

Security Risk Analysis of the Internet of Things: An Early Cautionary Scan

Mounika Mandapuram

Cognizant Technology Solutions, Teaneck, New Jersey, USA

(mounikamandapuram09@gmail.com)

This journal is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License (CC-BY-NC).

Articles can be read and shared for noncommercial purposes under the following conditions:

- *BY: Attribution must be given to the original source (Attribution)*
- *NC: Works may not be used for commercial purposes (Noncommercial)*

This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms.

License Deed Link: <http://creativecommons.org/licenses/by-nc/4.0/>

Legal Code Link: <http://creativecommons.org/licenses/by-nc/4.0/legalcode>

ABC Research Alert uses the CC BY-NC to protect the author's work from misuse.

Abstract

The Internet of Things is assisting in developing a new and more intelligent world in which everything will fall under its purview. The issue of security is by far the most critical concern and component regarding the Internet of Things. With billions or trillions of connected devices, it will be difficult for future generations to find solutions to the security concerns we face today. The Internet of Things (IoT) paves the way for various entities and applications that benefit humanity. Although it is the most significant accomplishment of the decade, it has also given rise to catastrophic scenarios due to security concerns such as threats, vulnerabilities, and attacks on connected and interconnected devices and objects. Despite this, it is still the most significant achievement of the decade. Businesses and organizations are backing the current paradigm shift by providing financial assistance to researchers and academics. The industry expected to have the most growth over this decade is the Internet of Things, which will connect trillions of different devices. It is anticipated that IoT will alter the method by which we communicate. The Internet of Things poses many significant dangers, including physical attacks, network attacks, encryption attacks, software attacks, authorization, surveillance, identity theft, vandalism, and secure communication. The findings of this research show that none of the IoT security architectures include a security layer.

Keywords

IoT, Risk Analysis, Security Threats

INTRODUCTION

In recent years, the transmission and reception of data via diverse technologies has evolved into a calm and relaxing experience for the vast majority of the world's population. By making this contribution, it will assist in creating a security solution that will be more effective in the years to come. Because of its quick expansion and impact on people's lives due to adjustments in regime or paradigm, the Internet of Things industry is considered the most advanced emerging industry in this decade. This recognition is because the industry has brought about fundamental societal changes. In the not-too-distant future, the Internet of Things will reportedly be connected to one billion different pieces of technology, according to predictions.

Consequently, the success and upward trajectory of Internet of Things devices with a promising future are contingent on their ability to maintain their level of security. If we wish to deal with the vulnerabilities that this revolution or paradigm shift causes, we should adopt a layered architecture, such as the OSI model, to cope with the challenges that it provides. This will allow us to deal with the vulnerabilities that it creates. Additionally, the Internet of Things (IoT) is a new industry paradigm that, in addition to its estimated worth of trillions of dollars, is a new industry paradigm that promises to transform the concept of communication by enabling the connectivity of billions of devices and objects through its substantial virtual and physical infrastructure (Alberto et al., 2015). This is a new industry paradigm that, in addition to its estimated worth of trillions of dollars, is a new industry paradigm that promises to transform the communication concept. The Internet of Things is another promising paradigm since it is a new industry paradigm that can change the idea of communication through the interconnection of billions of devices and products through its enormous virtual and physical infrastructure. As a result of this potential, the Internet of Things is also a paradigm with much promise. Internet of Things (IoT)-connected devices, such as smartphones and smart grids, as well as video connectivity and video conferencing, GPS connectivity and vehicular connectivity, health monitoring devices, and other devices, are examples of how the Internet of Things (IoT) has the potential to change how people communicate with one another (Sha et al., 2016).

REVIEW OF RELATED LITERATURE

It is gaining recognition as a driver for change in business principles while transforming the modes of operation of people's lives and the channels through which they communicate. This co-occurs as it changes the channels through which people interact. Every researcher who has paid close attention to the Internet of Things has considered its layered architecture (Lin & Wu, 2013). This is an intriguing development given that the Internet of Things has emerged as the business sector expanding quickly in this decade. We will look more in-depth at the information covered in the previous section in this part of the article.

As a consequence of our research, the Internet of Things design does not have a security layer, which could prove extremely important for future generations. It is possible to classify the numerous architectural proposals presented by various researchers (Qian et al., 2016). If we do so, we will discover that these researchers proposed three levels of security (three layers, four layers, five layers, and even some illustrated six layers). However, none of these researchers included a security layer as a separate layer, which is essentially required or mandated by architectural design. Hackers can acquire or get personal information while gaining access to the device's data thanks to a built-in problem in virtually every communication device, regardless of whether it is software or hardware. This defect is present in almost all communication devices. According to Zhang and Qu (2013), the fundamentals are the same whether downloading, uploading, or installing software through a network or a service that facilitates file sharing. We have therefore concluded, with the assistance of this article and a survey of the literature, that the security layer is the essential layer in the architecture of an Internet of Things (IoT) network and that it is currently absent from the architecture of an Internet of Things (IoT) network (Mandapuram, 2016).

SKETCH OF METHODOLOGY

In this section, we define the risk assessment technique shown in Figure 1 by beginning with the standards and procedures discussed in the preceding section.

The following are the steps that make up our method:

- 1) The initial stage involves identifying the assets using the IoT domain model.
- 2) The risk assessment methods in Section II propose a shared threats database to identify asset threats in the second stage. EBIOS database, compatible with all ISO standards, provides a complete list

of information system dangers. Risk evaluation utilizes the EBIOS threats database. Some IoT risk analysis works have used it.

- 3) The third stage is to extract the security objectives from the present dangers. At this stage, we will extract relevant objectives for IoT systems from ISO, which offers a set of generic security objectives supported by a set of controls that are an essential component of information security management. In addition, ISO provides a set of security objectives that can be applied to any system.
- 4) The final step involves the construction of security requirements in order to put the security objectives into action and provide countermeasures for the dangers that have been identified.

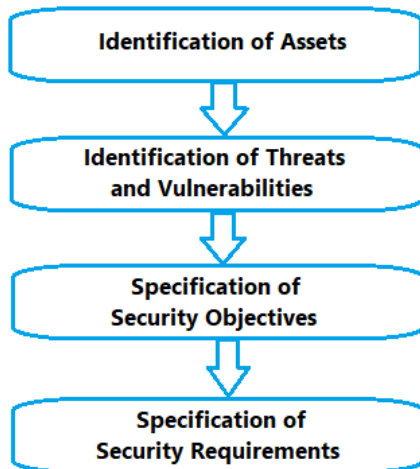


Figure 1: Risk Assessment Practice of IoT

THE CURRENT CYBERSECURITY RISK ASSESSMENT PARADIGM

Core concepts of risk assessment

Risk assessment involves recognizing, estimating, and prioritizing organizational assets and processes. Risk management relies on this to treat recognized risks. Risk acceptance, mitigation, transfer, or avoidance by eliminating the asset are choices. Risk assessment includes assets, vulnerabilities, threats, attack likelihood, impact, and cyber-harm.

Assets are something valuable to the organization. Assets might be tangible (e.g., technological infrastructure), intangible (reputation or a business process), minor components, or the system itself. Vulnerabilities are asset flaws or risk controls that can be exploited. Threats use vulnerabilities to harm assets. Such behaviors may be intentional (e.g., stealing company data) or unintentional (e.g., social engineering). Cyber risk evaluates the chance of a successful threat or attack and the potential asset damage.

Approaches to risk assessment

Cybersecurity risk assessment's core process is well-defined, but its sub-processes are flexible. This versatility has led to many risk assessment techniques, manuals, and tools. These depend on the context and the organization being assessed. The most prominent and well-regarded of these approaches are NIST SP800-30, ISO/IEC 27001, OCTAVE, CRAMM, and EBIOS, which come from standard-setting agencies (NIST and ISO/IEC) and governments (CRAMM from the UK and EBIOS from France). As a result, organizations frequently assess risk using these methods.

Instead of analyzing each risk assessment methodology individually, focus on their differences. Recent surveys show that strategy and risk measurement are the most critical components. Some risk assessment techniques focus on key assets and the harm they may suffer, while others focus on threats and

their feasibility. The NIST strategy starts with threat sources and occurrences. After that, it recommends evaluating vulnerabilities and the likelihood and impact of threat events before assessing risks.

However, other approaches like OCTAVE start with identifying critical assets and then work outwards to identify threats and their effects. This process reveals risk. The asset-oriented strategy prioritizes vital assets over ephemeral threats, while the threat-oriented approach is better suited to current threat landscapes.

Risk measurement is also disputed. Most methods use high, medium, and low qualitative measures to rate a threat's likelihood and impact. The benefit is simplicity in defining risk appetites, monitoring risks (via threat likelihood and impact ratings), and communicating risk information. The qualitative approach's subjectivity and imprecision are drawbacks. For example, one person's low threat may not be another's.

Probabilistic models are used in numerous methods to solve such challenges. These often raise new issues while addressing some. The most common is the analysis's complexity (making it error-prone and hard to communicate) and the need for more data to estimate the threat event's probability and impact accurately. These factors have limited quantitative analytic approaches, and their use in complex and highly interrelated systems is rare. Therefore, periodic evaluation methods are used because dynamic risk assessment methods are not rigorous.

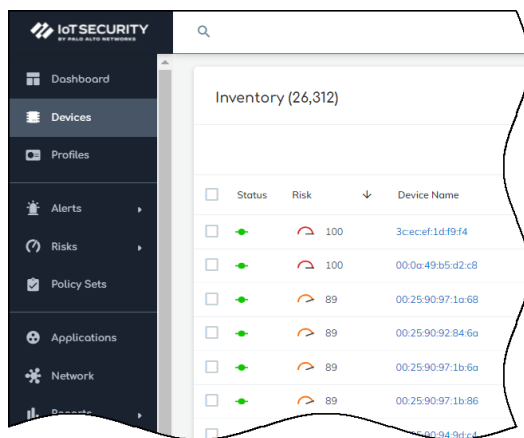
Several more elements characterize and inform risk assessment methodologies in our IoT setting. For example, surveys have shown how the methodology accounts for risk propagation or dependencies; how organizational infrastructure resources are valued and from what perspectives; and whether the approach prioritizes reducing known system risks or expanding analyses to future scenarios and postulating based on past experiences. Each has unique characteristics and uses.

IOT THREAT ANALYSIS

IoT Security performs daily calculations of risk through data collection and modeling processes and the analysis of vulnerabilities and threats. The warnings, vulnerabilities, behavioral anomalies, and threat intelligence that it identifies are the components that make up the risk scores that it generates. For example, IoT Security considers not only individual devices' scores within a given group but also the percentage of hazardous devices about the total number of devices in the group when calculating the risk scores of device profiles, sites, and organizations. This ensures that accurate results are obtained.

Device Risk

The Risk column on the Devices page gives each device's risk score. For example, IoT Security provides this information. Daily, risk scores for various gadgets are calculated by it.



The screenshot shows the IoT Security dashboard with a sidebar menu on the left containing options like Dashboard, Devices, Profiles, Alerts, Risks, Policy Sets, Applications, and Network. The main content area displays an 'Inventory (26,312)' table with columns for Status, Risk, and Device Name. The table lists several devices with their respective risk scores and MAC addresses.

Status	Risk	Device Name
🟢	100	3c2cecf.1d.f9.f4
🟢	100	00:0a:49:b5:d2:c8
🟢	89	00:25:90:97:1a:68
🟢	89	00:25:90:92:84:6a
🟢	89	00:25:90:97:1b:6a
🟢	89	00:25:90:97:1b:86
🟢	89	00:24:0d:c4

Figure 2: Device risk

The Risks section shows a graph showing how the risk score has changed over the day, week, month, year, or all to date, depending on which option we choose. The graph enables us to observe the progression of the risk score over time. For example, when we move our cursor over a marker on the line, a list of alerts that pertain to that specific point in time will appear. For example, a list of notifications will appear below the graph when we click on a marker.

Device Profile Risk

IoT Security provides device profile risk scores in the Risk column on the Profiles page. IoT Security calculates the device profile risk score from the scores of at-risk devices (40 or above) in the same profile. However, more than averaging the risk scores of all devices in the profile is required. The amount of dangerous devices in the profile affects the computation. For example, IoT Security calculates the profile risk score as 89 if five devices in a profile have risk scores of 42. The profile score is higher than predicted because all devices are in danger. Again, five devices are in the same profile. A 98-scoring device is a high risk. The remaining four devices score 30 and are at average risk. IoT Security gives their profile a 64 risk score. In such a small set, the profile score is much more affected by the one high-risk device than if more devices were used.

Site Risk

Please refer to the Risk Score column in the Sites panel on the Dashboard >> Summary for Executives.

IoT Security's algorithm to create a site's risk score is a weighted average of device profile risk ratings. The weight for each profile is determined by the number of devices included in the profile and the amount of risk associated with the profile.

THE ABSENCE OF A SAFETY LEVEL

The Internet of Things architecture has levels like perception and items. Middleware: 6lowpan, data-links; internet; adaption; transport; sensing; decision; support; action; link session; transmission; router; hub; cloud messaging; object-oriented; SOA layers; etc. None of these models separate the Internet of Things security layer. Those papers described different layer architectures and IoT risks. Those papers also described their potential solutions. However, daily risks rise alarmingly as the Internet of Things business matures. Within a decade, all devices will be online. The Internet of Things (IoT) will be attributed to modernity for redefining communication. These innovations are transforming the Internet of Things into the Internet of Everything. Beyond these realities, risks are emerging where the Internet of Things provides overwhelming intelligence to help humans with various entities and applications. Despite its superb acquisition in this decade, some persuade are provoked by devastating situations and conditions subject to security concerns such as threats, vulnerabilities, and attacks in the Internet of Things with its connected and interconnected devices and objects, despite all accomplishments.

Physical assaults, network assaults, encryption attacks, software attacks, authorization, surveillance, identity theft, vandalism, and secure communication are some threats to the Internet of Things. Internet of Things security architecture is the biggest issue. Active or passive hackers get access to a system or network. Active attackers seek system or network access. The system's morphing behavior alerts victims to active attacks, which are usually violent. Many are harmful, deleting memory or files, locking users out, or forcing access to a targeted network or system. Active attackers usually do not care about being caught since the damage is done by the time they are caught. Passive attacks avoid notice by using non-disruptive methods. Passive assaults aim to access a user's system or network and steal data without being discovered. Targeted data collection—including debit and credit card payment information, user identifying information, and legitimate access to protected data—causes many security breaches and data hacking events.

The attacker/hacker steals data, reconfigures the system, and acquires sensitive information. These factors make security infrastructure standardization harder. Hydra, Runes, the IoT Alliance, the E Japan

Strategy, I-Core, Sensei, IoT-6, IoTivity, and AllJoyn are working to solve these problems. Fp7, horizon2020, one M2M platform, 4ward&sail, Fire++, Find, FIA, GENI, and others are underway. Data collection by proliferation devices like smartphones, tablets, and laptops, which contain personal information like a credit cards, debit cards, bank accounts, passwords, email accounts, business history and information about the company's office and contacts, controlled vehicle information, and others, has increased dramatically in recent years. These devices are vulnerable to user error and easily accessible, hacked, and stolen by hackers. Threats have targeted 80% of organizations, according to surveys. Internal and external risks exist. Web interfaces, authentications, insecure networks, transport encryption, cloud interfaces, mobile interfaces, security configurations, firmware security, physical security, and other variables cause the most dangers. Internal threats make up 60% of hazards, and external threats 40%.

Internal and external threats exist. Most threats are internal. Weak attacks target unclassified data, weak passwords, and less sensitive information while monitoring system vulnerabilities. Thus, they occur daily. Moderate dangers are more likely without classified data monitoring. Systems transfer a lot of sensitive data through networks with standardized user interfaces. These events usually occur weekly or monthly.

Access to confidential and classified data and private/regulated data sources are high-risk due to data transfer security issues. These attacks occur annually or every five years on isolated systems. These attacks are rare. The four main types of attacks are physical, software, encryption, and network. Nearby physical assault. Network assaults are used to influence or damage the Internet of Things network, hack passwords and data, and steal information. Software attacks occur when system weaknesses allow hackers to enter and do damage. Encryption attacks usually break encryption. Sensors attack nodes and gateways. The four most frequent assaults have subclasses that can bring down an IoT network. The following assaults could cause network disasters.

While protecting, security and privacy must be considered. The Internet of Things has three trust management-related privacy issues. First, discuss data privacy and vulnerabilities. Since the Internet of Things (IoT) will be a trillion-dollar industry with billions of customers and more than half the world dependent on it, consumer and customer privacy must be protected. Wireless communications must address big data, data processing and management, efficient battery management systems, communication infrastructure, technology infrastructure, standards immaturity, procuring, privacy breaches, and security risks. Thus, internet of Things privacy and security issues are most pressing. Integrity, secrecy, authentication, data management, and interoperability must be set to ensure safe and dependable communication.

Most assaults today target the Internet of Things network, software, and encryptions. Since the Internet of Things will eventually include the security layer, there should be a standard model or frame of the reference model to secure data and liabilities. Attacks will skyrocket as the Internet of Things matures. Thus, adding security requires a frame of reference model. In technology, great opportunities come with significant responsibilities. For example, the Internet of Things is creating unprecedented security issues like data security, network security, operating system security, server security, device/physical security, secure devices; authorization and authentication; device updates management; data confirmation; communication security; data privacy; data integrity; high availability; data transmission safety; and utmost software security.

CONCLUSION

It is imperative that the security layer be incorporated into this architecture and that it be treated as a distinct layer from the other ones. This study takes a look at research, scholarship, and scientific work that has been previously published. While those works give three, four, five, and six layers of IoT-layered architecture, the security layer is more independent than the previously published work. They did a fantastic job protecting the Internet of Things but did not include an independent security layer

that could have made these models even more secure over time. Because the security layer can operate more effectively and achieve more significant results on its own, it can be utilized to provide improved security and secure communication. In the not-too-distant future, there will be a significant growth in the number of connected devices due to the development of IoTs. Consequently, the number of dangers or assaults will significantly increase.

As a consequence of this, additional work needs to be done in order to build a global standard architecture model for IoTs. Particular attention must be devoted to incorporating security layers as independent layers, an essential component of such an architectural model. Consequently, it will be very challenging to exercise control over the potential security concerns posed by IoTs.

REFERENCES

- Alberto M. C. Souza, José R. A. Amazonas, An Outlier Detect Algorithm using Big Data Processing and Internet of Things Architecture, *Procedia Computer Science*, Volume 52, 2015.
- Lin, C., G. Wu, Enhancing the attacking efficiency of the node capture attack in win: a matrix approach, *J. Supercomput.* 66 (2) (2013) 989–1007.
- Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement*, 7(1), 50–57. Retrieved from <https://4ajournal.com/article/view/76>
- Qian, J., H. Xu and P. Li, "A Novel Secure Architecture for the Internet of Things," 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), Ostrawva, 2016, pp. 398–401. doi: 10.1109/INCoS.2016.36.
- Sha, K., W. Wei, A. Yang, W. Shi, Security in the Internet of Things: Opportunities and challenges, in *Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016)*, 2016.
- Singh, D., G. Tripathi and A. Jara, "Secure layers-based architecture for the Internet of Things," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, pp. 321–326. doi 10.1109/WF-IoT.2015.7389074.
- Vashi, S., J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), Palladam, 2017, pp. 492–496. doi 10.1109/I-SMAC.2017.8058399.
- Zhang, W., Qu, B. "Security Architecture of the Internet of Things Oriented to Perceptual Layer," *International Journal on Computer Consumer and Control (IJ3C)*, vol. 2, no. 2, 2013.