Framework for the Integrated Maturity Index for Internet of Things (IoT) Resilience against Cyber Attacks

[1]Seema Goel, [2]Ashish Jindal
[1]Jamia Hamdard, [2]Devi Ahilya Vishwavidyalaya
[1]New Delhi, India [2]New Delhi, India

Abstract— Internet of Things (IoT) is the latest wave of development in the information technology sector. Commonly used objects are now becoming 'smart' with intelligently embedded information technology peripherals. However, such devices were not initially developed with security as one of the foundation pillars and hence face complex challenges of data security concerns. These insecure "smart" devices lure cyber criminals due to the possibility of exploiting missing or insufficient security controls to avail access to precise personal information. This research aims to develop a 'Framework for the Integrated Maturity Index for IoT Resilience against Cyber Attacks' by analysing the underlying technical weakness in the IoT technology being implemented in the present day. (Abstract)

Index Terms— Cyber Security, Internet of things (IoT), Risk Assessment, Threat Intelligence, Vulnerability Analysis. (key words)

I. INTRODUCTION

IoT is gaining popularity as it offers benefits to organizations in managing physical assets, consumers in managing their health and fitness, and cities in managing automated operations. Any device which utilizes internet connection for data collection and exchange in existing equipment being used in homes, cars or industrial control to deliver its complete set of features is broadly classified as Internet of Things. IoT has numerous applications ranging from routine gargets like smartwatches, fitness trackers, home-monitoring cameras, smart TVs to critical systems like building and home automation, smart cities, healthcare and industrial control. According to Gartner, Inc. 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020.

The Internet of Things technology (IoT) aims to make everyday objects smart by embedding information technology at the core of electronic devices. IoT employs an array of efficient technologies such as accurate sensors and streamlined wireless connectors into the actual devices while deploying detailed data collection and precise analytics at the server end. In effect, each such internet connected smart device participates to form a highly distributed mesh of internetworked devices. IoT is gaining popularity due to its ability to deliver substantial improvement in asset utilization by introducing additional features to enhance built-in product efficiency. Ordinary devices communicating with human users alongside other devices, nowadays, possess a layer of communication technology interlaced with the original functionality. Device manufactures are investing heavily into the IoT technology due to increasing demand of appliances with enhanced sensors with the ability stay connected to the internet for communication.

Successful cyber-attacks have been made possible by crawling the internet to find unsecured devices and infected with malicious code in order to create a large network of compromised internet-connected digital devices called "bots", such as home routers and surveillance cameras. Such massive networks called "botnets" have been utilized in attacks against internet service providers and creating massive power outages by compromising the underlying smart grid IT infrastructure in the last few years.

Apart from disrupting the internet services, successful demonstrations have been displayed around the hacking abilities in SCADA (supervisory control and data acquisition) systems being used in industrial control systems, nuclear power plant systems, electrical grid systems, air traffic control systems and rail control systems.

II. OBJECTIVE OF THE RESEARCH

IoT devices often collect personal data during use and share with their manufacturers without the users being aware of any such data is being collected. The manufacturer also utilizes the underlying network channel to control the IoT devices by controlling them remotely in order to keep internal and external software applications up to date.

This research aims to develop a 'Framework for the Integrated Maturity Index for IoT Resilience against Cyber Attacks' by analysing the underlying technical weakness in the IoT technology being implemented in the present day. In order to unfold the latest attack techniques with underlying IoT based devices for facilitating cyber-attacks with maximized damage and minimized detection, established techniques of vulnerability assessment and penetration testing shall be implemented.

It further aims to analyses the ease of exploitation factor of the IoT devices to uncover the dangers of insecure codes embedded into such devices and develop an 'Overall Maturity Index' comprising of readiness in different domains, existing gaps and security recommendations. In addition to the identifying the cyber-attack resilience and readiness of the existing devices, the results of this research can be applied to secure development of IoT devices thus increasing the cyber security index of such devices being used in critical infrastructure as well as daily use objects. Additionally, the details of the existing gaps and proposed security strategies can lead to reduces damages and breaches that will lead to enhanced implementers and user's confidence in the use of IoT devices.

III. BACKGROUND

IoT devices are getting repeatedly hacked primarily because a number of such internet-connected devices are so deficient in even the most basic cybersecurity proprieties that it's possible to hack them almost effortlessly. With successful exploitation the hacker may steal data, conduct espionage on enterprise activities, or even cause physical damage. Existing challenges in implementing established cyber security measures include:

- IoT devices typically are not equipped with high-level computing capability, restricting the ability to introduce complex security strategies like encryption, two factor authentication, anti-virus etc. to secure the devices and the data they generate.
- The remotely connected and software-related security updates and configuration changes are generally harder to maintain in IoT devices, often leaving them insecure due to unpatched vulnerabilities.

- Additional challenge lies in the fact that the low-powered devices cannot meet the required uptimes if additional security software are running on them.

By leveraging the insecure connected devices, hackers can cripple our infrastructure, systems, and way of life. Or, they can directly exploit a device and use it as a gateway to deeper levels of a network where they gather sensitive and valuable private data. As IoT grows, the attack surface will also mature and the vulnerabilities present in the digital world will flow into our real world. Before IoT, attackers used vulnerabilities for data theft or to make money or sometimes just for fun, but with IoT, the attack surface has grown to such extent that attacker can use vulnerabilities or loopholes in the car, TV, camera, industrial control systems etc., to invade somebody's private life, record conversations, cause power outages, cause a blast in industry or even kill a person, and all possible remotely with a few strokes of the keyboard.

Beyond the risk of self-exploitations, the poor security in Internet of Things products including IP connected security systems, connected energy meters, connected printers, VoIP phones, smart video conferencing systems, smart fridges, and even smart lightbulbs etc have been leveraged to pose an inherent risk to the security of organizations by creating a massive attack network called botnets.

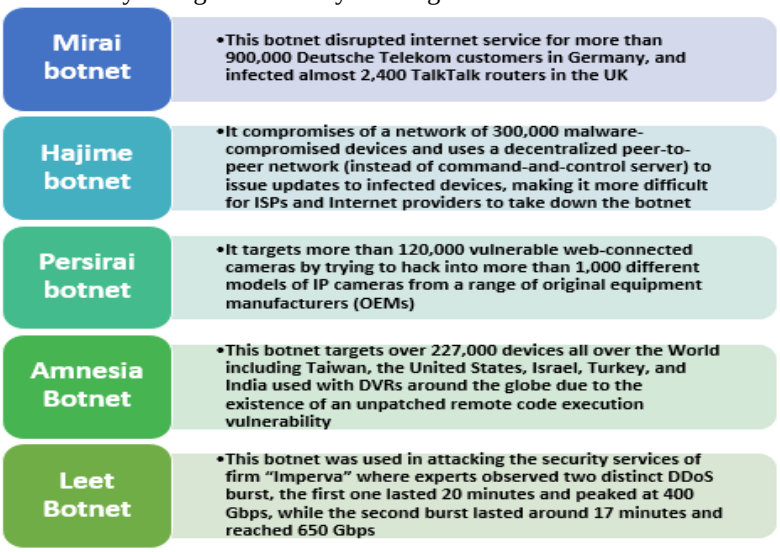

Figure 1: List of stablished IoT botnets

IV. Literature Review

Zoltan Balazs in his research titled "The real risks of the IoT security-nightmare Hacking IP cameras through the cloud" has considered the current IoT threat landscape to create a methodology about the different risks IoT devices can introduce into a network. He demonstrated that IoT devices (IP camera) with cloud connections are also susceptible to hacks due to basic security weaknesses in the cloud servers, like lack of brute-force protections or weak default passwords.

The study titled "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses" analyzes the security and privacy properties of an implantable cardioverter defibrillator (ICD). It provides a scientific baseline for understanding the potential security and privacy risks of current and future implantable medical devices (IMDs) while introducing human-perceptible and zero-power mitigation techniques that address those risks. This document discussed wirelessly reprogrammable implantable medical devices (IMDs) that include pacemakers, cardioverter defibrillators and implantable drug pumps. The researchers outlined not only privacy issues associated with these devices, but also the ability to change device settings, change or disable therapies, and even deliver a shock to the patient.

The Exploitee.rs Wiki has a range of IoT devices from a wide range of vendors including known vulnerabilities and directions on how to exploit them. The platform provides detailed exploitation mechanisms for IOT devices of various types from all leading vendors.

Figure 2: Exploitee.rs Wiki Homepage

The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.

Figure 3: Information areas of OWASP Internet of Things Project

The project looks to define a structure for various IoT sub-projects such as Attack Surface Areas, Testing Guides and Top Vulnerabilities.

OWASP Top Ten IoT Vulnerabilities	
1	Insecure Web Interface
2	Insufficient Authentication/Authorization
3	Insecure Network Services
4	Lack of Transport Encryption/Integrity Verification
5	Privacy Concerns
6	Insecure Cloud Interface
7	Insecure Mobile Interface
8	Insufficient Security Configurability
9	Insecure Software/Firmware
10	Poor Physical Security

Figure 4: OWASP Top 10 IoT Vulnerabilities

V. Gaps in Existing Research

Researchers are actively exploring potential risks in cyber security of the existing IoT infrastructure ranging from smart wearables, medical devices to drones and driverless cars. The scope of the present research revolves around security challenges, the potential vulnerabilities, and persistent threats that specific category of IoT systems may face.

An all-rounded approach incorporating the end customer has still not been devised. The majority of IoT product consumers admit that they don't fully understand the cyber security threats that IoT brings. Recent massive security breaches involving IoT devices suggest that consumers are afraid of using devices that they cannot trust and are willing to pay extra for products with enhanced security in order to protect the underlying network and data from being compromised.

Most established vendors have a dedicated team comprising of cyber security and network security experts that assess the security posture before the product is floated in the market, but the same does not stand true for all vendors/products. The security research aims at identifying the existing gaps or vulnerabilities that challenge the security posture of the IoT device remains limited to the knowledge of the developers. However, this data is not visible to the end consumer/buyer/user of that device and hence his confidence cannot be ascertained. As a customer, it becomes really impossible to judge the security posture of the product as they are not aware of the mechanisms that the developers have implemented at the backend and hence have no option but to simply rely on the brand value.

If the device in any manner can be labelled to give an indication of the hardening and security approaches that have been adopted in this product in terms of some score/rating, it surely can increase the confidence of the customer, since now he is aware of the product in terms of cyber-attack resilience. However, this rating does not specify that the device is hack-free or is cannot be tampered, but it does provide some minimum security assurance. In the present scenario, no such rating/score/marking exists, hence allowing developers to oversee the security aspects, but if a compliance can be brought around such a **prescriptive or mandatory rating/score/marking**, the security background of the IoT devices is definitely going to improve.

The research aims to develop a methodological approach to present the security index of IoT devices derived from numerous dependent vectors and formulas at the core. This is the right time to incorporate such a mechanism, since the technology is in initial adoption phase. To go by researchers, IoT is the next big thing and adoption of any such approach will only become more complicated to inculcate in the time to come.

VI. Approach and Methodology

Any IoT device comprises of three major components: hardware, operating system software, and the data it creates or senses. All three of these components are vulnerable to cyber-attack, perhaps even more so than other IT innovations due to the fact that IoT devices typically live outside an organization's normal IT boundaries. This limits the ability to use existing security infrastructure to provide security and management for IoT devices from intruders. Unlike other IT infrastructure endpoints, the IoT devices are still in the maturing phase and established strategies for endpoint protection like data leakage protection cannot be implemented on an as-is basis due to the volume of devices. Also adding any complicated security add-ons might substantially increase the cost of IoT devices, thus reducing customer demand and acceptance. Both hardware and software vulnerabilities contribute to overall data safety as the security of the data at rest and in transit is directly dependent on the security of the hardware and software generating it. This research targets to deliver a come up with a Security Breach Readiness Report comprising the following aspects:

1. Analysis of IoT implementation use cases in various industries to identify threats to IoT devices and implementations

The activities in this phase of research include the analysis of the existing implementations of the various types of IoT devices in different operating environments. It also tries to map the existing IoT device types in the accordance with the implementation volume across different sectors and geographies in order to identify the overall scope of research application.

2. Designing the IoT Cyber Threat Landscape

With the knowledge of the scope of research, the next step involves the designing of overall cyber threat landscape in the existing scope. This involves the identification of the various technical threats that lie in IoT devices.

3. Conceptualizing the Overall Maturity Index for IoT readiness against Cyber Attacks

This step utilizes the outcomes of the previous steps in order to generate the Overall Maturity Index, a levelled index that identifies the readiness of an IoT device implementation against Cyber Attacks. The index will indicate the cyber security posture of the IoT device that can be relied upon to indicate the deployment of that device, say a device with higher maturity index is established to be more secure against cyber threats than one with a lower maturity index.

Methods used to create a comprehensive threat landscape include the techniques mentioned in Figure 5.

This step involves the analyses and correlation of large volumes of data in order to identify both known and unknown indicators of compromise (IoC) by focusing on several behavior patterns used for attacking and compromising systems and network communications.
In addition to identifying the underlying threats within the IoT devices it also focuses on finding root cause of the uncovered threats in order to develop appropriate mitigation strategies in terms of developing secure devices to combat those threats and any potential compromise arising out of their exploitation.

Figure 5: Information areas of OWASP IoT Project

The Maturity Index will be identified in accordance with a detailed methodology developed around the following aspects:

Figure6: Components of Maturity Index for determining Internet of Things (IoT) Resilience against Cyber Attacks

VII. BENEFITS OF RESEARCH

A	For Some critical product lines like medical devices, driverless cars or drones that may involve loss of life or national security, the minimum acceptable score of security preparedness can be kept high to ensure immunity against any cyber-attack.
B	The consumer can decide upon the use-case of that particular device and the level of security that's important for its placement. For example, a lock at the main door of the apartment might be more critical and have a greater impact if compromised than one placed on the closet.
C	It helps the organization and the developers understand the varying security postures of their product/device and the corresponding demands for each of them. Hence it serves as a market analysis of which variant is being most demanded to alter and manage the respective production lines.
D	In addition, the organizations will also develop an insight into if the potential customer is ready to spend more on the same product with enhanced cyber security and thus trigger higher spends on the security research and development program in lieu of customer demand.
E	This rating/score/marking over the time will also enhance the cyber security awareness posture of consumers towards the IoT devices, which at the moment is a grave concern as many of them are unaware of the potential of these devices in terms of cyber-attacks.

REFERENCES

[1] Tobias Heer, Oscar Garcia-Morchon, Ren´e Hummen, Sye Loong Keoh, Sandeep S. Kumar and Klaus Wehrle, Security Challenges in the IP-based Internet of Things, (2014)

[2] Bellekens,, Xavier, Amar Seeam, Kamila Nieradzinska, Christos Tachtatzis, Alison Cleary, Robert Atkinson, and Ivan Andonovic, Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures, (2015)

[3] Mark Stanislav and Tod Beardsley, HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities, (2015)

[4] Glenn A. Fink, Dimitri V. Zarzhistky, Thomas E. Carroll, and Ethan D. Farquhar, Security and Privacy Grand Challenges for the Internet of Things, (2015)

[5] Mahalle, Parikshit N.; Anggorojati, Bayu; Prasad, Neeli R.; Prasad, Ramjee, Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things, (2013)

[6] Mohamed Abomhara and Geir M. Køien, Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, (2015)

[7] Cesar Cerrudo, IOActive Labs. An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks, (2015)

[8] Bitdefender's The Internet of Things: Risks in the Connected Home, (2016)

[9] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Cybersecurity for the Internet of Things (IoT) program https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[10] The Open Web Application Security Project (OWASP) Internet of Things Project https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project