A REVIEW OF CYBER SECURITY AND THE INTERNET OF THINGS

[1]Mrs.C.Radha, [2]Mr.S.Nithyananth, [3]Ms.I.Meena
Associate Professor/MCA , II MCA
[1]radhamca7@gmail.com, [2]nithyananth85@gmail.com, [3]meenaaiyyamuthu3@gmail.com

Abstract - Internet of Things (IoT) devices are rapidly becoming everywhere while IoT services are becoming invasive. The number of threats and attacks against IoT devices and services are on the increase as well. Cyber-attacks are not new to IoT, but as IoT will be deeply interwoven in our lives and societies, it is becoming necessary to step up and take cyber defense seriously. The threat of cyber-crime is increasing reality in both the private and professional sectors. The purpose of this research is to make awareness regarding cyber-crimes happening in today's world and also to create awareness of cyber security. This paper attempts to analyze the understanding of cyber-crime among internet users with different age groups and educational qualifications. Linear Regression Model has been applied for analyzing both the objectives. Hence, there is a real need to secure IoT, which has therefore resulted in a need to widely understand the threats and attacks on IoT infrastructure. This paper is an attempt to classify threat types, besides analyze and characterize intruders and attacks under IoT devices and services.

Index Terms—Cyber attacks, IOT, Security, Vulnerability

I. INTRODUCTION

The internet in India is growing rapidly. It has given rise to new opportunities in the field of entertainment, business, sports, education, and many more. With the advent and increasing use of internet, the businesses have crossed the barriers of local markets and are reaching out to customers located in every part of the world. Computers are widely used in enterprises not only as a tool for processing information, but also for gaining strategic and competitive advantage. Computers can be used both for constructive and destructive reasons.

India is on the radar of cyber criminals with growing cyber-attacks on Indian establishment. India rank third as a source of *malicious activity* on the internet after US and China, second as source of *malicious code* and fourth and eight as source or origin for *web attacks* and *network attacks*.

According to the Indian Computer Emergency Response Team (CERT-In), 27,482 cases of cybercrime were reported from January to June (2017). These include phishing, virus or malicious code, defacements, scanning or probing, site intrusions, ransom ware and denial-of-service attacks.

The number of threats is rising daily, and attacks have been on the increase in both number and complexity. Not only is the number of potential attackers along with the size of networks growing, but the tools available to potential attackers are also becoming more sophisticated, efficient and effective . Therefore, for IoT to achieve fullest potential, it needs protection against threats and vulnerabilities .

It has been shown that in the first six months of 2017, at least one cybercrime was reported every 10minutes in India which is higher as compared to every 12 minutes in 2016.India has seen a total of 1.71 lakh cybercrimes in the past 3.5 years and the number of crimes so far this year has been 27,482, which indicates that the total number is likely to cross 50,000 by this December. Analysis of data from 2013 to 2016 shows that 6.7% of all cases accounted for network scanning and probing while virus or malware accounted for 17.2%.

According to the latest report National Crime Records Bureau(NCRB), a total of 11,592 cases were registered under the cyber-crimes (which includes cases under Information Technology Act, offences under related sections of IPC and offences under Special and Local Laws (SLL)) in comparison to 9,622 cases registered during the previous year (2014) which shows an increase of 20.5% over the previous year. Uttar Pradesh has reported the highest number of such crimes followed by Maharashtra and Karnataka.

II. BACKGROUND

The IoT is an extension of the Internet into the physical world for interaction with physical entities from the surroundings. Entities, devices and services are key concepts within the IoT domain, as depicted in. They have different meanings and definitions among various projects.

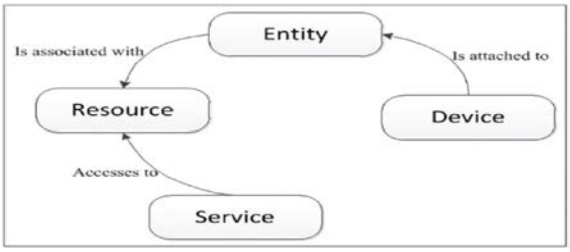

Fig. 1 IOT Domain

A. IoT device

This is a hardware component that allows the entity to be a part of the digital world . It is also referred to as a smart thing, which can be a home appliance, healthcare device, vehicle, building, factory and almost anything networked and fitted with sensors providing information about the physical environment (e.g., temperature, humidity, presence detectors, and pollution), actuators (e.g., light switches, displays, motor-assisted shutters, or any other action that a device can perform) and embedded computers.

B. Security in IoT devices and services

Ensuring the security entails protecting both IoT devices and services from unauthorized access from within the devices and externally. Security should protect the services, hardware resources, information and data, both in transition and storage. In this section, we identified three key problems with IoT devices and services: data confidentiality, privacy and trust.

C. IoT services

IoT services facilitate the easy integration of IoT entities into the service-oriented architecture (SOA) world as well as service science . According to Thomas , an IoT service is a transaction between two parties: the service provider and service consumer. It causes a prescribed function, enabling interaction with the physical world by measuring the state of entities or by initiating actions that will initiate a change to the entities.

A service provides a well-defined and standardized interface, offering all necessary functionalities for interacting with entities and related processes. The services expose the functionality of a device by accessing its hosted resources.

D. Security Threats, Attacks, and Vulnerabilities

Before addressing security threats, the system assets (system components) that make up the IoT must first be identified. It is important to understand the asset inventory, including all IoT components, devices and services.

An asset is an economic resource, something valuable and sensitive owned by an entity. The principal assets of any IoT system are the system hardware (include buildings, machinery, etc.) , software, services and data offered by the services .

E. Vulnerability

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks . Vulnerabilities can be found in variety of areas in the IoT systems. In particular, they can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves.

F. Exposure

Exposure is a problem or mistake in the system configuration that allows an attacker to conduct information gathering activities. One of the most challenging issues in IoT is resiliency against exposure to physical attacks. In the most of IoT applications, devices may be left unattended and likely to be placed in location easily accessible to attackers. Such exposure raises the possibility that an attacker might capture the device, extract cryptographic secrets, modify their programming, or replace them with malicious device under the control of the attacker.

G. *Threats*

A threat is an action that takes advantage of security weaknesses in a system and has a negative impact on it . Threats can originate from two primary sources: humans and nature . Natural threats, such as earthquakes, hurricanes, floods, and fire could cause severe damage tocomputer systems. Few safeguards can be implemented against natural disasters, and nobody can prevent them from happening.

H. *Attacks*

Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. Attack actors are people who are a threat to the digital world . They could be hackers, criminals, or even governments .The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost.

III. PRIMARY SECURITY AND PRIVACY GOALS

To succeed with the implementation of efficient IoT security, we must be aware of the primary security goals as follows:

A. *Confidentiality*

Confidentiality is an important security feature in IoT, but it may not be mandatory in some scenarios where data is presented publicly . However, in most situations and scenarios sensitive data must not be disclosed or read by unauthorized entities. For instance patient data, private business data, and/or military data as well as security credentials and secret keys, must be hidden from unauthorized entities.

B. *Integrity*

To provide reliable services to IoT users, integrity is a mandatory security property in most cases. Different systems in IoT have various integrity requirements . For instance, a remote patient monitoring system will have high integrity checking against random errors due to information sensitivities. Loss or manipulation of data may occur due to communication, potentially causing loss of human lives .

C. *Authentication and authorization*

Ubiquitous connectivity of the IoT aggravates the problem of authentication because of the nature of IoT environments, where possible communication would take place between device to device (M2M), human to device, and/or human to human. Different authentication requirements necessitate different solutions in different systems. Some solutions must be strong, for example authentication of bank cards or bank systems. On the other hand, most will have to be international, e.g., ePassport, while others have to be local . The authorization property allows only authorized entities (any authenticated entity) to perform certain operations in the network.

D. *Availability*

A user of a device (or the device itself) must be capable of accessing services anytime, whenever needed. Different hardware and software components in IoT devices must be robust so as to provide services even in the presence of malicious entities or adverse situations. Various systems have different availability requirements. For instance, fire monitoring or healthcare monitoring systems would likely have higher availability requirements than roadside pollution sensors.

E. *Auditing*

A security audit is a systematic evaluation of the security of a device or service by measuring how well it conforms to a set of established criteria. Due to many bugs and vulnerabilities in most systems, security auditing plays an important role in determining any exploitable weaknesses that put the data at risk. In IoT, a systems need for auditing depends on the application and its value. 2.3.7 Non-repudiation The property of non-repudiation produces certain evidence in cases where the user or device cannot deny an action. Non-repudiation is not considered an important security property for most of IoT. It may be applicable in certain contexts, for instance, payment systems where users or providers cannot deny a payment action. Privacy goals Privacy is an entitys right to determine the degree to which it will interact with its environment and to what extent the entity is willing to share information about itself with others.

The main privacy goals in IoT are:

- Privacy in devices – depends on physical and commutation privacy. Sensitive information may be leaked out of the device in cases of device theft or loss and resilience to side channel attacks.
- Privacy during communication – depends on the availability of a device, and device integrity and reliability. IoT devices should communicate only when there is need, to derogate the disclosure of data privacy during communication.
- Privacy in storage – to protect the privacy of data stored in devices
- Possible amounts of data needed should be stored in devices

F. Accountability

When developing security techniques to be used in a secure network, accountability adds redundancy and responsibility of certain actions, duties and planning of the implementation of network security policies. Accountability itself cannot stop attacks but is helpful in ensuring the other security techniques are working properly. Core security issues like integrity and confidentiality may be useless if not subjected to accountability.

IV. PURPOSE AND MOTIVATION OF ATTACK

Government websites, financial systems, news and media websites, military networks, as well as public infrastructure systems are the main targets for cyber-attacks. The value of these targets is difficult to estimate, and estimation often varies between attacker and defender. Attack motives range from identity theft, intellectual property theft, and financial fraud, to critical infrastructure attacks. It is quite difficult to list what motivates hackers to attack systems. For instance, stealing credit card information has become a hackers hobby nowadays, and electronic terrorism organizations attack government systems in order to make politics, religion interest.

The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost .

A. Intruders, Motivations and Capabilities

The motives and goals of intruders vary from individual attackers to sophisticated organized-crime organizations. Intruders also have different levels of resources, skill, access and risk tolerance leading to the portability level of an attack occurring . An insider has more access to a system than outsiders. Some intruders are well funded and others work on a small budget or none.

Intruders have different motives and objectives, for instance, financial gain, influencing public opinion, and espionage, among many others.

Intruders are categorized according to characteristics, motives and objectives, capabilities and resources.

Every attacker chooses an attack that is affordable, an attack with good return on the investment based on budget, resources and experience.

V. IOT SECURITY CHALLENGES

Challenges for IoT and key IoT security concerns include:

A. Lack of testing and development

Some IoT manufacturers have treated security as an afterthought in their haste to bring products to market. Device-related security risks may have been overlooked in the development process, and once launched, there may be a lack of security updates. However, as awareness of IoT security has grown, so too has device security.

B. Default passwords leading to brute-forcing

Many IoT devices come with default passwords and these are often weak. Customers who buy them may not realise they can (and should) change them. Weak passwords and login details leave IoT devices vulnerable to password hacking and brute-forcing.

C. IoT malware and ransomware

Given the considerable increase in IoT connected devices in recent years – which is forecast to continue – the risk of malware and ransomware to exploit them has increased. IoT botnet malware has been amongst the most commonly seen variants.

D. Data privacy concerns

IoT devices gather, transmit, store and process a vast array of user data. Often, this data can be shared with or sold to third parties. While users typically accept terms of service before using IoT devices, many people don’t read the terms – which means it's not always apparent to users how their data may be used.

E. Escalated cyberattacks

Infected IoT devices can be used for distributed denial of service (DDoS) attacks. This is where hijacked devices are used as an attack base to infect more machines or conceal malicious activity. While DDoS attacks on IoT devices more commonly affect organizations, they can also target smart homes.

F. Insecure interfaces

Common interface issues that affect IoT devices include weak or no encryption or insufficient data authentication.

G. The rise of remote working

Following the Covid-19 pandemic, remote working has increased around the world. While IoT devices have helped many users to work from home, often home networks can lack the security of organisational networks. The increased usage has highlighted IoT security vulnerabilities.

H. Complex environments

Research shows that in 2020, the average household in the US had access to 10 connected devices. All it takes is one overlooked security misconfiguration in one single device to put the whole household network at risk.

VI. CONCLUSION

It was concluded that much work remains to be done in the area of IoT security, by both vendors and end-users. It is important for upcoming standards to address the shortcomings of current IoT security mechanisms.We hope this survey will be useful to researchers in the security field by helping identify the major issues in IoT security and providing better understanding of the threats and their attributes originating from various intruders like organizations and intelligence agencies. As future work, the aim is to gain deeper understanding of the threats facing IoT infrastructure as well as identify the likelihood and consequences of threats against IoT. Definitions of suitable security mechanisms for access control, authentication, identity management, and a flexible trust management framework should be considered early in product development.

REFERENCES

[1] Dr. Shikha Gupta, Vaama Nikam, Tanay Mukadam, Prathmesh Deshmukh, Prathamesh Bhanse, “Cyber Security for Internet of Things,” IJRASET, ISSN : 2321-9653, Volume 10 Issue X Oct 2022.

[2] R.Vignesh, A.Samydurai , “Security on Internet of Things (IOT) with Challenges and Countermeasures,” IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939, 2017.

[3] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, “Internet of Things (IoT) Applications and Security Challenges: A Review “ IJERT, ISSN: 2278-0181, Vol 7 Issue 12, 2019.

[4] Mohamed Abomhara and Geir M. Køien , “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks”, Journal of Cyber Security, Vol. 4, 65–88, 2015.

[5] Ricardo Jorge Raimundo , Albérico Travassos Rosário , “Cybersecurity in the Internet of Things in Industrial Management”, Appl. Sci. 2022.