Internet of Things Offers Great Opportunities and Much Risk

Marcelo Hector Gonzalez, CISA, CRISC, supervises IT environment and internal control in banks operating in Argentina. He is also responsible for auditing cross-border data processing outside of Argentina for international financial entities. He is a member of the Commission of e-Banking in the Central Bank of the Republic of Argentina, which has published several booklets on e-banking best practices. Gonzalez can be reached at *marcelohgonzalez@gmail.com.*

Jana Djurica works at the National bank of Serbia as an IT supervisor of the Serbian financial sector. She is an IT expert with experience in auditing IT areas such as IT governance, risk assessment, internal IT audit, IT security, business continuity management, disaster recovery planning, IS development and IT outsourcing. She can be reached at *janadjurica@yahoo.com.*

There are a number of definitions of Internet of Things (IoT), with all of them having slightly different meanings. Some define IoT as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure; others say that IoT represents appliances connected to the Internet, and there are many more definitions. The definition that, for now, seems to make the most sense is: "IoT is a scenario in which objects, animals or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT is a world where virtually everything is imbued with one or more tiny computers or smart sensors, all transmitting a flow of data onto the Internet."[1] Wikipedia.com defines IoT as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure;[2] and Webopedia.com describes IoT as the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.[3]

Keeping in mind the variety of definitions and the many differences between them, it can be concluded that IoT remains in its initial phase of evolution. Soon, cars, homes, major appliances and other basic objects from everyday life, even city streets, will have the capacity and the need to be connected to the Internet, creating a network of objects that will be able to control everything. This network will be made of millions of devices with sensors that can generate or capture constant streams of data. The potential appears endless.

FORUM

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

THE POSSIBILITIES WITH IOT

IoT consists of three principal components:

- **The things themselves** that, in most cases, represent the devices or sensors with the ability to capture or produce data, and the time to create an effect on the environment in which they have some influence
- **The communications network** that interconnects the things (this network connectivity, in most cases, is wireless)
- **The computing systems** that process and use the data received and/or transmitted by the things, with, in most cases, a minimal computational capability

Turkçesi de bulunmaktadır
www.isaca.org/currentissue

By using this infrastructure, things can communicate with each other and even optimize activities among each other based on the analysis of data streaming through the network.

These data can be personal data (which, if compromised, carries significant legal implications with regard to privacy) or environmental data, such as measurement of temperature, barometric pressure and wind activity, for example.

Imagine that someone is about to leave home to go to work or for a walk. The sky is somewhat cloudy and the person wonders, "Will it rain?" There is not enough time to go back inside and wait for the weather forecast on television or to turn on a computer to see the weather forecast. However, next to the front door is the umbrella stand and the handle of the umbrella has a red light, a warning that there is a chance of rain, so the person decides to bring the umbrella as a prevention when he/she leaves the house.

The purpose of IoT is for regular elements to perform the functions for which they were designed but at a higher intelligence rate, adding to their aggregate value. This is shown with the umbrella example where a simple device is connected to the Internet to obtain some useful data that will provide it with the ability to fulfill the same original function of protecting against the rain, but at an improved level because of additional valuable information. David Rose, author and instructor at the Massachusetts Institute of Technology (Boston, USA) Media Lab, has the following vision: "IoT is technology that atomizes, combining itself with the objects that make up the very fabric of daily living."[4]

Examples of IoT are slowly becoming reality. A US company, Ambient Devices, already develops these kinds of devices, including an umbrella that connects to AccuWeather[5] and alerts the user of the need for an umbrella.

The imagination could take this much further. Imagine a water sprinkler that uses Internet forecasts, weather sensors and usage information to optimize water expenses and improve ecological behavior. What about a public trash can that can compact all the trash inside it and alert the city trash gatherers when it is full?

Home security systems already allow homeowners to remotely control door locks, lights and thermostats (**figure 1**), but what if they took proactive measures such as cooling the home and opening windows or turning lights on based on owner preferences, weather conditions, owner proximity to home or cost expectations?

Figure 1—Internet of Things All Around the Home

Source: Gonzalez and Djurica. Reprinted with permission.

POTENTIAL RISK

We are living in a continuously increasing smart world where not only personal computers, tablets and smartphones are connected to the Internet, but also an incredible amount of different devices—everything from pill bottles and umbrellas to refrigerators, watches and cars—are coming online. The only limitation seems to be the imagination.

This technological trend is remapping how the world and individuals interconnect with each other and everything else. This implies a higher immediate security risk for people, homes and enterprises than the risk caused by current consumer technologies.

The increasing trend of making buildings more energy efficient, green friendly, secure and responsive to changing environmental conditions is resulting in diverse Internet-enabled technologies. These building or home management systems are not only becoming increasingly more integrated with each other, they are also integrating into systems outside the perimeter of each edifice, creating a smart grid.

Many of the Internet-enabled intelligent devices embedded in modern homes and organizations have little security built into them, making them vulnerable to attacks that could disrupt normal use or operations and create safety concerns. This is a critical problem that must be resolved.

As the number of lamps, thermostats and sensors that can connect to mobile phones increases, so does the number of malicious hackers who will want to try to disrupt these devices, or make money by wreaking havoc. Weakly protected building management systems connected to the Internet could also provide a way for malicious attackers to break into systems connected to the same network, but outside the originally targeted one.

Someone could take control of a home, a whole building or a town. Security systems must develop in the same way and at the same pace as do all these new intelligent systems being created with the things around us.

> "Security systems must develop in the same way and at the same pace as do all these new intelligent systems being created with the things around us."

The threat is not only that someone could penetrate a home or a building system to cause serious disruptions. There is also a potential impact on technology infrastructure that could result in a loss of communications due to a system outage or unauthorized access to data because of poor segmentation between the automation network and the infrastructure security network.

> “Establishing trust in a broad range of things across dispersed settings and on a massive scale is a challenge for information security experts.”

Traditionally, home and building management systems have not been considered IT systems; they are not overseen by an information officer and have long been considered operational technology under the management of facilities designers. This will have to change with the emerging use of IoT in homes, buildings and cities. Facilities designers, administrators and IT experts will need to work together to identify and mitigate potential security risk. “The IoT offers a very appealing vision of harnessing technology today to lead to a better tomorrow. But focusing too much on the data and not enough on the beliefs and behaviors of the people attached to the ‘things’ can create major privacy and security risks.”[6]

Several barriers exist that prevent mass prevalence of IoT as a part of smart buildings, at home or in an enterprise. Those are:

- Smart technology in IoT is still not cheap and becomes even more expensive if the technology is designed with strong security measures. In fact, the security of these systems is currently at a fairly low level.
- Smart technologies in IoT are not totally interoperable and at the moment do not exist in a unique architecture.

However, it is just a matter of time before these obstacles are overcome. Thus, information security and control experts need to begin adjusting to these possibilities now.

PRIVACY ISSUES RELATED TO INTERNET OF THINGS

The things in IoT, such as cars, toys and home appliances, can be used for unlawful surveillance. These Internet-connected things could allow attackers to obtain far more information than they could previously. For example, attackers may be able to monitor children through cameras installed in toys, monitor people’s movements through Internet modules installed in a smart television, or monitor when a person enters or leaves his/her home by connecting to an Internet-connected door lock. Such threats are not merely speculative. Many of those present real vulnerabilities in Internet-connected modules installed in cars, medical devices, airplanes engines and children’s toys, because not all of those devices were designed with privacy or security in mind.

Those Internet-connected modules could allow attackers not only to passively monitor their victims, but also to actively intrude into their private lives. This is because many of those things can be remotely controlled so an attacker can divert the signal in order to remotely stop the refrigerator, start the heater or unlock the door.

Another important issue is that IoT enables the creation, storage and sharing of enormous amounts of data about a person’s habits, behaviors and preferences. As a result, regulatory bodies, including the US Federal Trade Commission and the European Commission, are turning attention toward the potential privacy and security issues that the IoT presents in citizens’ everyday lives.

Needless to say, establishing trust in a broad range of things across dispersed settings and on a massive scale is a challenge for information security experts. The devices themselves are vulnerable to physical attacks, the networks over which they communicate are not always secured and the back-end systems and data repositories are attractive targets for thieves and terrorists. Opportunists, hacktivists, malicious insiders and even unscrupulous governments are all potential attackers with the ability to intercept critical data in transit or seize control of these devices.

With more and more things connected to the Internet, the potential privacy implications, the general false sense of security associated with design and the possibility of data compromise grow more critical. Thus, IoT needs to rely on two things: trust and control. These two concepts present an opportunity and a challenge at the same time for information security experts and IT auditors.

> “It is an Internet-scale problem that will require an Internet-scale solution.”

This leads to the same questions e-commerce posed 15 years ago when Amazon was interacting with millions of customers. The difference now with IoT is that, for example, a utility company can interact with millions of smart meters or a transit center can interface with thousands of cars. Mutual authentication, secure communications and high-integrity messaging, all at an Internet scale, will become core security foundations for these systems, so it is an Internet-scale problem that will require an Internet-scale solution.

This is much more serious than a privacy issue; it is about rights to modify things that can then profoundly impact the security, health, environment, finances, relations and more of millions of individuals (**figure 2**).

If IoT use increases, as experts expect, millions and millions of devices will come online and managing security around a very large network of different kinds of devices will be a crucial, urgent and complex issue.

If a large, branded supplier of IoT devices implements a complete home or business IoT solution and an intruder manages to attack and steal personal health or financial data or physical belongings, it will be a disaster not just for the individual, but also for IoT device suppliers around the world. For example in the worst-case scenario, if an attacker modifies the parameters of when a medicine dispenser has to alert a pharmacy to refill it, this becomes a potential matter of life and death.

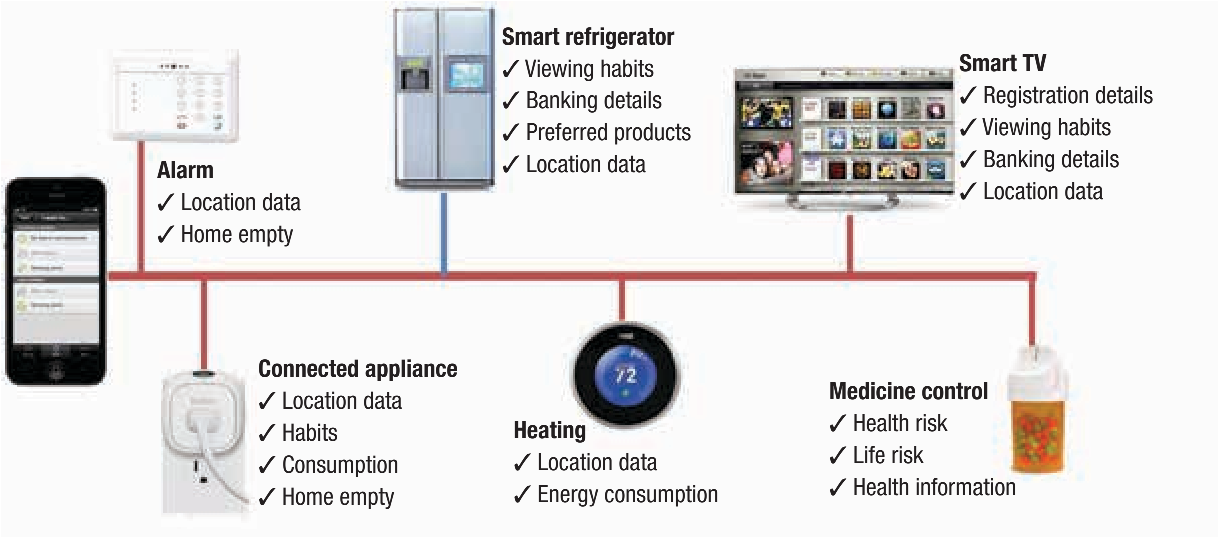
Attacks can also multiply in scale as one attack goes viral. For example, if a burglar hacks a door system in a home while the homeowner is out, this can escalate to a viral situation in minutes across a large territory in which the same door lock provider has installed similar systems.

SECURITY FOR IOT

Most of the devices in IoT are always connected and, thus, always vulnerable. Issues around Internet security and mobile devices' interrelations already present a challenge in this era of constant connectivity. In the scenario of a home or business owning numerous connected devices, those challenges will be even greater.

An ineffective or nonexistent plan for deploying security updates will be the single largest impediment for IoT. The reality is that vulnerabilities appear in all code from time to time, so a solid security life cycle that considers security throughout design and development will have notably fewer security issues. However, all software manufacturers must be ready to quickly respond to vulnerabilities and release patches to protect their users.

Figure 2—Personal Data at Risk



Source: Gonzalez and Djurica. Reprinted with permission.

As all these scenarios show, securing connected devices should be a major component of IoT, but security is not at the top of the to-do list for the companies that are manufacturing connected devices. Many of the engineers who develop the devices have more experience in design and the interconnection of devices, which may result in security not being considered in depth or worse: being totally overlooked.

Another cause for the lack of security in connected devices may be cost. To make these devices secure, manufacturers need to take extra steps, such as developing security models, creating patches to maintain secure devices and doing penetration testing for vulnerabilities. Because of these, some companies might opt out of security altogether. And further complicating matters is the fact that many of these devices use embedded software and cannot easily be patched.

To accelerate IoT development, some companies are developing technologies to address the security, interconnection and interoperability challenges and enable solutions. For example, Intel offers several versions of development kits with a combination of performance and software capabilities—the reason being that there are different types of developers, ranging from hobbyists and enthusiasts to professionals.

Unfortunately, every new technological development comes with a new set of security threats.

FACTORS TO CONTROL IN THE INTERNET OF THINGS.

Attention must be paid in order to achieve control and minimize the potential IoT risk and to:

- **Minimize collection of personal data.** Sensors such as smart meters are aimed at encouraging end users to shift electricity usage to off-peak hours or to control water usage with the goal of helping the planet and lowering costs. Those sensors are designed to collect consumption data in order to determine the usage of electricity, water or other utilities and set prices accordingly. These data are collected at the individual level, so one measure could be to control which data can be exposed to the Internet without an individual's consent.
- **Minimize connecting data with individuals.** It is important to assess whether devices or software need personal information or some other data that could be connected with individuals or their private information. For example, is it necessary to use Internet service provider (ISP) data or can static Internet Protocol (IP) data be provided? The optimal method is to collect data without connecting it to individuals. It is always preferable to aggregate data on a higher level rather than using data that could be connected to an individual person.
- **Minimize and secure data retention.** Sometimes, depending on the sensor or device brand or configuration, data are not only sent, but also stored inside the device or in several devices around the Internet, in the communication or with the utility provider. Therefore, one best practice is to make certain that data sent through the network are encrypted to prevent personal information leakage in transit. Also, if there is a connection with a utility provider, no additional data (apart from data that were agreed upon at the assumption of the service delivery contract) should be transmitted.

Additionally, traditional controls should not be forgotten:

- If something is connected to a home or business network, it can be accessed over the Internet and, thus, ensure that it is secured in relation to that which it is exposed.
- Review the security settings on any device installed. If it is remotely accessible, disable this feature if it is not needed. Change any default passwords to something difficult to guess. Do not use common or easily guessable passwords.
- Depending on the complexity of the IoT installation in a home or a business and the level of existing exposure, install a firewall to protect all of the resources inside it.
- Regularly check the manufacturer's web site to see if there are updates or patches to a device's software.

It is important to keep in mind that the requirements for connecting a car information system sensor are quite different than the security requirements for a home, business, corporation, or public safety or government entity. All of these unique requirements add complexity to the implementation and control of IoT security. There is no simple solution that would secure such a diverse collection of devices, and there is no single, effective security strategy because different devices from different manufacturers have different security risk profiles. Meanwhile, until a consolidated security solution is in place, IoT security's focus would be most effective if on the data, rather than on the devices. As such, when data are stored, in process or in transit, protections enable individuals and enterprises to provide security and privacy simultaneously.

> “There is no simple solution that would secure such a diverse collection of devices.”

THE HUMAN PERSPECTIVE RELATED TO IOT

The Jetsons[7] was set in the sky-high Orbit City and the show featured a family living an average life in the future with flying space cars, instant transport tubes, robots and lots of technological gadgets that enabled them to get work done in a matter of seconds.[8]

In a not-too-distant future, the reality will be even more sensors, gadgets, micro devices, and perhaps robots that will do a lot of things that people used to do, a lot of things that people are not able to do and a lot of things that people do not like to do.

The future holds many uncertainties with regard to how IoT will affect people. Perhaps many people will have to learn different skills at home and at work, as some basic jobs will be replaced by devices that work together in collaboration with the Internet.

The Google Self-driving Car is an example. Imagine a world full of cars with no human drivers where people enjoy the car journey doing things such as resting, reading or playing. It sounds amazing and in many ways unimaginable, but to get there, many changes will have to take place beyond the simple creation of the technology. For example, such IoT technology may provide malicious hackers an opportunity to implant a virus in the network of traffic sensors and traffic controls, changing information about where traffic jams are located or where there are demonstrators.

> “IoT challenges should be met proactively with sound planning, good security strategies and frequent IoT audit assessments.”

The industry must get prepared for profound changes to current cybersecurity strategies and operations as IoT introduces an avalanche of new devices, network traffic and protocols, physical and physiological risk, applications that demand data security improvements, and wider and deeper malware attack surfaces. IoT challenges should be met proactively with sound planning, good security strategies and frequent IoT audit assessments.

ENDNOTES

[1] TechTarget, WhatIs.com, “Internet of Things,” *http://whatis.techtarget.com/definition/Internet-of-Things*

[2] Wikipedia, “Internet of Things,” *http://en.wikipedia.org/wiki/Internet_of_Things*

[3] Stroud, Forrest; “Internet of Things,” *Webopedia*, *www.webopedia.com/TERM/I/internet_of_things.html*

[4] Rose, D.; *Enchanted Objects*, Scribner, USA, July 2014

[5] AccuWeather is an American media company that provides for-profit weather forecasting services worldwide.

[6] Stroud, Robert; “The Convenience/Privacy Trade-off on the Internet of Things,” *Wired* Innovation Insights Blog, 17 December 2013, *http://insights.wired.com/profiles/blogs/the-convenience-privacy-trade-off-on-the-internet-of-things?xg_source=activity#axzz3MNq2UmCe*

[7] Hanna-Barbera, *The Jetsons*, an animated US television series (sitcom) that aired from 1962-1963.

[8] Tucker, Jeffrey A.; “The Attempted Militarization of the Jetsons,” Mises Daily, Mises Institute, 21 September 2005