INTERNET OF THINGS (IOT) AND THE FUTURE OF THE DIGITAL SPACE: A REVIEW OF THE SECURITY IMPLICATIONS

Fidelis ObukohwoAghware
Computer Science Department
University of Delta, Agbor

Abstract
This review investigates whether the current approaches to Internet of Things(IoT)security prioritize transparent security over security by obscurity, focusing on four key IoT domains: hardware, data, communication, and applications. The findings reveal that security by obscurity remains prevalent, with real-time security assessments indicating a lack of robust cryptographic solutions. As IoT brings traditionally isolated systems into an interconnected digital space, it introduces new vulnerabilities, especially since many IoT devices lack the processing power for advanced security features and may be deployed in critical infrastructures. The remote accessibility of IoT devices heightens the risk, exemplified by the 2016 Mirai botnet attack, while privacy concerns grow with the integration of IoT in home smart devices

Keywords: IoT Security, Security by Obscurity, Cybersecurity Transparency, Cryptographic solutions, Vulnerability in IoT Devices

Introduction

Large numbers of recent studies are used. Security in future IoT is collective intelligence and/or digital connected devices and touches the chasm of the art of interconnected security. In an era of IoT, digital intelligence (software code drained with digital brain performs the specific action via a digital space) becomes the trigger that instructs the chip to do sensitive functions.

The future of research involves performing security risks, challenges, and security mechanisms that create IoT and the digital ecosystem. Unlike the conventional study, this survey touches the digital parcel, security concerns in real time, and mouth-watering (digital packet) sniffer-friendly handlers.

The concept of the Internet of Things (IoT) is rapidly evolving, and it will soon be a commonplace feature of the coming digital space. Later, a transformation from analogue to digital world and human intelligence is transferred to digital chips, and now all the processes are governed and controlled in the digital space. There are 40 billion electronic machines that will be connected in the form of cameras, drones, sensors, thermostats, and many automation systems which will be controlled via mobile apps, and the conventional device is modernized.

The biggest challenge and threat to this modernized world is security. "By the year 2023, more than 25% of identified enterprise attacks will involve the IoT, although IoT will account for only 10% of IT security budgets." Every evolution is screen played in terms of what is innovative and future challenges and gaps due to the society's limitation.

Objectives

To achieve this, three steps are needed. First, an understanding of the IoT is necessary, not from a technical perspective but to understand the landscape in which open data and IoT may meet. Second, to consider the case of smart cities in detail. Third, to investigate cyber security attacks in the IoT (project the Mirai attack) and the NIS directive. These actions enable the darker potential of open data-integrated IoT to be flagged. Networking smart cities with open data may be useful, but has major side effects around security. This report may contribute to the various communities around it. We also notice that this work may contribute to the ongoing investigation of the National Cyber Center on the security of smart cities. The study is policy driven and does not add much in terms of new technologies or algorithms.

This paper reviews the opportunities in the digital space of the merging of the two trends of recent times, the Internet of Things (IoT) and the increasing use of open data, and possible implications for security. There are four policy-related drivers: the boost of the GDPR and the NIS directives, the growing attention to the security of IoT devices, the call to change frameworks following the cyber incidents (the Mirai attack), the role of game-changing artificial intelligence (AI) in the creation of artificial social networks (bots), and the growing attention to security in the cloud and industrial IoT. These issues lead to questions that this report will investigate. First, we want to understand to what extent increasing integration with digital networks is driving the IoT, especially in smart cities.

Research Gaps and Literature Reviews

Agricultural and rural communities associated with the Internet have also gained some attention. Traditional producers and consumers, aided by the IoT system, can actively or instantly purchase or sell their agricultural products. It may sound nice, but this vital condition also needs to be easy. An ecosystem for the Internet of Things demands the same quantity of protection required for another novel network framework. Some IoT versions, like sensors and small systems, are almost hard for this security. Furthermore, these sensors may have less memory, CPU, duress safety limbs, backbones, and battery power. These digital artifacts' slim size of operating conditions also limits the extent and implementation of typical digital artifacts' structural security methods and treatments. Even in the last rewrite IOT conference 2010, however, these techniques do not appear to be studied. Having focused on this bridge, this book extends and conducts defense and security measurements in a natural ecosystem.

Despite some good and significant work done in the cyber science field, the formal acceptance of a book chapter has many research gaps as it sets the ground for further investigation and development of a study. Only a few studies have looked at IoT security in the digital space. In the future, a researcher needs to extend work on these IoT security implications. The idea of harm, loss, and the appropriateness of different security measures should also be commented upon and examined. Some business strategies, technical development, and regulatory initiatives allow the public to participate in proving digital devices and digital assets are worthy. Furthermore, the analyst is conducting extensive research to examine the surroundings in the future. Most key companies and groups now attempt to evaluate the advantages and risks of IoT and how they impact the Internet, digital systems, consumers, service providers, and network infrastructure.

Materials and Method

The members of the Internet of Things (IoT) access forms of transportation to access resources over a network. The composition of the two separate terms of IoT in the emerging spectrum has an association to chemistry and physics. All the items/resources have the responsibilities of collaborating with one another, communicating with humans, and interacting with the outside world.

In the collaboration of human and smart thing component, it interacts with intelligent things and collaborates with the things. The intelligent things have become an unprecedented integral part of the digital environment. The access to everything has created new lifestyles that are deeply eye-catching. It dispatches the daily traditional existing things connected with a digital environment. It gives a basic explanation of the cyber-physical systems. It can systematically conduct many different tasks such as human life entertaining tasks, medical tasks, security tasks, system maintenance, and creating knowledge.

Materials and Methods: Retaliatory attacks on servers to turn them into bots are usually performed using a botmaster-server communication.

Consequently, many of the botmasters that performed those DDoS attacks are not only still at large, but they have noticed the use of digital graffiti to mark servers and other systems as their own. We employ the common key for which the

first 800,000 of such fingerprints were derived (i.e. from Tim Bogut's digital graffiti). Many of the tools used to derive unique systems were previously developed and have been available over the years.

Results and Discussions

The discussion of the results is initially presented in the light of the stages proposed for the protocol development process. Each step is now examined in more detail to highlight the respective vulnerabilities. In doing so, the explanation is divided into layers of the communication protocol of interest and data types seen through this network communication. Both basic communication attacks, which rely on network traffic, and exploitation of vulnerabilities are concerned - which depends on such input for actual attacks. The sequence control of AT commands and the actual part of the I2C communication, in turn, do not exhibit the phased vulnerabilities but are natural features of the respective protocols. What can be stated, however, is that each layer of the communication protocol is under attack. The cause of the attacks varies: from operating system update protocols to using protocol commands, from transferring data between various memory types to improper functioning of the processing. If it is possible to overload the I2C communication using commands and substitute the hardware components, data will be transferred from a controlled application to a controlled memory and these parts of memory can be stopped. If the stoppage occurs between the layers of the personas communication protocol, any further persona change will be impossible, which is in line with the later observations. Finally, at the software level, the FDC vulnerabilities can be noted, resulting from characters creating a barrier in communication of AT commands, which cause the device to freeze. All of these (observed) attacks seem possible to be executed in the real world, which at some points will be outlined in designated subsections. The discussion will thus refer to the traded data displayed in Table, which at this moment will provide a brief preview of the traffic of both persona A and persona B. It is now generally assumed that only persona A is connected to personally. All these data are FTP server communication. After replacing persona A with persona B device can gather data of the attack executed. In some cases, the left side of the table presents the addresses of the used ports.

Conclusion and Contributions to Knowledge

The work has also highlighted a resource dependence and regulatory environmental dimension critical to IoT in the work of Ransbothan and Frey related to the next wave of the Internet revolution. As we have shown in emerging technologies, IoT is also developing in a world with significant cyber threats, and it is also clear that the assumptions underlying much of the work in this field are based on the assumption of low-level conflict/threat. In short, the conclusions from the literature review are that the security implications of IoT have yet to be thought through in a way that addresses this. The research has contributed to a consolidation of the state of the art of our understanding, advancing knowledge, and has provided an integrative framework to guide future research. Furthermore, the research has made a series of normative recommendations to guide policy.

Arising from the analysis of relevant literature, it is clear that while practitioners have taken a keen interest in the security implications of IoT, such work has not been well integrated with theoretical thinking in this area, especially in the fields of strategy and security. The result has been articles describing how IoT will transform the world and, in the next breath, warning about the lack of security that can be found in IoT systems. There have also been numerous calls for greater integration between design and security-related processes such as risk management (or governance). That being said, the importance of examining the relationship between the potential for new approaches and practices of security will necessarily be found in new manifestations of IoT. In this way, drivers for development of IoT require greater attention.

Summary

This study aimed to discover a link between the security implications of IoT on a digital space with applications in various fields. A complete delving into the facets of IoT, heterogeneity,

industry 4.0 hindrances, POS malware, ransomware, social networks, SIP and VPN attacks, USB and security tools, SSL/TLS and prototyping, cloud computing, malware trends, Dosed applications of Android and mobile phone. The results from a review essentially confirm that flaws in IoT systems can unlock security threats that can have significant implications for the digital space. As a contributing factor in the rise of patterns in security threats, IoT has become a key member. The need for an improved strategy and a coordinated approach to cope with vulnerabilities that IoT perpetuates. It is essentially in the findings that ties between applications that have a direct effect on the digital space.

The ability to connect, share, and process information has transgressed physical boundaries, creating a parallel digital space through the phenomenon of the Internet of Things (IoT). This phenomenon has become the consolidator of smart technology, interconnected and interdependent. The digital space is an unpredictable web of connectivity and relationships that can reveal new threats in unexpected ways, all thanks to the multidimensionality and diversity at its core. It is predicted that digitally everything under the sun will be connected to the digital ecosystem – nearly 50 billion things form the core environment of the IoT ecosystem. It can be observed that with IoT, health, industry, agriculture, logistics, and most importantly, critical physical infrastructures are linked, making cybersecurity vital for market stability, operation, and protection of livelihoods.

References

Abushark YB, Sarker IH , Khan AI, Alsolami F, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," Mobile Networks and Applications, vol. 2023, Springer, 2023. preprints.org

Aghware F. O, Okpor M. D., , Akazue M. I, Ojugo A.A, Emordi F.U, Odiakaose C.C., Ako R E, Geteloma V. O.,. Binitie A. P, and Ejeh P. O. (2024) "Comparative Data Resample to Predict Subscription Services Attrition Using Tree-based Ensembles," Journal of Fuzzy Systems and Control, vol. x, no. x,

Aghware F. O., Ojugo A.A., Adigwe W, Odiakaose C.C.,Ojei E.O, Ashioba N. C., Okpor

M. D., and Geteloma V.O, (2024)"Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection," *Journal of Computing Theories and Applications*, vol. 2, no. 2, 2024. DOI: 10.62411/jcta.10323.

Aghware F.O, Yoro R.E, Akazue M.I., Ibor A.E, and Ojugo A. A,(2023) "Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian," *International Journal of Electrical and Computer Engineering (IJECE)*. 13(2) 1943-1953,

Aghware F. O., Yoro R.E, Ejeh P.O, Odiakaose C.C., Emordi FU, and Ojugo A(2022), "Sentiment analysis in detecting sophistication and degradation cues in malicious web-contents: a myth or reality?" Kongzhi Yu Juece/Control and Decisions. 38 (1), 635-665.

Ali M. Laghari AA, Wu K, Laghari RA, "A review and state of art of Internet of Things

(IoT)," Journal of Computational Methods in Sciences and Engineering, vol. 2021, Springer, 2021. researchgate.net

Goel S and Nussbaum B, (2021) "Attribution across cyber attack types: network intrusions and information operations," in IEEE, *Open Journal of the Communications Society*, 2021. ieee.org

Hossein Motlagh. N, Mohammadrezaei M., Hunt, J.(2020)"Internet of Things (IoT) and the energy sector," Energies. mdpi.com

Vermesan O, Friess P, Guillemin P, "Internet of things strategic research roadmap," Internet of Things ..., 2022. unit.noieee.org

Wang B, Zheng P, Yin Y, Shih A, and Wang L, "Toward human-centric smart manufacturing: A human-cyber-physical systems (HCPS) perspective," *Journal of Manufacturing,* vol. 2022, Elsevier. parkjonghyuk.net

Yoro R. E, Aghware FO, Malasowe B.O, Nwankwo O, and Ojugo A.A(2023) "Assessing contributor features to phishing susceptibility amongst students of Petroleum Resources Varsity in Nigeria," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, (2)1922-1931.