An Impact Review on Internet of Things Attacks

Attlee M. Gamundani
Computer Science Department: School of Computing & Informatics
Polytechnic of Namibia
Windhoek, Namibia
E-mail: agamundani@polytechnic.edu.na

***Abstract*—The heterogeneity of devices that can seamlessly connect to each other and be attached to human beings has given birth to a new computing epitome referred to as the Internet of Things. The connectivity and scalability of such technological waves could be harnessed to improve service delivery in many application areas as revealed by recent studies on the Internet of Things' interoperability. However, for the envisaged benefits to be yielded from Internet of Things there are many security issues to be addressed, which range from application environments security concerns, connection technology inbuilt security issues, scalability and manageability issues. Given the increasing number of objects or "things" that can connect to each other unsupervised, the complexity of such a network is presenting a great concern both for the future internet's security and reliable operation. The focus of this paper was to review the impact of some of the attacks attributable to internet of things. A desktop review of work done under this area, using the qualitative methodology was employed. This research may contribute towards a roadmap for security design and future research on internet of things scalability. The deployment of future applications around Internet of Things may receive valuable insight as the nature of attacks and their perceived impacts will be unveiled and possible solutions could be developed around them.**

***Index Terms*—Attacks, Denial of Service, Internet of Things, Man in the middle, Replay, Security**

I. INTRODUCTION

One of the evolving technologies is the Internet of Things (IoT). Despite the various definitions available, the common understanding on IoT revolves around the interconnection capabilities among things, objects and people. As supported by [1] that we are moving towards internet of things as device to device communication takes the toll of connectivity to date. Such a heterogeneous network environment is enabled by various connection technologies and protocols available such as RFID, WIFI and Wireless Sensor Networks [1].

An overview of the field of Internet of Things(IoT) will highlight the potential network capabilities and likely fears of such an elastic technology. The envisaged future capabilities of IoT are feared to be under threat of the emerging security concerns since their deployment. Security concerns include Denial of Service (DoS), Replay, Man in the middle attacks and many common attacks to networked environments [2]. If such security concerns are not addressed to acceptable levels, an out of hand security grip on the technology is feared.

The potential market for the IoT applications will suffer grossly if the security concerns are not solved[6]. As espoused by [6], security is one of the major issues which reduce the growth of applications such as IoT. As [6] rightly put it across, "complications with data privacy and data protection continue to plague the market". This affirms the fear of the magnitude, the security threats are likely to be extending to IoT as they propagate to enormous levels across application environments.The need to affirm that solutions are being worked on and will address the perceived threats and attacks is critically important, as service delivery may be halted, yet certain application environments cannot compromise (even to a lesser extent) on safety, like life saver machines in the health sector, such real-time systems have strict compliance requirements, hence their security is of paramount importance.

The projections to 2024 on the number of gadgets per user averaging six (6) or more are quite alarming[1]. This raises great security concerns on privacy and accountability, leaving unanswered questions on whether it will be possible to specifically attribute a particular gadget to a particular individual. This points to yet another critical issue of identity management, which can help localise the threats instead of a plane approach to try and combat any identifiable threat.

The anticipated results from this research points to further research on possible solutions that could be proposed towards alleviating the security challenges, discussed herein.

This paper in organised as follows: Section II outlines the research methodology employed. Section III gives an overview of Internet of things, with a brief explanation on the possible application areas. Building on the application areas, highlighted in section III, section IV, will dwell on the types of attacks that are attributable to Internet of Things. This section discusses the core of this paper, as it hints on the security point of view of different attacks. Section V will summarize the security point of view with a focus on clearly highlighting areas of serious concern for security developers. Section VI will attempt to detail the performance analysis of the identified attacks in section IV. Section VII will pave a road map for future work as it summarizes the key security areas of attention, via a discussion. Section VIII will conclude this paper emphasizing the need to solicit solutions that could be implemented to secure internet of things applications.

978-1-4799-7707-9/15/$31.00 ©2015 IEEE

II. Desktop Review And Qualitative Analysis

The methodology employed for this research is justified by the need to gain the preliminary understanding of the work being done in light of the research focus on attacks that are inherent to IoT. The limited existence of practical resources to fully test some of the challenges motivated the need to have a desktop review of the issue in question. A desktop review gives an entry point understanding of a concept to be fully developed into a full fleshed research with limited resources. A qualitative analysis comes in handy in this context as the information to be analysed is from other sources that have also not had fully published results, hence the need to establish a basic conclusion from such sources.

III. IoT Applications Overview

The horizon of application environments for IoT is growing at an alarming rate. The application areas are no longer confined to communication platforms alone as the applications are stretching even to public safety [2], which among other application domains encompasses firefighting [3]. Despite the ability to improve and respond to public emergencies in cities [2], IoT applications should be secure and dependable. The application domains are not isolated from some privacy issues which may compromise citizens' safety and the right to confidentiality, as [3] clearly outlines in the context of firefighting, as an example, the home firefighting will entail supervision of the protected facilities; this is increasingly weakening the security points to any targeted object, despite the initial plan to ensure safety.

Cloud computing platforms have facilitated the growth of IoT application domains, because of the storage and communication platforms they avail. However the hesitancy around users to participate in active usage of such platforms and such technologies is attributable to the security fears. The need for assurance of whether the user on the other receiving end is exactly the person they are communicating to, and can be identified as such is vital for IoT's survival and thriving. Hence it is important to consider non repudiation/verification methods.

We now have smart cities; the agricultural sector is also not spared with farmers being able to track their animals, the education and health sectors almost receiving greater impacts in many application environments, as technology pockets continue to open and improve in such areas. There is a diverse hybrid of application capabilities in most of the technology capable environments, such as museums, where the tourism sector has evolved to be more interactive. The import and export industry is also witnessing the impact of improved service delivery as the processing of goods and services at border posts is gradually being automated especially in developing countries, where technology inception could be hampered by the pool of resources such as bandwidth and many indirect resources, that should ensure efficient technology consumption. The heterogeneous nature of applications is thus explained by the various platforms IoT are capable of being implemented and promise to impact.

It can safely be concluded that internet of things are almost everywhere and continue to expand as technological trends continue to unfold new dimensions and possibilities.

IV. Types Of Attacks On IoT

The major challenges inherent to IoT design, implementation and survival as summarised by [1], revolve around technological and security challenges. Among the key security challenges attributable to IoT applications, authentication could assume the toll, as other security loopholes are likely to sprout if the authentication level is weak; hence by addressing authentication requirements, we are creating a cascading solution to the IoT networks. However, there is need to breakdown the sources of threats into various small areas and tackle the challenges from such manageable horizons as the following four categories are going to attempt some classifications.

A. Application based

Application environments for IoT are seemingly complicated as there are huge data volumes of data to process from different sensor technologies that are supposed to feed their processing activities to the backend databases in some instances. As indicated in Fig 1, below, some of the challenges could be internal and some external. Considering the application based threats, the application environment could have its own vulnerabilities that are external to the IoT objects or devices, for example, physical insecurity compromising the efficient operation and results generated thereof. As an example, trying to capture the data pertaining to the local activities around a certain object, if there are interferences from people, data read from such an object is obviously biased and wrong information might be captured and decisions made from such data items, are likely to be compromised.

The constrained application environments for some IoT objects contribute to the security threats being stretched. Considering for instance the storage capacity of the application environment being small and not being able to fully store and process all the required security software, will present a susceptible IoT object to various intrusions and attacks. The need for lightweight security application software for such IoT objects is also met with application limitations. The application environment may not be compatible with the inherent security mechanisms of the IoT gadgets, hence extending the vulnerability of the entire application landscape.

The nakedness of the application environments in terms of security capabilities presents a complex security focus, where both the application environment and the IoT enabler object need serious security considerations for reliable functionality to be yielded.

The need for privacy protection for IoT data processing, data hiding methods for high-source heterogeneous data, is quite mandatory. Consider the CCTV cameras in banks, the positioning of such cameras should be strategic to get the

maximum coverage of the surface under surveillance. The data that may be of interest to the bank may have to do with protection against thieves, but there is no way to seclude the other bits and details. There is need for a study on the privacy protection methods in the process of mining in the chain of IoT data repositories. The study by [2] on the data processing mechanisms hints also on privacy protection through collaborative algorithms [2], however these still will remain short circuited for whole security packages towards other types of threats, hence the need to expand on this dimension.

The application environments contribute to huge amounts of metadata files that most importantly leave behind trails for attacks to be extended to application environments. A typical scenario could be a phone being tracked by hackers, they are able to connect various places and that in turn compromise security for all such visited areas by the innocent holder of the mobile phone. The biggest challenge being that, IoT are mostly communicating unsupervised.

B. Connection based

The existence of data flow paths to an object or an environment that may indirectly be connected to a particular IoT sensor, compromise the very private nature of that object. In trying to gain the holistic representation of the application domain a lot of other hidden components are exposed. A typical example could be a location aware device, which may pave way to dormant non-suspecting and unsecured devices to be attacked, because they are somehow connected to an IoT device broadcasting information to the outside world.

Resource constrained things are connected to the unreliable and untrusted internet via IPv6 and 6LoWPAN networks [4], explains how connection platforms contribute to the vulnerability of IoT. Internet by its very nature is not secure, added to the insecurity is now an IoT device that is also not fully secured, the end result is a wave of attacks being extended to a whole web of IoT networks.

Considering the work done by [16] on RFID obstacles, if we consider the internal obstacles of integration with legacy systems, there are two sides to such a setup, the legacy systems may be the ones vulnerable or the RFID connections to the legacy system will weaken the existing setup. Either way the connection links established at any point is an option for a different dimension of an attack.

The invisibility nature of networking [5] which is the most prevalent characteristic feature of IoT makes the analysis of potential network attacks even tougher. [5] highlighted capabilities of heterogeneous hardware among IoT, which renders them a complex networking domain to handle, this is so because of security, privacy and trust issues[5] that differ from one hardware manufacturer to the other. As further pointed by [5], such critical issues need to be resolved to get applications of future internet feasible and accepted by users.

C. Platform based

Platforms vary and as such present specific challenges. Some platforms by their very nature still have security issues that are unsolved to date. As presented by [6], the growth of cloud computing and communications platforms with data privacy and data protection issues continue to plague the market, hence hampering the growth of such platforms. IoT applications have already capitalised on the cloud computing platforms for extensibility and coverage and many other application based reasons. In such a scenario, there is need to first address the platform security loopholes as the inheritance level by applications that utilise such a platform are high and such inheritance cannot be isolated.

WSN has pending issues to be addressed which comprise of applications like communication platforms, security and management [7]. This again points to a serious concern in as far as the platform for communications being employed is concerned. As the growth of IoT connections increase, it implies that, they continue to proliferate the security concerns to be addressed. There is need to establish a secure communication path and improve the security level of the very interactions among the IoT objects themselves as they pass data items from point A to point B.

D. Other forms of attack

The categories mentioned in A to C above may not be an exhaustive analysis of attacks on IoT, hence not a comprehensive representation of the nature of attacks that are attributable to IoT. We may consider such issues as the absence of particular standards and specific laws that support the application development and deployment of IoT. The absence thereof, causes the sustenance and implementation of strict security measures from manufacturing points. We appreciate work underway to have such standards and laws enacted and in some sections being already in practice, however their grip on ensuring security adherence is still an open issue.

A combination of the highlighted sources of threats also breeds another hybrid source of threats and attacks to IoT. Combining application and platform based threats, gives an intertwined force of challenges that leave the whole security ground weakened, hence proper thriving of IoT applications is endangered. In the same vein, connection based threats combined with application based threats makes the whole application zone susceptible to serious threats. Bringing the entire three in one basket and adding the IoT in the same basket, we have a serious weaker product. This leaves a serious challenge in terms of how IoT will thrive in their various deployment domains.

V. SECURITY POINT OF VIEW

Security in IoT design mainly focuses on the end- to end communication links among the participating nodes. However considering the architectural view of IoT as presented by ITU, the security levels for IoT need to be focused on the

middleware level, since this is where the interaction amongst various node connections takes place. This is normally following an assumption that for all participating nodes in the internet of things to function effectively, they pass through some virtualized middleware. Reality will present a different challenge all together, where connection links created among nodes could so happen on an M2M(Machine to Machine) basis, hence little to no human interaction, under such scenarios. The security designs of the internet of things are better embedded inside the nodes or things themselves. This is met with physical and technological limitations of the nodes or things. The need to balance among size, memory and storage capacity makes the plan to implement robust security algorithms a futile effort.

The implementations of Intrusion Detection Systems (IDS), as there are no current IDSs that meet the requirements of IPv6 connected IoT, makes the security design for IoT complicated [4]. The existing security approaches are either specifically designed for wireless sensor networks (WSN) or the conventional internet, this explains why there is need to focus on standardised IDS designs for IoT communication platforms [4].

The SVELTE designed by [4], primarily targets routing attacks. The SVELTE security design is however limited to "spoofed or altered information, sinkhole, and selective forwarding [4]," these are not the only attacks IoT experience. To precisely have a solution that address all the security concerns in IoT is still a hard problem to solve.

VI. Performance Analysis Of Attacks

The attacks on IoT continue to increase in complexity as the number of connections and the possibilities of interaction among different heterogonous platforms increases. This is creating a complex security challenge to deal with, both on the virtual level and physical layer of IoT application platforms. As a result we are now faced with a different calibre of threats to deal with in IoT unlike in networked and confined networked environments; this is mainly amplified by the wireless capabilities coupled with the sensor technology inherent to IoT devices. High processing capabilities that could be harvested from such platforms as cloud computing, quantum computing and all possible ensuing computing technologies are also contributing factors in as far as the possible attack challenges increases are concerned.

"Attacks have to be intercepted, data authenticated, access controlled and the privacy of customers (natural and legal persons) guaranteed" [12]. These requirements seem to be at their infancy in terms of their realisation at a large scale, still presenting an apt ground for threats to continue to grow. Addressing one or two will not ensure the threats are contained, yet to have all addressed at once is a mammoth task.

Issues to deal with confidentiality, authenticity and integrity of data in IoT, should receive attention [13]. These three areas form the pillars of a security package. To realise all three all possible sources of IoT attacks should be identified and addressed to the full. Since it is not easy to have a generic solution that can qualify to embrace all the security requirements and ensure realisation of these security goals, this paper suggests adopting application models that interact via a middleware where such security measures could be enforced and monitored.

If security features are not strengthened, attacks and malfunctions in the IoT will outweigh any of their intended benefits. Protection mechanisms such as lightweight cryptography, secure protocols, and privacy assurance are not adequate to provide security to IoT [14]. This evidently supports the magnitude of the challenge at hand in advancing security to IoT applications.

The proposal by [15] to advance digital signatures as a measure to address the problem of spamming the IoT is only a one stop gap measure and may not practically apply to the diverse nature of IoT platforms. As a result of the different application domains that may not harness the existence of a solution in one area to cover the next area, still signal the need to have a direct focus on a particular breed of IoT applications and address them in isolation not universally.

VII. Discussion

Secure solution of trusted internet of things based on TCM [8] is based on cryptographic modules, which have limitations for some of the lightweight internet of things objects and hosting platforms. This solution is centred on the trustworthy of internet of things development and applications, which by nature may be limited in scope, considering the heterogeneous applications environments [9]. "The need to validate how existing security protocols can be adapted to meet the challenge of heterogeneous environments of IoT," as espoused by [9] is still an open issue.

Authentication and access control are crucial components to consider when designing secure communication of IoT [1], however the biggest challenge as highlighted by these authors, is provision of a distributed, lightweight and attack resistant solution to ensure comprehensive security for internet of things. The need to improve on the authentication and access control schemes available will remain a critical research call, as there still remain room for further improvements to the existing protocols.

The proposed solution by [1], was evaluated on the basis of DoS, man-in-the-middle and replay attacks. This cannot conclusively be the list of possible attacks that Internet of Things are susceptible to. As the classifications presented in section IV above, these three attacks can be application based, platform based or connection based, however, there is a new breed of attacks under hybrid based. As the journey towards security solutions design is not an event but a process that is marred with evolving threats, the need to refocus attention and considering endless possibilities to attack sources cannot be overemphasised.

The work done by [10] under the identity management handled some security issues to be focused on, but the

effectiveness of security protocols was not handled to the latter. Considering the same work done by [10], the capability levels computationally of IoT devices were not assessed thoroughly. The need to understand the computational capabilities is in light of the need to design implementable solutions that suit the technological build and capabilities of IoT.

Strategically, the need to focus on authentication and access control issues in IoT promises to avail a holistic solution to the technological and security challenges identifiable to IoT environments. Access control will avail a solution for the technological challenges and authentication on one hand will present the security solutions needed to avert the key threats attributable to IoT for the various application platforms especially powered by wireless and sensor connectivity.

VIII. CONCLUSION

The heterogeneous nature of IoT demands a versatile and unique legal framework that can broadly tackle globality, verticality, ubiquity and ethnicity of the IoT [12]. In considering security of typical IoT enabled devices and objects the interaction of such objects is not limited among the homogenous interactions, which they can create, but the various modalities that can be possible both horizontally and vertically. As a result of this approach, it can be anticipated that, a holistic approach to security challenges that could be identified for IoT could be uniquely extended to different classes of IoT implementations. A one size fits all strategy will not yield results.

ACKNOWLEDGMENT

For availing a thriving research environment, all gratitude is extended to the Polytechnic of Namibia which is transforming into Namibia University of Science and Technology. All the input from the research colloquial team that kept the research spirit enduring is highly appreciated.

REFERENCES

[1] N.Mahalle,B.Anggorojati, N.R. Prasad and R.Prasad, "Identity Authentication and capability based access control (IACAC) for the internet of Things," Journal of cyber security and Mobility, River Publishers, Vol 1, 2013, pp309-348.

[2] D.C. ZHU Shunbing, "Research on urban public safety emergency management early warning system based on technologes for the internet of things," 2012 International symposium on safety science and technology, Procedia Engineering Vol 45, 2012, pp 748-754.

[3] Z. Ying-Cong and Y. Jing, "A study on the fire IOT development strategy," Procedia Engineering, SciVerse ScienceDirect, Elservier, Vol 52, 2013, pp314-319.

[4] S.Raza, L.Wallgren and T. Voigt, "SVELTE:Real-time intrusion detection in the Internet of Things," Ad Hoc Networks Vol 11,2013, pp 2661-2674.

[5] P.Jappinen, R. Guarneri and L. M.Correia, "An applications perspective into the future internet," Journal of network and computer applications, Elservier, Vol 36, 2013, pp249-254.

[6] S. Subashini and V.Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, Elservier, Vol 34, 2011, pp 1-11.

[7] J.Yick, B. Mukherjee and D.Ghosal, "Wireless sensor network survey," Computer networks, Vol 52, 2008, pp2292-2330.

[8] Han,W. Qiu-xin and Li, "Secure solution of trusted Internet of Things based on TCM," The Journal of china universities of Posts and Telecommunications, 2013, pp47-53.

[9] Y.B.Saied,A.Olivereau,D.Zeghlache and M.Laurent, "Lightweight collaborative key establishment scheme for the internet of Things," Computer Networks, 2014, pp273-295.

[10] M.P. Narendra, "Identity management framework for internet of things,"Centre for Telefrastruktur & Aalborg University Denmark, 2013.

[11] P. Kassal, I. M. Steinberg and M. D. Steinberg, "Wireless smart tag with potentiometric input for ultra low-power chemical sensing,"Sensors and actuators Vol B 184, 2013,pp 254-259.

[12] R. H.Weber, "Internet of Things-New security and privacy challenges," Computer law & security review, Vol 26, 2010, pp 23-30.

[13] H. Suo, J. Wan, C. Ou and J. Liu, "Security in the internet of things: A review," 2012 International conference on computer science and electronic engineering.IEEE Computer Society, 2012, pp648-651.

[14] R. Roman, P. Najera and J. Lopez, "Securing the internet of Things," IEEE computer, Vol 44, No.9 , 2011, pp 51-58.

[15] F.Razzak, "Spamming the internet of Things: A possibility and its probable solution," Procedia computer science Vol 10,2012, pp 658-665.

[16] M.Aharan, "Critical success factors and challenges of implementing RFID in supply chain management," Journal of supply chain and operations management,Vol 10, No.1,2012, pp144-167.