NOW IS THE TIME TO GET SERIOUS ABOUT IoT SECURITY

Introduction

Nearly four decades ago, programmers at Carnegie Mellon University came to a decision. Dismayed by treks to an often dysfunctional Coke machine, they installed micro-switches and connected the machine to the internet and a departmental computer. A program allowed them to see if the machine was stocked and the bottles chilled.[1] Amazingly, this event served as the first Internet of Things (IoT) device.

Figure 1. CMU Coke Machine: First IoT device.

Today, active IoT device connections are expected to reach 9.9 billion globally, and with a potential to double in size over the next five years.[2] Gartner says enterprise and automotive IoT will grow to 5.8 billion in 2020, with the utilities industry leading the way for most IoT endpoints.[3] Another source expects IoT technology spending will reach an astronomical $1 trillion by 2020.[4]

After experiencing explosions with cloud and mobile computing, IoT represents yet another technology challenge in our digitally transformed world. And like every fledgling technology, IoT will be challenged – for both legitimate reasons and motives from the dark side.

In this paper, we'll discuss IoT security and discover how vulnerable you are to hacks. Is IoT a breeding ground for cyberattacks? We'll also look at the implications for user and data security, and what you can do to secure your organization.

[1] "The 'Only' Coke Machine on the Internet," Carnegie Mellon University Computer Science Department
[2] "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating," by Knud Lasse Lueth, IOT Analytics, August 8, 2018
[3] "Gartner Says 5.8 Billion Enterprises and Automotive IoT Endpoints Will Be in Use in 2020, Gartner press release, August 29, 2019
[4] "Six IoT predictions for 2019," by Fredric Paul, Network World, January 2, 2019

What Are IoT Devices and Where Do They Come From?

IoT devices are physical objects that automate home, business, and industry tasks. Internet-connected devices with embedded sensors detect and respond to input from the physical environment, giving information to another system or to guide a process.[5] The infographic below shows the diverse range of sensor-enabled IoT devices that control many aspects of our personal and work lives.[6]

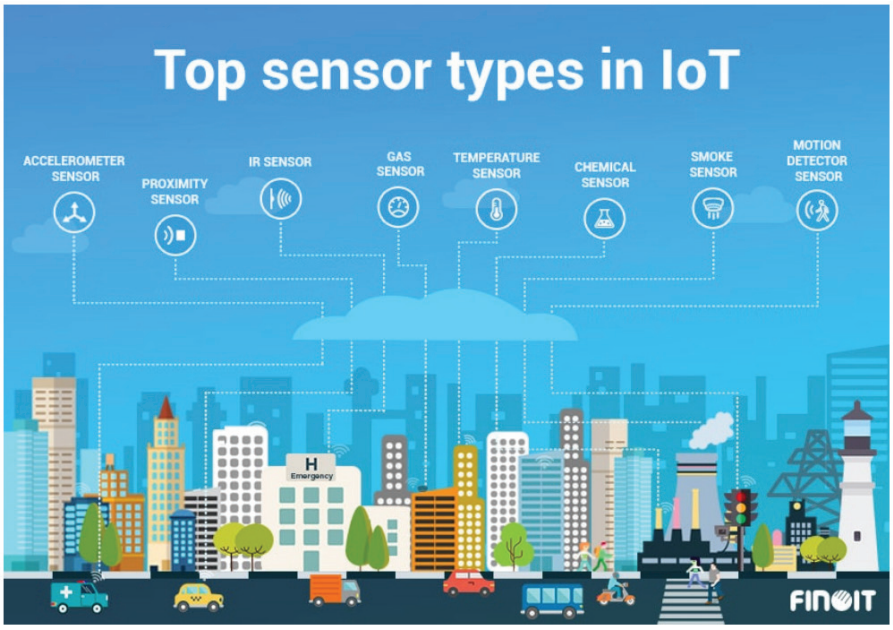


Figure 2. Source: Finoit – Sensor types

IoT's massive network of devices collect large amounts of data. Some devices we encounter daily such as security systems, thermostats, electronic appliances, lighting systems, alarm clocks, digital assistants, and speaker systems.

Figure 3. Dashboard symbols

Automobiles are filled with sensors. Tiny icons on dashboards reflect the sensors that monitor the status of your car's functions. Proximity sensors help you park or avoid cars in blind spots. Sensors track the operations with the engine, brakes, heating/cooling, emissions, and more.

[5] "Sensor Data," by Margaret Rouse, IoT Agenda, TechTarget

[6] "Top 15 Sensor Types Being Used Most by IoT Application Development Companies, by Rita Sharma, Finoit

Enterprise Industrial IoT (IIoT)

Industrial IoT (IIoT) refers to the billions of industrial devices that use sensors connected to wireless networks. The low cost of sensors and high wireless bandwidth have sparked a market with an estimated $197 billion in 2019.[7] Existing technologies such as 5G, IoT sensors and platforms, edge computing, AI and analytics, robotics, blockchain, additive manufacturing, and virtual/augmented reality are helping to fuel IIoT technology.[8] One source conducted a survey to pinpoint the top 10 use cases for IIoT. The results are offered in the graphic below:[9]

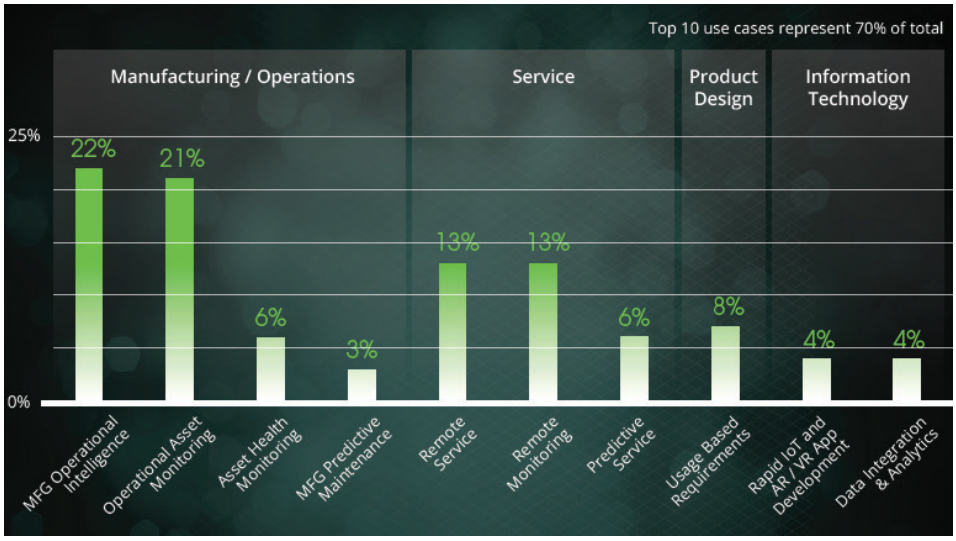


Figure 4. Source: PTC – Top 10 use cases (70% of total)

Not surprising, the top two use cases, manufacturing intelligence and operational asset monitoring, are sweet spots for manufacturers and other industries. In order to increase operational efficiencies, manufacturers require constant process improvements, including increased automation, improved analytics, and of course, digital connectivity.

INDUSTRIE 4.0, Germany's strategic initiative, is moving the country to the forefront of advanced manufacturing solutions. Some likened this movement to the fourth industrial age, shifting to decentralized internet-based production technology and services. INDUSTRIE 4.0 promises to increase manufacturing productivity levels by up to 50 percent and halve the amount of required resources. IIoT is the important link that pairs production with network connectivity.

German manufacturer, Schwering & Hasse, produces 32 million miles of high-grade copper wire a year at a rate of 50,000 production events a second. IoT helps control the temperature, conductivity, tension, and thickness for each type of wire it produces. Other IIoT examples include Amazon's smart warehousing, Airbus factories, and Hitachi. Caterpillar, the heavy-equipment manufacturer, has used augmented reality and IoT applications to give operators an insight into the machine's overall condition.

---

[7] "Sensor Data," by Margaret Rouse, IoT Agenda, TechTarget
[8] "Top 15 Sensor Types Being Used Most by IoT Application Development Companies, by Rita Sharma, Finoit
[9] Ibid.
[10] "INDUSTRIE 4.0," by Owen Huang, Germany Trade and Invest
[11] Ibid.
[12] "Germany Turns Manufacturing into an IoT Art Form," by Dr. Stefan Sigg, RTInsights, September 4, 2019

Healthcare IoMT

Figure 5. IoMT wearable process.

The Internet of Medical Things (IoMT) is a collection of internet-enabled medical devices and applications. They can be configured with machine-to-machine communication and be connected to a cloud platform. The data is analyzed by practitioners to suggest treatment.

Manufacturing of Internet of Medical Things (IoMT) has reached nearly $18.8 billion in 2018,[13] and projected to reach an astounding $322.2 billion by 2025.[14] Diagnostic equipment accounted for the lion's share, but improved patient behavior monitoring in real time is receiving wide attention. With almost half of the world's population lacking basic healthcare services,[15] preventing a medical condition with real-time monitoring (and avoid costly treatment in hospital visits) has major ramifications, especially for underserved populations. This trend was validated in Figure 3 as remote service and remote monitoring occupied the top two capabilities in the Service category.

Telehealth practices are important for healthcare. They can improve patient-centric care and reduce provider costs. Connected wearable medical devices collect patients' health information remotely. Patient activity data is transmitted in real time to a computer, tablet, phone, or to the cloud for inspection by patients and caregivers.[16] Insulin pumps, defibrillators, scales, CPAP machines, cardiac monitoring devices, and oxygen tanks are connected to the internet for remote monitoring. This segment is forecasted to grow at a CAGR of 35.9%.[17]

[13] "IoT-Enabled Healthcare Equipment to Surpass $69 Billion by 2020," 24x7 Solutions for Healthcare Technology Management, March 13, 2019

[14] "Internet of Things (IoT) Healthcare Market to Reach $322.2 billion by 2025," Meticulous Market Research, July 31, 2019

[15] "World Bank and WHO: Half the world lacks access to essential health services, [100] million still pushed into extreme poverty because of health expenses," World Health Organization, December 13, 2018

[16] "Internet of Things (IoT) Healthcare Market to Reach $322.2 billion by 2025," Meticulous Market Research, July 31, 2019

[17] "IoT-Enabled Healthcare Equipment to Surpass $69 Billion by 2020," 24x7 Solutions for Healthcare Technology Management, March 13, 2019

IoT Devices: Hiding in the Shadows

IT professionals have lived through the security nightmares with shadow IT, or when employees install and use unauthorized hardware and software. History is repeating itself with shadow IoT, the practice of using internet-connected devices without IT knowledge or approval. Gartner predicts that by the end of next year, one-third of all successful attacks on enterprises will take place on shadow IoT resources.[18]

Virtual assistants, smart TVs and speakers, gaming consoles, fitness trackers, and wireless thumb drives are IoT devices that have entered the workplace. Even company kitchens are beginning to see internet-connected appliances, including next-generation WiFi-connected vending machines that accept payments via mobile apps. HVAC systems are controlled by Wi-Fi-enabled thermostats. One source claims one-third of companies in the U.S., U.K., and Germany have more than 1,000 shadow IoT devices connected to their network on a typical day.[19]

There's no disputing the convenience and productivity with IoT devices. However, without built-in security controls, they represent a definite risk. How often has a router, for example, been delivered with easily obtainable default IDs and passwords that user fail to change? Even worse, these credentials can be added to an organization's wireless network without IT intervention or knowledge.

Connected devices can be discovered using botnets. Shodan is a search engine that gives visibility into what's connected to and visible from the internet. You can search a subnet or domain for connected devices, open ports, default credentials, and even known vulnerabilities. However, attackers can see the exact same detail.[20]

[18] "Shining light on dark data, shadow IT and shadow IoT," by Mike Elgan, Insider Pro, September 13, 2019

[19] "What is shadow IT? How to mitigate the risk," by James A. Martin, CSO, March 5, 2019

[20] Ibid.

IoT Security

As the IoT ecosystem continues to grow with more devices, data, and market solutions, organizations will need to get serious about IoT security. It's not just manufacturing or healthcare industries that need to secure devices. It's a concern for everyone.

IoT devices, often with outdated software and legacy operating systems, are highly vulnerable to cyberattacks. These devices increasingly collect and store data attractive to cyber thieves. The risks of a cyberattack on healthcare organizations is huge. Such attacks could lead to loss and sharing of personal data, altering a patient records such as prescribed medicine and dosages. Hacking of MRI, ultrasound, and x-ray machines is also a worry with hospitals. Smartphones and tablets on Wi-Fi networks common place. Patient data is valued by hackers as it can be sold on the dark web. A compromised device also allows attackers to move laterally across the network, stealing other sensitive data.

The fears about insecure IoT devices on the internet is already playing out. Hackers are using powerful botnets to target IoT devices. One recent example is Echobot, a new variant of the Mirai IoT Botnet. This far-reaching attack has exploited over 50 different vulnerabilities, causing a sharp rise in the "Command Injection over HTTP" vulnerability. Researchers have found this attack has impacted 34% of organizations globally.[21]

IoT devices face other security challenges. IoT appliances are resource-constrained and lack the compute resources to implement strong security. Sensors, for example, cannot handle advanced encryption. Mindset is another challenge. Many devices are installed in the field or on a machine and basically forgotten. Manufacturers consider built-in security too costly from a development standpoint.[22]

The concept of networking IoT appliances and other objects is fairly new, so security is not considered a priority during the product design phase. Plus, the nascent IoT market has fueled manufacturers to launch their IoT products quickly and without security features.

Some older non-IoT assets were connected to networks and retrofitted with smart sensors. These units with weak or non-existent security are no match for modern cyber threats. Finally, there are no industry-endorsed security and interoperability standards for IoT.

[21] "August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices, Check Point Research, September 12, 2019

[22] "IoT security," by Margaret Rouse, IoT Agenda, Tech Target

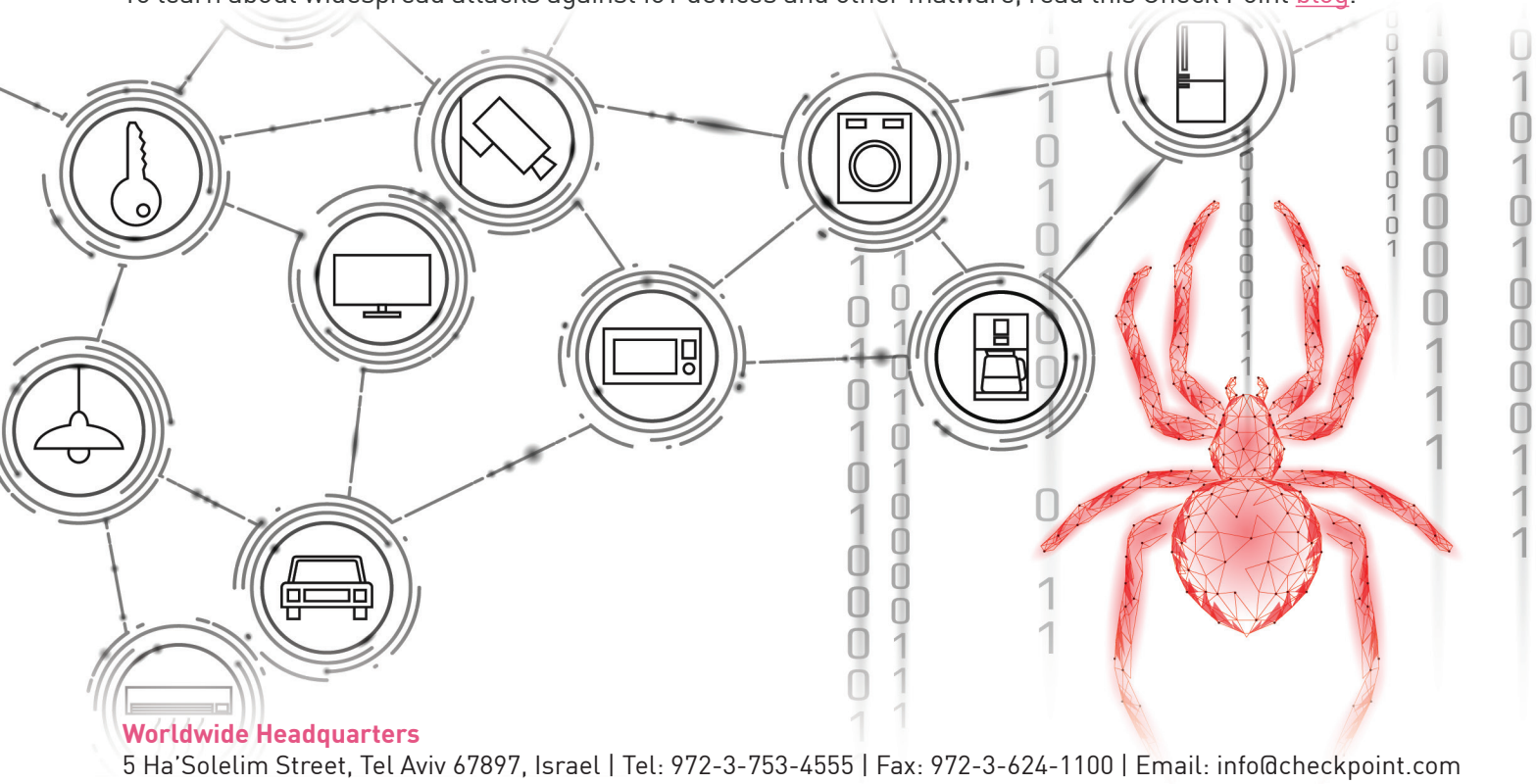
Conclusion: IoT at a Serious Inflection Point

The usefulness of connected devices is threatened by cyber criminals who scrutinize the digital landscape for vulnerabilities. No device, service, program, or application is immune from a breach. The internet serves as the conduit for cyberattacks which puts computers, smartphones, clouds, and IoT devices at risk.

Now is the time to get serious about IoT security. The vulnerabilities discussed in this paper highlight the importance of putting IoT protections on their IT security posture. While there are still issues and vagueness with IoT security protocols, an organization can much to protect data.

Whether you're a manufacturer, utility company, or a healthcare network, large business or small, you must be aware of the entry points across your network. With potentially thousands of devices connected to the IT network, and any one containing hardware or software vulnerabilities, it's important to consider advanced, proactive prevention security. Creating network segments is a best practice that allows IT to embrace new digital solutions while providing another layer of security to network and data production, without compromising performance and reliability.

To learn about widespread attacks against IoT devices and other malware, read this Check Point blog.



Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com