Module 2 Discussion Topic: Internet of Things (IoTs) Security Challenges

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity, Professor Dr. Joseph Kovacic

September 6, 2025

Instructions:

In your opinion, what are the biggest IoT security risks and challenges? Cite resources and references that back up your assertions.

Internet of Things (IoTs) Security Challenges

The Internet of Things (IoT) is a network of physical and non-physical devices equipped with sensors and connectivity, enabling them to exchange data with other devices over the internet (Kim & Solomon, 2021). Examples of personal IoTs include home appliances (i.e., refrigerators and microwaves), home security devices (i.e., cameras and alarm systems), home maintenance devices (i.e., sprinkler systems and thermostats), personal home devices (i.e., entertainment and video game consoles, health monitoring wearable watches), and vehicles (i.e., Teslas for updating firmware). Many industries utilize IoT to run, monitor, and safeguard their organizations and businesses. Industries utilizing IoTs include operational monitoring technologies such as Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS), as well as Supply Chain and Logistics, government environmental monitoring devices, and remote patient monitoring devices used by hospitals (Polat, 2019; Fortinet, 2025). Although the expansion of IoT devices has introduced convenience into daily life, it has also created a complex landscape of security risks and challenges. In my opinion, IoTs are arguably the most reported targets of cyberattacks.

IoTs pose a significant security problem for both home and organizational networks because of weak authentication, a lack of secure update mechanisms, and the insecure nature of data transmission. First, the IoT industry lacks a unified and clear set of security standards to follow, making it difficult for developers and manufacturers to incorporate security at the start (i.e., “security by design”). Also, many developers and manufacturers prioritize convenience and accessibility over secure authorization and data integrity (Prat, 2025). Second, there are challenges related to maintenance and updates. IT administrators struggle to maintain an up-to-date inventory

of their devices, making it difficult to monitor and update them promptly with necessary firmware and security protocols.

Third, there is insecure hardware and a lack of visibility into the IoT devices. Many corporations have utilized IoTs in remote field locations for years, with some devices becoming forgotten, lost, or entirely inaccessible to humans. The devices that remain accounted for may be too complex to update, as they often lack built-in security features due to limitations in their embedded firmware or software. Additionally, shadow IoT (i.e., unsanctioned devices deployed without the express permission of IT administrators and security departments), such as extra home router installed in a company office, may cause problems because the IT team is unaware of these devices. They are unable to monitor and control the flow of traffic to them. Such vulnerabilities provide hackers unpoliced access (i.e., additional attack vectors) to critical parts of an organization's network infrastructure.

Fourth, many IT administrators do not reset and change the default login credentials during the initial installation phase. The manufacturer's default login credentials and settings are not particularly secure, which is done on purpose to make the onboarding process easier and simpler for IT professionals. If default login credentials persist, then hackers can easily scan for and infiltrate those devices, granting the hackers unauthorized access to them to conduct nefarious things like installing malware, exfiltrating internal data to be sold on the black market, or taking control over them for large-scale botnet attacks, like the Mirai botnet, to conduct massive Distributed Denial of Service (DDoS) attacks (Fortinet, 2025). Lastly, when IT administrators change these default settings, they often fail to store the new login credentials in a secure and organized environment for later use by company IT administrators.

References

Fortinet. (n.d.). ICS/SCADA security: A comprehensive guide. CyberGlossary. Retrieved September 2, 2025, from https://www.fortinet.com/resources/cyberglossary/ics-scada

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Polat, G. (2019, January 2). Security issues in IoT: Challenges and countermeasures. ISACA Journal, 1. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures

Pratt, M. K. (2025, July 2). Top 15 IoT security threats and risks to prioritize. IoT Agenda. https://www.techtarget.com/iotagenda/tip/5-IoT-security-threats-to-prioritize

SentinelOne. (2025, July 23). Top 10 IoT security risks and how to mitigate them. Cybersecurity 101. https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/