INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES (IJNAS), VOL. 12, Special Edition (2019); P. 74 – 78, 5 FIGS.

Solving the Disconnect – Conceptualisation of a Unified Security Framework for the Next Generation IoT Platforms

A. E. Ibor[1]*, A. O. Otiko[2] and O. I. Ofem[1]

ABSTRACT

The gradual expansion and adoption of the Internet of Things (IoTs) platforms has come with a lot of enhancements in the way we live, work and transact business. This improvement in every aspect of our lives creates new environments that come with new applications and services to enhance device to machine interactions. As more devices and machines are connected to each other, there is the likelihood of the applications and services that run on them to be vulnerable to exploitation and targeted attacks. Where vulnerabilities are easily identified and exploited by malicious users, the extent and cost of attacks can completely overrun the entire IoT platforms leading to a possible device crisis. To think out a solution in this direction requires a unified security framework that will serve as a backbone for all IoT-enabled devices and machines. The security backbone will be useful for protecting all IoT-based platforms with their respective device IDs, applications, and services. The proposed framework will implement a hierarchical security architecture that assigns security functions to devices and machines at different levels of abstraction and largely based on the level of protection required with respect to the requests initiated by the device. In the instance of an identified vulnerability, the device running the vulnerable application or service can quickly trigger a patch alert that allows the unified framework to broadcast this message to the relevant vendor(s) to fix the identified flaw(s).

INTRODUCTION

The Internet of Things (IoT) is a seamless and strong interconnection of devices, machines, people, services and physical objects that can interact and exchange information about themselves and their environment. According to Babar et al., (2011), IoT promises to deliver a digital environment with the possibilities of merging the power of high calibre proximity and physical objects such as sensors and actuators. Similarly, Kouicem et al., (2018), posits that the integration of the digital and physical worlds is likely to trigger an intelligent era of Internet that has the potential of offering huge business values for organisations and opportunities for energy, transportation, healthcare, education, commerce, and other sectors.

As the disruption in IoT technology becomes pervasive, new security challenges and concerns are likely to emerge. With IoT having tremendous impact on the way we live, make decisions and transact business, possible vulnerabilities in the technology including the devices that interact and exchange information, will have very drastic consequences on the overall architecture of the Internet through which these devices interact. IoT sensors collect a lot of privately owned data and the devices in which these sensors are embedded are mostly linked to the lives of people.

In the event of an attack, it may be increasingly difficult to truncate or mitigate it; a situation that can trigger a device apocalypse and extended risks to human lives. IoT devices are basically resource-constrained, and as such extant security architecture may not be tenable in protecting them against targeted exploits.

Issues arising from confidentiality, integrity, privacy of users' data and policy considerations must be properly managed through an entire reengineering of extant security architectures, which are predominantly vulnerable to attacks. Traditional approaches, which are already failing in the conventional Internet and its related domains must be properly tuned to recognise the specificities of IoT-related implementations. To this end, this paper will discuss the various security concerns of current IoT technologies and attempt to suggest a possible solution through a unified security framework for the future.

Review of Related Literature

Babar et al., (2010) and Babar et al., (2011) proposed an embedded security framework for IoT. The paper highlights the various attacks on IoT systems including physical, side channel, cryptanalysis, software, and network attacks. The authors went further to discuss the strategies for achieving an in-built security for IoT devices. Similarly, Sadeghi et al., (2015) mentioned the emerging challenges of industrial IoT.

*Corresponding author. Email: *ayei.ibor@gmail.com, foladeji@unilag.edu.ng,*
[1]Department of Computer Science, University of Calabar, Calabar, Nigeria
[2]Department of Computer Sciences, Cross River University of Technology, Nigeria

The authors posit that the proliferation of IoT systems permit devices to generate, process, and transmit huge amounts of classified and safe-critical data. This data also includes privacy-sensitive information, which can be targets for attacks. The paper suggests the need for a holistic security framework for IoT systems and considered the components of this framework to include security architecture, integrity verification, and secure IoT device management.

Heer et al., (2011) discussed the limitations of existing Internet protocols and security architectures when applied to IoT. An overview of the deployment model for IoT is given with the lifecycle of devices and architectural considerations. In addition, the authors identified the challenges of current IP-based IoT systems and suggested that there is the need to proffer a security architecture that will fit into the lifecycle of devices and their capabilities. Some of the considerations for the required security architecture include the creation of the security domain, the relevance of a trusted-third party, or the protocols used. In Kumar and Patel (2014), the numerous concerns of IoT systems are described. Unauthorised access, denial of service, viruses or malware attacks, as well as privacy violations are some of these security concerns that necessitate a unified security framework.

Furthermore, Suo et al., (2012) and Jing et al., (2014) claimed that the extant security concerns of the conventional Internet are transferable to IoT systems since the IoT is built on the basis of the Internet. While Suo et al., (2012) discussed the security of IoT based on four layers viz-a-viz application, support, network and perceptual layers, Jing et al., (2014) identified three layers of the IoT, which are perception, transportation, and application layers. In each of these layers, a plethora of security issues were identified in their work. For instance, at the application layer, the authors identified security-related issues in intelligent logistics, smart homes, intelligent traffic, smart grid and many more. In the same sense, ad hoc security, 3G security, WiFi security and local area network security were indicated as concerns at the transportation layer. Radio Frequency Identification (RFID) security, Wireless Sensor Network (WSN) security, and Geographic Positioning System (GPS) security were also mentioned at the perception layer.

Leo et al., (2014) proposed a federated architecture for IoT security. The approach leveraged the dynamic detection, prevention and isolation of attacks using countermeasures such as authority delegated mechanism, identify-based capability and dynamic context information. According to Granjal et al., (2015), Sicari et al., (2015), and Conti et al., (2018), the pervasiveness, connectivity, and smart interaction of nodes in IoT has made it an ideal target for cyberattacks. IoT nodes typically collect, process, and transit private information. This private information has become the baseline for exploitation by malicious users, thus leading to the escalation of attack surfaces on IoT platforms. Sicari et al., (2015) further emphasised that applying traditional security countermeasures to IoT technologies is a mismatch due to its diverse standards and communication stacks. This diversity in standards and communication stacks must be unified to achieve an efficient security standpoint for future IoT platforms.

However, these researches did not address the issue of unifying the disparate architectures of different vendors of IoT platforms to allow for a seamless collaboration of devices to identity and flag vulnerabilities and possible attacks. Therefore, this research proposes a unified security framework that considers the different levels of protection for IoT devices suitable for the next generation IoT platforms.

RESULTS

An Overview of IoT Security Issues

Security concerns for IoT are increasing as more devices interact and exchange private data over the Internet. The data collected by IoT device sensors is so enormous that malicious users are finding it easy to quickly infer the attributes of users from big data to escalate attacks. Most extant security approaches are resource-intensive with attendant computational complexity while IoT embedded devices, on the other hand, require low power consumption. The disparity in the usage and implementation of secure algorithms and IoT-enabled platforms is a huge gap in enhancing the security of IoT devices. As studied by Mineraud et al., (2016), IoT platforms largely depend on the architecture of the traditional Internet to deliver services to users. In Figure 1, it can be clearly seen that the conventional Internet provides the backbone for the seamless connection of devices, machines, people and things in IoT.

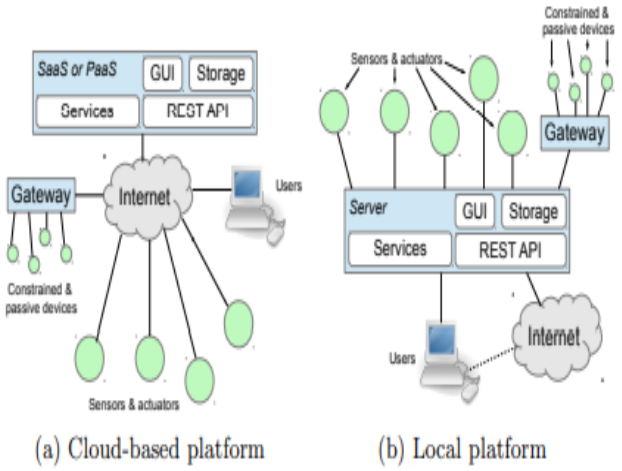

Fig. 1. a) Cloud-based and b) Local IoT Platforms (Mineraud et al., 2016).

With new applications and services, new security challenges are becoming prevalent, arising from new vulnerabilities and exploits, most of which do not have immediate mitigation strategies. The major elements of an IoT device (sensors and actuators), which collect, process, and transmit information are also dependent on the availability and reliability of Internet connection. An IoT application, for instance, will have components such as sensors, actuators, gateway, device, and the web. Mazhelis and Tyrväinen, (2014) demonstrated the linkage between these components using Figure 2.

Fig. 2. The Components of an IoT Application (Mazhelis and Tyrväinen, 2014).

From Figure 2, the web component, which defines the cyberspace, is already inundated with various attack vectors, thus giving rise to exploitations at different stages of an IoT system. Furthermore, most of the major players in an IoT ecosystem are only interested in applications and services that can work quickly for users without recourse to the security implications of such components. As illustrated in Figure 3, Al-Fuqaha et al., (2015), defined IoT as a combination of five elements. These elements include identification, sensing, communication, computation, services and semantics. All these elements have been studied to demonstrate one security flaw or the other in the literature.

Fig. 3. Elements of IoT (Al-Fuqaha et al., 2015).

Consequently, it is pertinent to have a critical assessment of extant technologies in the IoT ecosystem to proffer an inclusive security framework that can be relevant for the current attack surfaces. Identifying the attacks on IoT may not be enough until a workable security architecture becomes available. As new exploits are targeted at IoT devices, there are possibilities of a device apocalypse in the near future. If about two-third of IoT devices are compromised through any process, several human lives will be affected since most of these devices have embedded components, which interact directly with physiology of the human body.

Unified Security Framework

We attempted to address the security flaws of the current IoT ecosystem by looking at the security concerns of its various layers. We aligned our thoughts with the five layer IoT architecture proposed by Al-Fuqaha et al., (2015). This architecture is given in Figure 4. In the architecture, we have the business layer, application layer, service management, object abstraction, and objects. Each of these layers can be susceptible to several vulnerabilities. To this effect, we proposed the layered framework of Figure 5. This framework allows security at different stages of the IoT ecosystem and provides the possibility of isolating any layer that is targeted for attacks without completely compromising the entire IoT ecosystem.

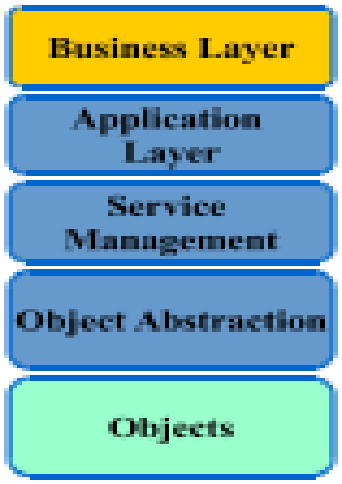

Fig. 4. 5-Layer IoT Architecture (Al-Fuqaha et al., 2015).

As depicted in Figure 5, IoT security should begin with policies and procedures, which are tenable within the IoT ecosystem, and not only relying on conventional internet policies. Subsequently, physical security of IoT devices and security at the network layer should be effectively structured. Attribute and identity-based encryption schemes will be useful at the network layer. Furthermore, the security of Wireless LANs and WSNs, IoT platforms, applications, and users should be hardened using various approaches such as public key solutions, symmetric key solutions, data tagging and obfuscation, zero knowledge proof, deep learning, and blockchain technology.

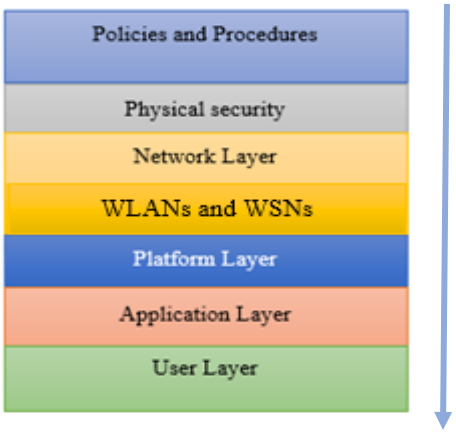

Fig. 5. Proposed Unified Security Framework for IoT.

At the topmost level, we have policies and procedures that also include government legislation, collaboration between different vendors for the initiaton and endorsement of security policies for IoT devices, and the publication of vulnerabilities of IoT devices and platforms to help vendors quickly find a fix to stem a possible attack. These policies and procedures should then apply to the control and use of the physical IoT devices incluuding hardcoded authentication modules for access to IoT devices.

Security at the network layer is essential for truncating attacks targeted at IoT software and hardwarre components. At the point of message passing, informtion exchange or data extraction, every communication protocol that is used within an IoT ecosystem should have hardened security configurations that cannot be easily compromised. This should be complemented by the security of WLANs and WSNs, which are mostly used to enable communication on-the-fly for IoT devices. At this stage, encryption schemes, netwoork access protocols, time-based passwords and tokens, and Media Access Control (MAC) filtering can be applied to protect IoT devices.

Platform, application, and user layers can be configured with antivirus and antispyware software, end-to-end encryption, patch management plans, one time pads (OTPs) for the authenticaton of devices, hardware tokens, vulnerability identification modules, and patch broadcast triggers. Furthermore, identity management schemes, web service security, and application proxies can be deployed to realise a unified security framework that is suitable for the evolving IoT ecosystem.

As depicted in Figure 5, the framework configures into each layer, the requiered security functions for protecting devices. In this sense, each device ID is connected to other devices IDs such that a vulnerable device can trigger a patch, and when compromised, its ID is broadcast across the network. This broadcast will allow other devices to reject messages from such a device. In the event of a device triggering a patch alert, the network communicates this message to the respective vendors to quickly fix the patch over the broadcasting network. Compromised devices can also be isolated at this stage until the vulberability is fixed, at which point all other devices will be notified to enhance smooth data tranmission and message passing.

CONCLUSION

Several security breaches and targeted attacks at IoT devices are becoming prevalent. The IoT ecosystem is already populated with a swarm of devices, which collect, process, and transmit sensitive information using the Internet as the backbone. As attendant

security flaws on the Internet are migrating to IoT systems, the need arises for an effective security framework that will enhance the overall security structure of the IoT.

To address this concern, this paper highlights the security issues of current IoT implementations, and attempts to proffer a solution using a unified security framework. The proposed framework can be implemented using 7 layers, such that the compromise of one layer does not completely lead to the compromise of the entire IoT ecosystem. We posit that it is possible to isolate one layer while still maintaining the functionality of other layers. In this way, when devices are compromised at a certain stage of the IoT system, other devices can be allowed to communicate by sending messages to each other and rejecting messages from the compromised devices. This process will continue until the vulnerable device is fixed, and normal communication resumes.

REFERENCES

Mineraud, J., Mazhelis, O., Su, X., and Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications*, *89*, 5-16.

Mazhelis, O. and Tyrväinen, P. (2014, March). A framework for evaluating Internet-of-Things platforms: Application provider viewpoint. In *WF-IoT* (pp. 147-152).

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

Suo, H., Wan, J., Zou, C and Liu, J. (2012). Security in the internet of things: a review. In *2012 international conference on computer science and electronics engineering* IEEE. 3: 648-651).

Sicari, S., Rizzardi, A., Grieco, L. A and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, 146-164.

Kumar, J. S and Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, *90*(11).

Sadeghi, A. R., Wachsmann, C and Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). IEEE.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S and Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, *61*(3), 527-542.

Babar, S., Mahalle, P., Stango, A., Prasad, N and Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications*: 420-429). Springer, Berlin, Heidelberg.

Babar, S., Stango, A., Prasad, N., Sen, J and Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)* :1-5. IEEE.

Leo, M., Battisti, F., Carli, M and Neri, A. (2014). A federated architecture approach for Internet of Things security. In *2014 Euro Med Telco Conference (EMTC)* :1-5. IEEE.

Kouicem, D. E., Bouabdallah, A and Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.