simple, default passwords or no password at all due to user laziness and incompetence. A recent analysis indicated that there are 114,000 business and industrial control systems that are logged onto the internet with known security flaws and 13,000 of these devices/systems are accessible without passwords. Hackers could potentially use such access to reboot corporate and IT servers, and access medical device logs and industrial control systems at various utilities.[13]

There are also liability issues to consider. Equipment failure or faulty commands could potentially lead to injury, property loss and loss of income. The scope of liability, due to systems failing to properly control an intended device, is still being established.[14] There is no firm data on the scope of this type of loss. However, if hackers can circumvent your

system through a "back door" device and cause disruption to safety critical functions, the potential for loss could be significant.

Conclusions

IoT is upon us. Use of these systems can be of great benefit to companies and consumers alike. However, as with any emerging technology, security and privacy considerations need to be addressed and properly managed to maximize efficiency and mitigate risk.

- Security: Users may be unaware of system hacks because end-use devices are considered a low priority. Security settings on installed devices may have lower security settings because there is more concern with the primary system compared to end-use devices. A holistic approach needs to be taken with regard to the impact of a device on the entire system. According to Verizon Business' vice president for Strategy and Development in the Asia-Pacific region, Robert Le Busque, "If it has an IP address, regardless of whether it's fixed or mobile or a device, it needs a security protocol, and that security policy should be in line with the fully blown policy that the enterprise has." [15]
- Compatibility: Components and devices need to be assessed to determine their compatibility with existing systems. What security features are included? Is authentication required prior to activation? Are security patches and updates provided? Are adequate password selection and change protocols in effect?
- Privacy: The scope of usage for data obtained from devices such as smart meters and vehicle tracking devices must be clearly defined. Privacy policies for companies that use this data should be reviewed to ensure that the data is not being used in unintended ways.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Dan Bauman, Vice President of Risk Control for OneBeacon Technology Insurance at dbauman@onebeacontech.com or 262.966.2739.

References

1 "Connect the Unconnected" term developed by Cisco: http://newsroom.cisco.com/press-release-content?articleId=1114539

2 Talking House, Industrial Internet: http://www.industrialinternet.com/blog/3-questions-for-tom-coates-on-his-talking-house/

3 Big Data Republic: http://www.bigdatarepublic.com/author.asp?section_id=2635&doc_id=264165

4 Internet of Things, Wikipedia: http://en.wikipedia.org/wiki/Internet_of_Things

5 Princeton University: http://blogs.princeton.edu/etc/2012/02/24/the-internet-of-things

6 Internet of Everything, Cisco: http://blogs.cisco.com/IoE/?POSITION=SEM&COUNTRY_SITE=us&CAMPAIGN=internetofeverything&CREATIVE=IoE_IoE&REFERRING_SITE=Google&KEYWORD=internet+of+things_p|mkwid_sRhwW0y30|dc_27848629755_0v0xx7y7d0

7 Kevin Ashton: http://en.wikipedia.org/wiki/Kevin_Ashton

8 Machine to Machine, Wikipedia: http://en.wikipedia.org/wiki/Machine_to_machine

9 Internet of Things, McKinsey Quarterly: http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things

10 Waldner, Jean-Baptiste (2007). Nanoinformatique et intelligence ambiante. Inventer l'Ordinateur du XXIeme Siècle. London: Hermes Science. pp. p254

11 Internet of Everything (IoE) Value Index, Cisco: http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf

12 AT&T – Machine to Machine: http://www.business.att.com/enterprise/Family/mobility-services/machine-to machine/?WT.srch=1&WTPaidSearchTerm=machine+to+machine&source=EENT16MECguIhFSVp&wtpdsrchpcmt=machine+to+machine&wtpdsrchprg=Enterprise+-+Mobility+Services&wtpdsrchgp=ABS_SEARCH

13 Tom Simonite, Technology Review: http://www.technologyreview.com/news/514066/what-happened-when-one-man-pinged-the-whole-internet/?utm_campaign=newsletters&utm_source=newsletter-weekly-computing&utm_medium=email&utm_content=20130502

14 Ibid 9

15 M2M and the Internet of Thing: How secure is it?: http://www.zdnet.com/m2m-and-the-internet-of-things-how-secure-is-it_p4-7000008389/