ON THE GO

IOT: *IMPLICATIONS* (of Things)

By David Massarik

The United States Government Accountability Office (GAO) recently released its seminal report on IoT.

The GAO released the formative technology assessment report in May, 2017, entitled, "Internet of Things: Status and Implications of an Increasing Connected World". As IoT technologies are embedded in a growing number of devices and applications, the number of connected devices is expected to increase exponentially.

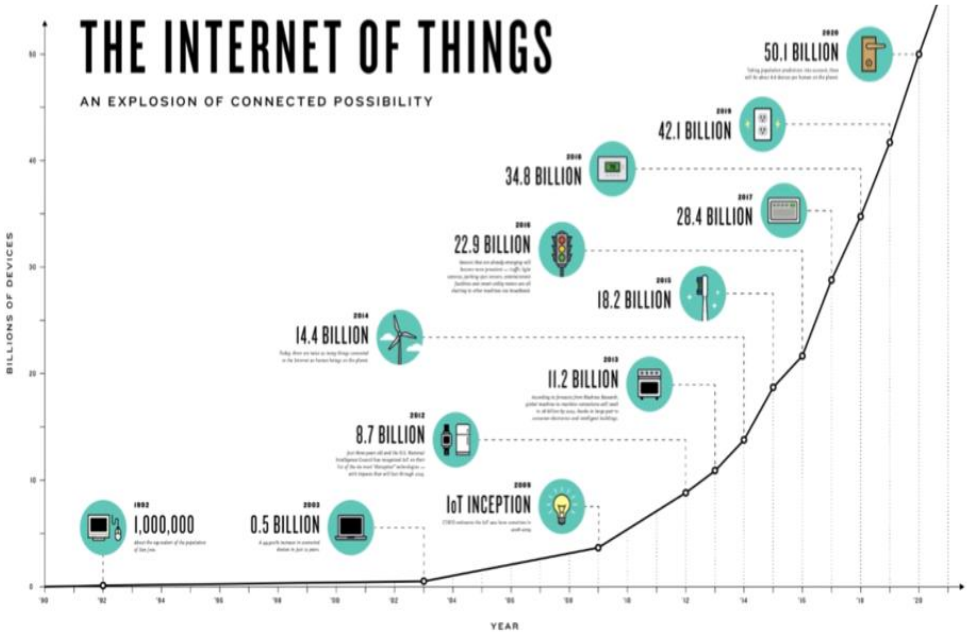
In 2013, the number of devices connected to the Internet globally was estimated to be over nine billion. According to the McKinsey Global Institute, an estimated 25 to 50 billion devices will be connected to the Internet by 2025. All of these connected devices will lead to significant technology and economic disruptions.

The IoT is being adopted globally across multiple sectors, including the public sector, agriculture, health care, IOT-mobility, security manufacturing, and energy, among others. IoT technologies have evolved from a tool for simple communication and tracking via networks to include service-based business offerings that rely on data analytics. Adoption will likely accelerate as IoT devices become more affordable and offer increasing benefits. However, significant challenges accompany the wider adoption of IoT technologies. For example, devices that collect health information on patients may be vulnerable to hacking.

With the rapid global expansion of IoT, security and privacy measures become increasingly important to curtail its misuse.

Although there is no single U.S. federal agency that has overall regulatory responsibility for the IoT, various agencies

(continued on page 20)



IOT: *IMPLICATION*

(continued from page 17)

oversee or regulate aspects of the IoT, such as specific sectors, types of devices, or data.

Generally, industries use the IoT to reduce costs through efficiencies, among other things, while addressing the challenges of enhancing interoperability of IoT devices, and maintaining security and privacy. Estimating the economic impact of the IoT is complicated due to the large number of widespread applications that span various economic sectors and related environmental impacts. Economic opportunities resulting from the IoT may be accompanied by disruptions that pose challenges to certain businesses and job categories. Examples of cyber-attacks that could affect IoT devices and networks are shown in the table (right).

IoT and security is becoming a recognized issue beyond this GAO government study. At the past several BLACKHAT and DEFCON conferences, numerous presentations have covered security issues related to IoT with topics such as, 'IoT-WILDLY INSECURE', and 'IoT security: broken and getting worse'. Implications for the future….of Things.

O T G

Types of attack	Description
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports. | GAO-17-75