**IoT Research Report – Introduction to Information Security**

Arthur H. Neumann

Carnegie Mellon University

Randy Trzeciak

April 25, 2022

IoT Research Report – Introduction to Information Security

## Abstract

The rapid growth of the internet of things (IoT) and the ubiquitous integration of IoT devices by organizations and individuals alike have enabled society to capitalize on a seemingly endless stream of new technologies. Each new IoT technology provides innovative ways to solve critical problems, enhance business capabilities, and streamline daily life. While IoT devices have the potential to create new opportunities, unfortunately, these opportunities can come at a high cost to organizational security. A rapidly changing IoT device market, lack of manufacturer incentives to implement secure design practices, low customer expectations for security, and no universal framework for IoT security have resulted in significant risks associated with the implementation of IoT devices. This paper will identify the emerging threats and vulnerabilities associated with IoT devices and analyzes the security implications of operating IoT devices within critical infrastructure, organizational, and personal networks. This analysis includes an examination of organizational, personal, and societal implications associated with implementing IoT devices leveraging insufficiently secured hardware and software. Lastly, this paper will explore three potential solutions to reduce the number of security defects in IoT devices and improve organizational and individual cybersecurity through software-defined networking, secure IoT frameworks, and an IoT device security certification process.

*Keywords: i*nternet of things, IoT, information security, network security, IoT design

## Introduction

Rapid enterprise adoption and sustained growth and investment in internet of things (IoT) devices are clear indicators that IoT is here to stay for the foreseeable future. A study conducted by IoT Analytics, a leading provider of market insights based out of Germany, indicated that the global IoT market grew by 22 percent in 2021, raising annual investments to USD 158 billion. IoT Analytics further estimates that the number of connected IoT devices will reach 14.5 billion worldwide by the end of 2022 (Wegner, 2022). While the COVID-19 pandemic has had a minor slowing effect on IoT growth, increased availability and affordability of high-speed 5G networks are expected to expand connectivity significantly and drive a new surge in IoT growth.

As more and more IoT devices are added to organizational and mobile networks, the likelihood of devices ending up in networks supporting critical infrastructure sectors identified by the Cybersecurity & Infrastructure Security Agency (CISA) rises. CISA defines critical infrastructure sectors as manufacturing, communications, commercial facilities, energy, financial service, agriculture, healthcare, IT, transportation, and water (Cybersecurity & Infrastructure Security Agency, n.d.). While IoT has great potential to change life as we know it today, it is not without significant security implications that pose a severe risk to critical infrastructure and society.

## Security Implications of the Internet of Things

Widespread enterprise adoption of IoT devices has not come without significant challenges and implications for organizational IT Security. Every new IoT device added to an organizational network widens its attack vector, increasing the number of targets for malicious actors, including nation-state Advanced Persistent Threats (APTs), hackers, cybercriminals, and hacktivists. According to the SANS Institute 2021 Survey of Operational Technology (OT)/Industrial Control System (ICS) Cybersecurity, hackers and organized crime represent the two most significant sources of ICS network intrusions in 2021 (Bristow, 2021, p. 8). While malicious actors are nothing new in the cybersecurity field, the widespread adoption of insecure IoT devices has enabled increases in activities such as ransomware, extortion, data exfiltration, and capturing devices to participate in botnets used in distributed denial of service (DDoS) attacks.

### IoT Vulnerabilities

IoT devices pose a unique security challenge to organizations. Many IoT devices are so specialized that there are no clear established security standards, no method for organizations to secure them properly, and insufficient support to maintain legacy devices. Of the organizations surveyed by the SANS Institute in 2021, 52.2 percent believe their biggest challenge is the lack of IT understanding of OT operational requirements, and 59.4 percent indicated their organization struggles to integrate legacy OT technology with modern IT systems (Bristow, 2021). An inability to configure and maintain IoT devices has severe implications for IT security and introduces the potential for significant vulnerabilities to exist within organizational networks.

Every device added to an organization’s network comes with risk; this is more so the case with IoT when combined with a lack of understanding of how to configure and secure IoT devices properly. Improperly configured devices expose organizational networks and offer attackers easy targets for exploitation. Due to a lack of understanding, users and administrators installing IoT devices with factory defaults often do not provide the adequate security functionality required to protect the device from compromise. Furthermore, improper configuration or failure to properly maintain legacy IoT devices leaves organizations open to exploitation due to insufficient access control, a lack of data protection safeguards, and known vulnerabilities in the device's software packages.

### Effects of Vulnerable IoT Devices

An example of these vulnerabilities affecting IoT devices used in households and organizations is the exploitation of unmaintained household appliances with IoT functionality. This exploitation is exhibited by smart refrigerators that have been compromised by attackers using replay attacks facilitated by flawed access control combined with insecure hardware and software design (Zetter, 2016). Unbeknownst to their owners, many of these compromised IoT devices participate in botnets that can be used to further damage critical infrastructure in Distributed Denial of Service (DDoS) attacks or even cause demand surges resulting in damage or disruption to power grids (Greenberg, 2018). In this example, not only is the organization or person implementing an IoT device impacted, but another critical infrastructure such as the electrical grid is also potentially affected.

Organizations adopting IoT must consider the risk associated with insecure IoT devices and understand the potential exposure and vulnerabilities related to improper implementation. To better understand and manage the risk, exposure, and vulnerabilities, organizations adopting IoT must ensure adequate network security and ensure IT staff understands how to correctly implement and maintain IoT devices and the networks hosting them. For many organizations, this means increasing security devices and adding funding to support additional maintenance costs, security staffing, and security technology. Organizations must understand that even after mitigating much of the risk associated with IoT implementation, there will always be residual risk that could have severe organizational consequences.

## Insecure hardware and software implications for the Internet of Things

In 2010, information security researchers discovered a worm that is believed to have been developed by a coalition of nation-states to disrupt Iran’s nuclear program. The worm, which affected Iran’s capability to enrich uranium throughout 2009 and 2010, targeted the subset of Industrial Control Systems (ICS) known as Supervisory Control and Data Acquisition (SCADA) systems. More specifically, Stuxnet targeted a particular Programmable Logic Controller (PLC) responsible for controlling enrichment centrifuges in Iran’s Natanz nuclear facility (Chen & Abu-Nimeh, 2011). For many organizations and cybersecurity practitioners, the Stuxnet worm was a wake-up call that emphasized the potential dangers of implementing insecure IoT devices on organizational networks.

### Market Pressures and Poor Security Design

While a major manufacturer with a vested interest in producing secure quality devices made the PLCs exploited by Stuxnet, many manufacturers face significant pressures that drive them to adopt poor manufacturing and software development security practices. In a rapidly growing and competitive IoT market with substantial investments coming from all sectors, these pressures incentivize developers to design IoT hardware and software as lean as possible, with only enough resources to complete specific tasks, leaving insufficient resources remaining for security. In his book, Geekonomics: The Real Cost of Insecure Software, SANS institute instructor and IT Security professional David Rice suggests that many software developers are driven to be the first and fastest to market with technology products. A significant implication of being first and fastest is the potential for rapid and sloppy development that leads to buggy or vulnerable systems. Rice proposes that a major contributor to this is the rapid pace of the software market and high competition within the industry. He further suggests that a poorly designed product released first can quickly become the standard in a highly competitive market instead of the well-designed product that came to market second (Rice, 2007).

Designing secure hardware and software adds costs associated with vulnerability analysis and testing both during and after the product has been built. Startup companies attempting to draw revenue as fast as possible to ensure their success may not develop products with security in mind. Furthermore, companies rushing to get a product to market may be incentivized to forgo security testing altogether to ensure they are first and fastest. In an IoT market with 1,207 startups, as indicated by IoT Analytics in 2021, every additional day is another day a potential competitor could secure their product as the market standard (Lueth, et al., 2021). Every extra day spent in design or testing is a day without the revenue required to fund future operations. Designing secure devices that can be adequately configured for security upon implementation requires additional resources and development time. The need for positive cash flow and revenues, combined with pressures to keep costs down, can lead to security bolted on as an afterthought rather than incorporated into the product’s design and the release of insecure devices that have not been adequately tested for proper functionality and security (Rice, 2007).

### Insufficient Device Maintenance and Replacement

The pressure to bring in new revenue also incentivizes manufacturers and developers to develop new products instead of maintaining existing products. Additionally, rapid improvements in hardware and software can quickly render existing devices obsolete. While some more prominent developers have the budget to support devices continuously, almost all manufacturers consistently design new products to replace older products. According to Failory, an organization providing information regarding startups, Startup Genome, an organization that collects and provides statistics and information about startups, and the United States Bureau of Labor, nine out of ten startups fail, with two out of ten failing in the first year of operations (Kotashev, 2022). Based on an analysis of 214 startups, 21 percent of tech startups failed because they ran out of cash due to either a lack of investment or poor use of investments (Cantamessa, Gatteschi, Perboli, & Rosano, 2018).

The constant need for innovation, investors, and revenue to survive can negatively incentivize IoT manufacturers to focus on designing new devices that bring in revenue rather than maintaining older ones that do not drive new revenue. Additionally, devices purchased from manufacturers that have gone out of business due to a lack of income or investments required to sustain operations also leave the purchasing organization without any means to maintain them. A lack of maintenance means that the amount of unresolved vulnerabilities on the organization’s network grows continuously, increasing the organization’s threat vectors and exposing the organization to more risk.

### Features Over Security

New innovative applications of IoT, particularly those enabled by 5G connectivity, have allowed businesses to capitalize on the mobile deployment of IoT to support business operations. In Geekonomics: The Real Cost of Insecure Software, David Rice suggests that organizations and users have become feature-hungry and look for benefits that offset the cost of software insecurity. As a result, Rice describes a feedback loop in which software developers are incentivized to add features to drive customer interest instead of identifying and fixing vulnerabilities before distribution. In the feature-driven business model, developers focus on adding functionality, only remediating vulnerabilities discovered by adversaries or security researchers. When customers choose software, they start with the expectation that devices are already insecure. Under this assumption, instead of looking for security, customers are driven to select products based on the value of the features a device or software provides. Since developers respond to customer and market desires, the tendency is to work on adding new features, once again leaving security to be an afterthought (Rice, 2007).

### A Lack of Standards

Before the first line of code is written, developers that set out to design and manufacture an IoT device face a significant challenge, choosing an IoT framework upon which to base their IoT device. Developers choosing an IoT framework have many options, each supporting a unique functionality and each having specific hardware and software requirements. In addition, each IoT framework supports specific application and communication protocols and provides particular security functionality. Many developers face the problem that devices are often required to operate on multiple platforms, and security functions cannot be implemented in the same manner across all platforms. For example, communication, access control, and cryptography functionality on a device using ARM’s Mbed framework use mbed TLS communication, uVisor and MPU access control, and mbed TLS/hardware cryptography, whereas an Amazon AWS IoT device uses SSL/TLS communication IAM Roles, Rules Engine, and Sandboxing access controls, and 128-bit AES cryptography (Ammara, Russello, & Crispo, 2018). Inconsistencies in IoT frameworks result in varying security across IoT devices, no universal standard for developers to use when designing IoT products, and few measures upon which customers may quickly evaluate device security during procurement.

### Implications and Societal Impact

Given the significant investment and rapid adoption of IoT devices, the security implications for organizations and critical infrastructure are severe. Our critical infrastructure and society have grown to depend on networked technology. While this technology has improved our quality of life, when organizations implement insecure devices, malicious actors, including those motivated by political and criminal factors, gain the ability to disrupt critical infrastructure, damage the economy, or cause harm to life. The potential severity of insecure IoT devices is illustrated by vulnerabilities discovered in implantable cardiac devices created by St. Judes Medical to monitor and manage patients' heart functions. These devices were found to have a vulnerability that could have allowed an attacker to access the device’s transmitter and control its functionality (Larson, 2017). If exploited by a malicious actor, this vulnerability could have resulted in severe harm or death to a patient. In addition to impacting personal health and safety, insecure IoT devices attached to critical infrastructure networks leave organizations and infrastructure at risk for service disruptions, data disclosures, financial losses, and reputational harm, potentially negatively affecting national and global economies.

## Potential solutions

Understanding the potential for damage to our way of life, organizations seeking to benefit from using IoT devices as part of their business model or operating strategy must work to reduce the threat vector and amount of exposure associated with IoT implementation. While much of the effort required to secure IoT devices depends upon the developer, some options exist for organizations and governing bodies to reduce the impact of insecure IoT devices and improve device security moving forward.

### IoT Device Management Using Software Defined Networking

One proposed solution to address the risk associated with implementing vulnerable IoT devices is using Software-Defined Networking (SDN) to manage them. Leveraging artificial intelligence, an SDN controller could identify and classify IoT devices and automatically detect vulnerabilities associated with devices connected to the network. The SDN controller would then use artificial intelligence and machine learning (AIML) to analyze each device’s vulnerability and classification and isolate insecure IoT devices from production networks using automated security rules (Iqbal, Abbas, Daneshmand, & Bangash, 2020). This solution could reduce the network attack vector associated with vulnerable IoT devices, allowing organizations to realize the device's benefit while minimizing the risk associated with its vulnerabilities. In addition, organizations could improve their awareness of IoT vulnerabilities by analyzing the classification and vulnerability information provided by the SDN solution.

### IoT Device Certification

With so many IoT devices and no clear standard, ensuring customers understand the security risks of IoT devices during procurement and incentivizing the development of more secure devices is extremely important to protect organizational networks. A possible solution to both goals is establishing an IoT device certification from a governing body that uses a standardized methodology to assess the security of each device. A device certification would enable customers to quickly evaluate device security during the procurement process and allow for informed risk-based decisions. This solution would require all devices seeking certification to undergo standardized risk assessments, vulnerability analysis, and security testing by a third party. Following evaluation, certified IoT devices would be assigned a label, and consumers would be able to access reports that provide information about the findings from the certification process (Baldini, et al., 2016). Security certification would allow consumers to quickly evaluate the device's security and the risk posed to their organization during the purchasing process. With more customers understanding the security posture of devices during the selection process, customer awareness and demand could prompt developers to incorporate security into their devices to obtain security certification, reducing the number of insecure devices rushed through the development process.

### IoT Development Standards

Another major issue with IoT devices is the lack of standards used during development and manufacturing. A potential fix is creating and adopting an international secure IoT framework. This solution would encourage IoT developers to use a single framework instead of the multiple existing standards used by different devices. An international secure IoT framework could ensure developers design and implement IoT devices that support standardized security requirements such as data encryption at rest and in transit, access control, and authentication methods (Ammara, Russello, & Crispo, 2018). In addition, a single IoT device framework could support integration with existing security technologies used by organizations to protect their networks, including the IoT SDN solution described above. An international IoT hardware and software standard would also reduce ambiguity by providing a baseline of requirements to support security-based functionality and ensure that each IoT device has the resources required to enable security features such as encryption and access control. Developers using the framework could quickly implement security features and then focus on the functionality of their devices, reducing the amount of development time and resources required to provide adequate security. By incorporating security into the development of IoT devices, organizations and critical infrastructures relying on them would be able to make security-based risk decisions and trust that the devices added to their network incorporate and support standardized security functionality.

## Conclusion

Rapid growth in IoT has the potential to drive significant innovations in business and society; however, when coupled with a lack of security during development and implementation, these innovations do not come without a cost. The security implications for organizations adopting IoT devices as part of their business strategy are substantial. When implementing IoT devices into their networks, organizations must remain cognizant of the risks and vulnerabilities associated with insecure devices and should, at a minimum, seek out devices and manufacturers with a reputation for quality security-based design and continued maintenance. Governments and industries should seek to strengthen critical infrastructure and drive changes in the IoT development market by establishing certification authorities and standardized frameworks for IoT devices, allowing informed procurement decisions, and incentivizing manufacturers to incorporate security in the design of IoT devices. As IoT becomes more ubiquitous in organizational operations, understanding and managing the threats and vulnerabilities associated with insecure IoT devices is critical. Governments and organizations must actively work on solutions that improve IoT security in all sectors and provide market incentives for IoT manufacturers to develop secure products to reduce the likelihood of realized harm.

# References

Ammara, M., Russello, G., & Crispo, B. (2018, February). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38*, 8-27. doi:doi.org/10.1016/j.jisa.2017.11.002

Baldini, G., Skarmeta, A., Fourneret, E., Neisse, R., Legeard, B., & Gall, F. L. (2016). Security certification and labeling in Internet of Things. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 627-632). Reston: IEEE. doi:10.1109/WF-IoT.2016.7845514

Bristow, M. (2021, 2021 August). *A SANS 2021 Survey: OT/ICS Cybersecurity.* Nozomi Networks.

Cantamessa, M., Gatteschi, V., Perboli, G., & Rosano, M. (2018). Startups’ Roads to Failure. *Sustainability, 10*(7), 2346-2365. doi:10.3390/su10072346

Chen, T. M., & Abu-Nimeh, S. (2011, April). Lessons from Stuxnet. *Computer, 44*(4), 91-93. Retrieved from https://ieeexplore-ieee-org.cmu.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=5742014&tag=1

Cybersecurity & Infrastructure Security Agency. (n.d.). *Critical Infrastructure Sectors*. Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/critical-infrastructure-sectors

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences, 11*(10), 4580. doi:10.3390/app11104580

Greenberg, A. (2018, August 13). *How Hacked Water Heaters Could Trigger Mass Blackouts*. Retrieved from Wired: https://www.wired.com/story/water-heaters-power-grid-hack-blackout/

Iqbal, W., Abbas, H., Daneshmand, M., & Bangash, B. R. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet of Things Journal, Vol. 7, No. 10*, pp. 10250-10276. doi:10.1109/JIOT.2020.2997651

Kotashev, K. (2022, January 9). *Startup Failure Rate: How Many Startups Fail and Why?* Retrieved from Failory: https://www.failory.com/blog/startup-failure-rate

Larson, S. (2017, January 9). *FDA confirms that St. Jude's cardiac devices can be hacked*. Retrieved from CNN Business: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/

Lueth, K. L., Wopata, M., Pasqua, E., Sinha, S., Annaswamy, S., Wegner, P., . . . Goel, A. (2021). *State of IoT – Summer 2021.* IOT Analytics.

O'Driscoll, A. (2022, January 29). *25+ cyber security vulnerability statistics and facts of 2021*. Retrieved from Comparitech: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

Rice, D. (2007). *Geekonomics: The Real Cost of Insecure Software.* Boston: Pearson Education.

Safe at Last. (2021, November 25). *80 Insightful ‘Internet of Things’ Statistics (Infographic)*. Retrieved from Safe at Last: https://safeatlast.co/blog/iot-statistics/

Wegner, P. (2022, March 30). *Global IoT market size grew 22% in 2021 — these 16 factors affect the growth trajectory to 2027*. Retrieved from IoT Analytics: https://iot-analytics.com/iot-market-size/?utm\_source=IoT+Analytics+Master+People+List&utm\_campaign=fbbb77d08b-What+CEOs+talked+about+in+Q1%2F2022+BLOG&utm\_medium=email&utm\_term=0\_3069fbcae4-fbbb77d08b-346063339

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017, October). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal, 4*(5), 1250-1258. doi:10.1109/JIOT.2017.2694844

Zetter, K. (2016, February 9). *How to Hack the Power Grid Through Home Air Conditioners*. Retrieved from Wired: https://www.wired.com/2016/02/how-to-hack-the-power-grid-through-home-air-conditioners/