Cognitive Computing and Internet of Things, Vol. 73, 2023, 68–72
https://doi.org/10.54941/ahfe1003975

Improving the Security and Usability of the Internet of Things Through a Scalable Network-Level Smart System

Mandeep Pannu, Iain Kay, and Ismail El Sayad

School of Computing, University of the Fraser Valley, Abbotsford, BC, Canada

ABSTRACT

The Internet of Things (IoT) is a network of interconnected devices, sensors, and systems that communicate without human intervention. This technology involves embedded sensors, software, and wireless communication protocols that enable devices to collect and exchange data in real-time. This allows businesses and individuals to monitor and control various aspects of their environment, from temperature and humidity to security and energy consumption providing intelligent insights and automating various tasks. However, these increasingly connected devices bring security vulnerabilities to homes and businesses facing digital attacks that were never possible. These could be IoT-connected door locks that leak network passwords or IoT coffee makers that can be set to make coffee from outside one's home network. These problems arise mainly from IoT devices where usability and functionality were the focus, and security was not considered. Furthermore, these IoT devices cannot implement security due to limited storage, memory, and processing power. This paper aims to assess the feasibility and develop an intelligent system that improves the security of Internet of Things (IoT) devices in the best possible way with minimal user interaction and a learning curve, which the IoT manufacturer may need to provide. At the same time, the system will provide end users with traditional intrusion detection methods and artificial intelligence-driven detection techniques that monitor the IoT devices to get timely feedback and possible actions with or without users' interactions.

Keywords: Internet of things, Security vulnerabilities, Interconnected devices, Intelligent system

INTRODUCTION

The IoT represents a significant shift in the way that we interact with technology, as it enables us to monitor and control a wide range of systems and devices in real-time, from anywhere in the world. The most recent research on IoT security is laid out in our 2019 paper [Pannu et al. 2019] on applying the NIST IoT security framework on a theorized IoT smart hub and the feasibility of such a device. The paper outlines inherent flaws in early IoT devices and the proposed method of ensuring device security for users on all devices going forward.

Authors earlier papers were aimed at attracting the attention of the scientific community and receiving feedback on the contribution of the research and how it would fit into the larger body of research. The reaction to our

research was positive, so we decided to move forward with the development of a reference prototype that can be used by private corporations and other researchers to advance the state of security in the IoT field. This diversion into the IoT security field was the logical result of our inquiries into network Intrusion Detection System (IDS) and our paper exploring Dynamic Security in the Workplace [Pannu et al. 2017].

Upon closer examination, we determined that a larger number of these devices were unable to be updated, due to manufacturers having gone out of business, or hardware needing to be more limited to support even the most basic of security measures. We also found that many IoT devices could not be patched due to hard-coded credentials nor run modern cryptography due to a lack of processing power. This is why we entered the field using our extensive knowledge of IDS, specifically network IDS [Pannu et al. 2016].

Our research in the dynamic security in the workplace paper [Pannu et al. 2017] revealed two main sources of security breaches: (1) social attacks targeting individuals, and (2) simple script attacks against un-updated network hardware. Given our pre-existing experience in IDS, we decided to redouble our efforts in the research field towards the network security devices leading to our production of the IoT paper. we realized, to be able to patch IoT devices at the application or hardware layer, we had to look for ways to apply these patches at the network layer. Looking back at our research in [Bul'ajoul et al. 2016], we realized that we had the capability to leverage our existing expertise in Network Intrusion Detection and Prevention Systems (NIDPS) to solve most of the security threats facing IoT equipped networks. Our research into Quality of Service (QoS) systems on Cisco routers [Sutter et al. 2016] gave us an idea of how we can enforce proxy settings and shape traffic through our own IDS filters on devices that cannot support these features due to hardware or software limitations.

RECENT PROGRESS

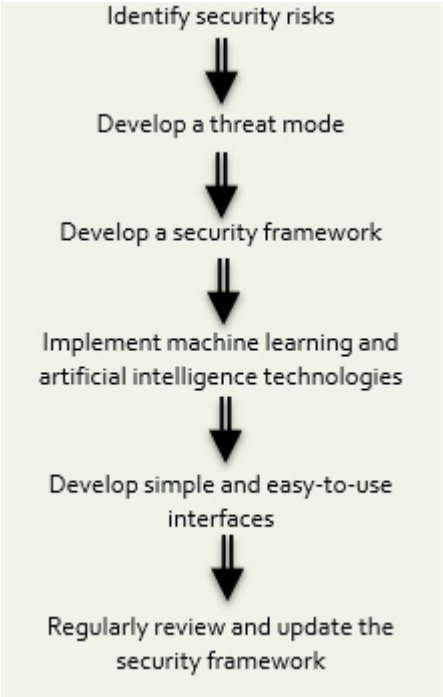
Recent research has shown that academic research to address the vulnerabilities of IoT systems has been largely positive. Current proposed methods of securing IoT devices follow the accepted standard of network security. That said, deploying conventional security measures on IoT devices is more complex than the average network. This is a result of the devices and protocols, in addition to nodes in the system, being relatively the same. The difficulty of reducing the threat to IoT devices, and other such issues, are covered in [Sha et al. 2018]. Other papers exist. The following papers, [Yuchen et al. 2015], [Lin et al. 2017], [Tewari et al. 2018], [Sfar et al. 2018], [Alaba et al. 2017], examine the challenges of the security issues that IoT systems face, as based on current countermeasures and layers of protection.

In [Kouicem et al. 2018], the paper covers how much research has been conducted to bring awareness to many of the key issues of policy enforcement, privacy, and integrity. This has led to the suggestion of new technologies, like Blockchain, to resolve new and on-going issues. Blockchain technology can provide a decentralized and tamper-proof platform for secure data sharing and communication among IoT devices.

It is crucial to continue exploring new technologies and approaches to enhance the security of IoT systems. As the number of IoT devices and applications continues to grow, so does the potential risk of security breaches and attacks. Therefore, it is imperative that we remain vigilant and proactive in addressing these issues to ensure the safety and security of IoT systems and their users.

PROPOSED DESIGN

The overall goal of this project is to assess the feasibility and develop an intelligent system which improves the security of Internet of Things (IoT) devices in the best possible way with minimal user interactive and learning curve, which may not be provided by the IoT manufacturer. The proposed system will utilize artificial intelligence (AI), machine learning (ML), and other technologies to improve the overall IoT devices security while keeping the systems simple and easy to use. This will provide significant benefit to protect the security of IoT devices and help to reduce attack surfaces of both private individuals and public institutions.



The first step in improving the security of IoT devices has been done by identifying potential security risks. This was done by analysing the architecture of the IoT system, the types of devices and sensors used, and the communication protocols used for data transfer. This helps to identify all the assets in the IoT system, including devices, sensors, networks, and data also helpful in understanding what needs to be protected.

After understanding the model, we analysed the system architecture to identify potential threats, such as unauthorized access, data breaches, and denial of service attacks. Consider internal and external threats and look for vulnerabilities in the IoT system that attackers could exploit. This includes vulnerabilities in the devices, communication protocols, and networks.

Once the security risks were identified, a threat model was developed, which involved analysing the potential threats and determining the likelihood of each one occurring and the potential impact of each threat on the system.

Based on the identified security risks and threat model, a security framework has been developed. This framework includes policies and procedures for securing the IoT system and technical controls to prevent and detect security breaches. The framework is an extension of NIST IoT Security and focuses on bringing legacy devices up to modern standards.

To improve the overall security of IoT devices, machine learning and artificial intelligence technologies can be used to detect and prevent security breaches.

These technologies can be used to analyse network traffic, identify anomalies, and detect suspicious activity.

While implementing technical controls and advanced security technologies, it is essential to keep the interfaces simple and easy for the end-users. This ensures that the system's security is not compromised due to user error or lack of understanding. As the threat landscape evolves, the security framework should be regularly reviewed and updated to ensure that it remains effective in protecting the IoT system from emerging threats.

CONCLUSION

This project will significantly contribute to the neglected aspect of the cyber security of legacy IoT devices. These devices are in widespread use and will never see a security update to address their many vulnerabilities. Additionally, many of these devices are physically incapable of being fixed through traditional means.

By analysing data generated by legacy IoT devices, AI and ML algorithms can identify patterns and anomalies that may indicate security breaches. Predictive models can be developed to anticipate and prevent security threats before they occur, reducing the attack surfaces for these devices.

Other technologies, such as blockchain and encryption, can also be used to improve the security of legacy IoT devices. Blockchain can provide a tamper-proof ledger for data and transactions, while encryption can protect data in transit and at rest, ensuring that it is only accessible by authorized parties.

Improving the security of legacy IoT devices is critical to the overall security of IoT systems. By utilizing advanced technologies such as AI, ML, blockchain, and encryption, we can address the many vulnerabilities present in these devices and reduce the risk of cyber-attacks.

REFERENCES

Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F. "Internet of Things security: A survey" Proceeding of the Journal of Network and Computer Applications, 2017. vol 88, pp. 10–28.

Bul'ajoul, W., James, A., Shaikh, S., Pannu, M. "Using Cisco Network Components to Improve NIDPS Performance" Journal of Third International Conference on Computer Science & Information Technology, 2016. pp. 137-157.

Fagan, M., Megas, K., Scarfone, K., Smith, M. Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers. In Pro. of July 2019, NISTIR 8259.

Kouicem, D. E., Bouabdallah, A., Lakhlef, H. " Internet of things security: A top-down survey" Proceeding of the Journal Computer Networks, 2018. vol 141, pp. 199–221.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W. "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications" Proceeding of the Internet Things Journal, 2017. Vol 4, pp. 1125–1142.

Pannu, M., Chong, J., Farrell, B., Cheng, J. "Application Development of a Driver Deployment and Communication System" Proceeding of the IEEE7th Annual Information Technology, Electronics and Mobile Communication Conference, 2016.

Pannu, M., Gill, B., Bird, R., Yang, K., Farrell, B., "Exploring Proxy Detection Methodology" Proceedings of the IEEE 4th International Conference on Cybercrime and Computer Forensics.

Pannu. M., Kay, I. "Internet of Things: Analyzing the impact on businesses and customers" Proceeding of 10th International Conference on Applied Human Factors and Ergonomics, 2019. Pp. 322–327.

Pannu. M., Salih, Q., Pappas, S., Roskell, R. "Exploring Dynamic Security in the Workplace" Proceeding of the IEEE 8th Annual Information Technology, Electronics and Mobile Communication Conference, 2017.

Sfar, R. A., Natalizio, E., Challal, Y., Chtourou, Z. "A roadmap for security challenges in the Internet of Things" Proceeding of the Digital Communication and Networks Journal, 2018, Vol 4, pp. 118–137.

Sha, K., Wei, W., Yang, A., Wang, Z., Shi, W. "On security challenges and open issues in Internet of Things" Journal of Future o Generation Computer Systems, 2018. vol. 83, pp. 326–337.

Sutter, P. QoS in Linux with TC and Filters, 2016 Project, http://linux-ip.net/gl/tc-filters.

Tewari, A., Gupta, B. "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework" Proceeding of the Future. Generation Computer. Systems journal, 2018. pp. 1–13.

Yuchen, H. Longfei, Y., Guisheng, W., Lijie, Y. "A survey on security and privacy issues in internet-of-things", 2015. Proceeding of the 10th International Conference Internet Technology Security Trans, 2015. Vol 4, pp. 202–207.