Analyzing Insider Risk Within the Internet of Things (IoT)

Justin R. Kinney, Ph.D.
Oak Ridge National Laboratory

Abstract

Recent technological advancement has created a growing convergence of innovation. From machine learning to ubiquitous computing to wireless networks and automation, the world is seeing new technology increasingly capable of connecting with each other. Devices and systems use open communications networks to interact, process information, and react. This is called the Internet of Things (IoT) and is comprised of physical devices that exchange data over networks, creating revolutionary possibilities. The most common way most people interact with an IoT is through "smart home" products which use microphones, speakers, and phones to control a variety of devices, from lights and thermostats, to cameras, to appliances and vacuum cleaners. But the open nature of IoT networks—necessary for their ability to communicate and operate—also introduces privacy and security concerns. At a personal level, this might mean a hack into a home to steal private information, but when applied in broader industries like health care, transportation, manufacturing, or the military, this vulnerability can have serious consequences. As IoT usage and interconnectivity increases, so too does the susceptibility to malicious actors. And the entire system is only as secure as its least secure member. This creates particular risk and vulnerability to radiological material industries, as an insider adversary with a certain level of skill could utilize the IoT to potentially steal or access sensitive information about employees, sites, or systems; or sabotage security or maintenance from a more remote—and less secure—device. The IoT relies on a secure network across the entire system, especially in transport which may lack the security of more permanent locations; if one device fails, it can create a ripple effect and an insider threat may seek to exploit that connectivity. Although IoT benefits drive increased innovation and usage, there are also vulnerabilities an insider threat could exploit; this risk of an IoT to radiological material must be addressed in any mitigation effort.

Introduction

The broad concept of a smart device dates back to at least 1982. Enterprising students at Carnegie Mellon University discovered a way to "program" a vending machine that could communicate its drink inventory status via a network. The idea of an Internet of Things (IoT) exploded in popularity as technology further developed the ability to communicate and connect. Physical objects used sensors and software to exchange information with other devices over the internet or similar networks. And the number of IoT devices in use and able to connect to broader networks is increasing at an exponential rate, evolving as new technologies are introduced; machine learning—a key component of artificial intelligence (AI)—and ubiquitous computing—where miniature computers can be found in a variety of forms and locations (e.g., smart glasses, clothing, home appliances)—are converging in new and exciting ways. These devices have the potential to be groundbreaking and innovative, changing how people interact with the world. AI home assistant

devices started as a way to play music, adjust the lights, or check the weather, but their uses have grown more sophisticated; it is now possible to use a smart home device to start a car, purchase items, and control major appliances like a fridge or oven. This connectivity eases tasks in a variety of contexts but also raises questions about how best to embrace them in a safe, secure manner. The "smart home" is far from the only scenario where the IoT has emerged; these networks can be found in health care, manufacturing, security systems, transportation, building and industrial automation, infrastructure, and agriculture. Other, more specified fields have even created derivative acronyms, such as IoMT (Internet of Military Things). IoT's benefits are numerous and widely embraced. However, concerns about privacy and security have emerged, and increased connectivity also increases vulnerabilities that an adept or well-positioned insider could exploit.

Why do we embrace the IoT?

Cornelius Peterson, CEO of NETsilicon Inc., said in 2004 that "The next era of information technology will be dominated by [IoT] devices" (Teresko, 2004). Roughly half a decade later, Cisco Systems estimated "more 'things' were connected to the Internet than people" (Evans, 2011), and that ratio has only grown since. An estimate from 2022 suggested that more than 40 billion IoT devices, sensors, and actuators were installed in the world, and the number will continue to grow (TechJury, 2022). The IoT is likely to become one of the most disruptive, society-altering technologies in decades, if not longer. Humanity has found applications for IoT devices in a number of spaces, but the average person is most likely to encounter them in consumer usage. From wearable technology to home automation, the IoT has many benefits that are becoming increasingly easy to access. In 2022, the average United States household used an average of 22 devices connected to their home network (Deloitte, 2022). Yet it is not simply about making life easier. Safety features like medical emergency recognition or disability assistive technology give users greater autonomy and quality of life (Demiris, 2008). And home automation includes industrial applications, such as the electrical systems in energy-efficient buildings and environmentally friendly alternatives to non-networked devices.

The medical uses for the IoT further expanded into "smart health care," sometimes called Internet of Medical Things. It is estimated that roughly 30% of all IoT devices are used in the health care industry (Frost & Sullivan, 2017). People can better monitor and track their own health, both in the moment and over time, creating a new culture of health cognizance with blood pressure and heart rate devices, hearing aids, and other sensors that can be monitored remotely, often with smart watches that anyone can purchase. Within hospitals, this technology is even more extensive, allowing medical professionals to better evaluate a patient's health concerns and act accordingly to address diseases, disabilities, and other conditions.

The benefits beyond the individual are also apparent; the IoT can monitor and automate farming data, operate public infrastructure like railways, and assist environmental and climate protection. Even the government and military have embraced the concept from wearable biometrics and sensor-covered robots to radar tracking systems. And the IoT is changing the way business sectors are thinking of operations; the World Economic Forum (2020) estimates that the Industrial IoT alone will add $14 trillion to the global economy by 2030.

Humanity has embraced interconnectivity with its many benefits to everyday life, health care, military applications, industrial and manufacturing, and more. However, interconnectivity also introduces concerns about privacy and security. Linking devices and using them to control aspects of one's life increases the likelihood of hacking, identity theft, and more. Therefore, IoT safety and security must be acknowledged and addressed.

IoT: The new safety and security threat

In 2018, a casino in Las Vegas was hacked. A secure database of their high-roller customers was stolen—nearly 10 GB worth of personal data about the casino's biggest spenders. It was a stunning heist; casinos are known for their top-notch security, and anonymity and personal information are worth a lot to their customers. So how was someone able to pull that off? The answer lies in the IoT. This particular casino wanted to create a relaxing, yet exotic atmosphere for their visitors and had installed a large aquarium in its lobby. The fish residing within required the water temperature to be within a specific range, so a smart thermostat was installed that could automatically adjust the water temperature and salinity remotely—it even allowed for remote feeding of the fish—and was connected to the casino's wireless network. But it was a weak link. Hackers exploited that device's vulnerable security features to gain access to the network. According to Nicole Eagen, CEO of the cybersecurity company used to protect the casino's infrastructure, "They then found the high-roller database…pulled that back across the network, out the thermostat, and up to the cloud." (Marks, 2021)

As the casino example shows, IoT connectivity creates vulnerabilities; it expands the potential attack surface a hacker could target and, if not well protected, opens holes in the overall cybersecurity defense strategy. And IoT security can be inadequate in many cases, particularly fields that use electronics and sensors that are older and possess outdated cybersecurity protocols. This security risk becomes especially problematic when older technology is integrated with newer systems because of their different levels of security capabilities. Several years ago at DEFCON 26, a hacker convention, researchers demonstrated how to use a standard printer and fax machine to steal company data with only a fax number and a phone line; vulnerabilities allowed them to send specialized malware through the fax line, which allowed access to sensitive information across the connected network.

The danger of networked devices not only includes stealing information or tampering with equipment, but it also involves life-threatening dangers. In 2017, the Food and Drug Administration announced that an implantable pacemaker by St. Jude Medical had security vulnerabilities; if someone hacked the remote monitor, they could alter how the pacemaker functioned, including sending fatal shocks to the individual (IOT Solutions World Congress, 2018). In 2015, a team of hackers demonstrated the dangers of onboard software in a vehicle by taking control of the speed and wheel of an SUV (IOT Solutions World Congress, 2018). If a malicious individual sought to harm a specific person, hacking into a similar networked device could have fatal consequences.

The IoT integrates a wide variety of systems and, once inside a single area, it is a trivial matter to pivot between two systems utilizing the same network. In fact, the IoT is purposely designed to be interconnected for ease of use; its interconnectivity is a feature, not a bug. It has become a part of

daily life and offers many benefits, but even a single unsecured or lesser-secured device that appears innocent, turns the IoT into a double-edged sword. An easily guessed or reused password, weak authentication protocols, or anything else that compromises security makes for an easy access point. Once one link begins to crack, the entire security chain becomes vulnerable. This makes those risks even more vital to prevent in sensitive, high-security industries, such as nuclear and radiological security.

Radiological/Nuclear Space

The IoT is rapidly expanding connectivity into a variety of spaces, including radiological and nuclear industries. On the radiological side, such material is often used in academic, environmental, and medical fields; radiation oncology—the branch of medicine dedicated to diagnosing and treating cancer—is one field that routinely uses radiological materials (Gupta et al., 2020). Continuous monitors, digital medications, AI, and even robotics have all begun to be integrated within the field (Thaker et al., 2022). Environmental monitoring networks have also been used to detect, identify, visualize, and control radioactivity within waste or recycling containers (Manzano, 2020; Tran-Quang et al., 2022), among other things. Yet probably the most direct space where the IoT and radiological materials have become most integrated in the materials' transportation and storage phases.

Infrastructure networks and surveillance systems are installed to secure and track radioactive materials during storage and transportation, and the IoT is slowly being implemented into those systems for more comprehensive, real-time monitoring. Like any other facility with security devices, interconnectivity is a key component of the system. The use of IoT allows for more data, better monitoring, and stronger understanding of any critical systems in place to safely maintain the materials. The ability to remotely collect data also permits greater flexibility for workers, facilities, and response personnel. When the material is being transported, this could include vehicle software, traffic monitoring and management, synchronizing traffic lights, GPS systems, communications networks, and more (Zorkany & Morsi, 2022). Many have noted the immense benefits that such a system provides, but it ultimately suffers from the same risks as any other comprehensive security network. Much like the casino case, the greater interconnectivity of the cybernetwork, the more nodes that can be accessed—both of the authorized and unauthorized varieties.

On the nuclear side, smart nuclear power plant (NPP) operating systems are increasing in popularity, due to safety concerns. Advanced control and instrumentation devices to remotely monitor real-time facility operations can help minimize manpower that would be required to work in close proximity (Ali et al., 2022). The adoption of this new technology allows for better data collection, better maintenance, and detecting potential failures earlier, which would give response teams more time to react. But as with any new innovation, there are risks, and when dealing with particularly sensitive materials, that risk is greater. So balancing and navigating that risk becomes of utmost importance. Because they deal in sensitive material and information, NPPs must be constantly kept at optimum levels of maintenance and security. Cybersecurity concerns and data privacy must be considered ahead of time and included within any mitigation plan. That's not to say those risks are too great to consider implementing an IoT, but any oversight in that implementation could see severe consequences.

The Insider and the IoT

A chain is only as good as its weakest link. If even a single link breaks, it compromises the strength of the entire chain. In a security sense, that means that a network is only as secure as the least secure device. Usually, devices which contain or have direct access to the most sensitive content are well protected, both with physical barriers and multiple cybersecurity measures. But like the thermostat in the casino aquarium, secured devices' innocuous-looking, network-connected counterparts can easily be overlooked. Whether it is a sensor designed to maintain a specific water temperature for exotic fish, a sprinkler system, smart light bulbs, CCTV cameras, a personal phone, HVAC systems (the access point in the infamous Target hack in 2014), or a smart watch with GPS tracking, once they connect to a larger network, it creates a new node for access. If that secondary or tertiary device has weaker security measures, that device creates a vulnerability. And IoT cyberattacks are already on the rise with roughly 1.5 billion breaches in a six-month span in 2021 (Cyrus, 2021).

Conventional approaches for dealing with information security threats are simply not strong enough for the IoT. Information flows freely across systems, which is what it is designed to do, but there is not enough agility in standard measures to deal with the new threat area that a webbed network of devices creates. Consider an art museum with a famous oil painting on display. The piece of artwork possesses a lot of similarities to digital information: it needs to be accessible to many different people because that is, ultimately, its designed purpose. But complete access must still be tightly controlled, and activity surrounding the painting is heavily monitored. When an unauthorized person attempts to get too close to the painting, alerts go off, and security closes in. Similarly, information security and the IoT is largely about access control and activity monitoring. Cutting off access entirely would defeat its purpose; it needs to remain accessible across the network in order to reap the benefits. But by tightly controlling who can get close and the actions they are allowed to take within the network, it is possible to better manage cybersecurity. Yet that is precisely why insider threats can be so damaging in an IoT world.

The insider is in a particularly vital position when it comes to protecting the IoT. The IoT exacerbates the challenge posed by insiders to the security of many companies because of their unique, trusted position (Kim et al., 2020). An insider possesses a certain amount of access, authority, and/or knowledge that could be used to harm an organization in some capacity. Thus, a person in this capacity could possess the knowledge of what devices are connected to the network, their specific locations and abilities, the types of security measures in place (physical and cyber), and how to access those devices through login information, key cards, or other measures. Even if that individual does not have login information or physical access to every device, they could feasibly still access the device using a more remote part of the network which, depending how the network is constructed, might be enough. But the risk is more than just the devices already on the organizational network; personal IoT devices could also be used to create insider adversary attacks. Smart glasses have hit the market in the last several years, capable of taking photos and recording video. Smart contact lenses with embedded cameras are on the way and would be even harder to detect (Business Insider, 2014). Even an accidental incident could expose real dangers involving unwitting insiders, and it would be even worse with malicious ones.

Insiders are more than direct employees of an organization as well, who may be vetted through thorough background checks or government security clearances. Third-party vendors, visitors to the site, or even the food caterers for a social event—all may have authorized access to certain locations of the organization. Even if only temporary access, that can be enough time to gather useful information. And anything they bring in from outside—a personal laptop that was not inspected, a wearable piece of technology with a built-in camera or microphone, or even just their personal cell phones—could be used in an insider adversary attack. Whether using that device to hack into a less secure device and access something it should not, or recording photos, videos, or audio and sending it via the cloud to a server elsewhere, the IoT creates security vulnerabilities. It is important to be aware of what knowledge, materials, and areas insiders possess access to, and what they could further access because of that entry point. Compartmentalization of knowledge or access, segmented security systems that are not all part of the same network, strong security measures across all devices—even seemingly innocuous ones, and careful vetting of authorized individuals to minimize insider risk are all measures that should be taken in light of an IoT. A carefully planned insider risk mitigation policy must be in place because the IoT raises the stakes.

Conclusion

The Internet of Things is a technological achievement that is growing daily as it expands into more fields and becomes more deeply integrated into daily life. For the average consumer, that might mean losing privacy or the theft of personal information. For an industry dealing in nuclear or radiological materials, that might mean the risk of unauthorized removal or use of dangerous material and sensitive data, or the sabotage of important systems. The insider carries an outsized risk in an IoT setting because access is more remote; no longer does an adversary need direct, physical access to gain control or information. That access is spread broadly to more places, both physically and through digital, online networks across devices with varying levels of security measures. Information is readily shared across an IoT, so access control becomes of utmost importance because that is where an insider threat could thrive. Therefore, while the IoT brings many benefits for ease and safety, increased innovation, and more, it also introduces vulnerabilities that could be manipulated by an insider adversary or exploited using an unwitting one. Any cybersecurity measures and insider mitigation efforts employed by an organization would be wise to strongly consider and address this threat.

References

Adams, Dominique. “Hackers Find a Back Dory: Vegas Casino Fish Tank Heist.” *Digit News*. 18 April 2018. Accessed 21 March 2023. https://www.digit.fyi/iot-thermometer-fish-tank-hack/.

Ali, Amanat; Gudarzi, Yasin; Abouabdellah, Bassma; Elzayat, T.; Furquan Ali, Mohammad; Saini, Gaurave. (April 2022). “Smart Nuclear Power Plants Operating System through IoTs,” *International Journal of Engineering Research & Technology*, 11(4): pp. 344–351.

Business Insider. (2014). “Google Wants to Create Smart Contact Lenses with Cameras Inside,” http://www.businessinsider.com/googles-smartcontact-lens-concept-2014-4.

Cyrus, Callum. (2021). “IOT Cyberattacks Escalate in 2021, According to Kaspersky,” *IOT World Today.* Published 17 September 2021. Access 20 March 2023. https://www.iotworldtoday.com/security/iot-cyberattacks-escalate-in-2021-according-to-kaspersky.

Deloitte. (2022, August 3). “Consumers Benefit From Virtual Experiences, but Need Help Managing Screen Time, Security and Tech Overload” [Press Release]. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/connectivity-and-mobile-trends.html.

Demiris, G; Hensel, K (2008). “Technologies for an Aging Society: A Systematic Review of ‘Smart Home’ Applications.” *IMIA Yearbook of Medical Informatics*, 17: 33–40.

Evans, Dave. (April 2011). “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything” (PDF). *CISCO White Paper.*

Gupta, S.; Johnson, E. M.; Peacock, J. G.; Jiang, L.; McBee, M. P.; Sneider, M. B.; and Krupinski, E. A. (2020). “Radiology, Mobile Devices, and the Internet of Things (IoT).” *Journal of Digital Imaging*, 33(3): pp. 735–746.

“Internet of Medical Things, Forecast to 2021.” (June 2017.) *Frost & Sullivan*. Accessed 21 March 2023.

IOT Solutions World Congress. (2018). “5 Infamous IoT Hacks and Vulnerabilities.” Accessed 19 March 2023. https://www.iotsworldcongress.com/5-infamous-iot-hacks-and-vulnerabilities/.

Kim, Aram; Oh, Junhyoung; Ryu, Jinho; Lee, Kyungho. (2020). “A Review of Insider Threat Detection Approaches with IoT Perspective,” *IEEE Access*, 8: 78847–78867.

Manzano, L. Gallego; Bisegni, C.; Boukabache, H.; Curioni, A.; Heracleous, N.; Murtas, F.; Perrin, D.; Silar, M. (December 2020). “A Distributed and Interconnected Network of Sensors for Environmental Radiological Monitoring,” *Radiation Measurements*, 139: 1–11.

Marks, Gene. “A Casino Gets Hacked Through a Fish-Tank Thermometer.” *Entrepreneur.com.* 1 June 2021. Accessed 21 March 2023. https://www.entrepreneur.com/business-news/a-casino-gets-hacked-through-a-fish-tank-thermometer/368943.

TechJury. (February 2023). “How Many IoT Devices are There in 2023? [All You Need to Know],” 7 February 2023. Accessed 21 March 2023. https://techjury.net/blog/how-many-iot-devices-are-there/.

Teresko, John.(December 2004) “NETsilicon Inc. Waltham, Mass.,” *IndustryWeek.* Retrieved 20 May 2022.

Thaker, Nikhil G.; De, Brian; Shah, Chirag; Manda, Sudhir; Royce, Trevor J.; Beriwal, Sushil. (September 2022). “Practical Application of the Internet of Things in Radiation Oncology,” *Applied Radiation Oncology*. pp. 7–17.

Tran-Quang, V.; D. V. Hung, T.-T. Dat and D.-V. Doan. (2022). “An IoT System for Detection and Identification of Radioactive Material in Scrap Metal Recycling,” *2022 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, pp. 1–6.

World Economic Forum. (2020). Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities. *World Economic Forum*. [Online] https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-iot-robotics-and-smart-cities.

Zorkany, M. & Morsi, H. (2022). “Safety of radioactive materials transportation and storing assisted by IoT,” *ASME Journal of Nuclear Engineering and Radiation Science*, 8(3): 031901.