ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 3, March 2016

Internet of Things: Understanding the Security Concerns

First Dr.P.B.Pathak

Assistant Professor and Head, Department of Computer Science & Information Technology

Yeshwant Mahavidyalaya Nanded

Maharashtra, India

***Abstract*— Internet of Things combines Things with Internet connectivity and powerful data collection and analytics. The next generation of Internet is the Internet of Things. The fully interconnected Internet of Things is beneficial and revolutionary with ample opportunity for progress. Ubiquitous connectivity, adoption of Internet Protocol, high computing power available at low cost, miniaturization of sensor, data analytics, cloud computing are the factors responsible for fast and widespread proliferation Internet of Things. Rapidly developing Internet of Things technology is useful in areas healthcare, transportation, manufacturing, energy. Internet of Things opportunity accompanies some risks. Cyberattacker look for Internet connected object for cyberattacks. Decision making machines and data capturing sensors are, creating serious problem of security. The present paper elaborates some definitions of Internet of Things and current security concerns.**

***Index Terms*— Devices, Ecosystem, Internet of Things, Network, Sensors, Vulnerability**

I. INTRODUCTION

Embedded intelligent and interconnected devices pose a security challenge of intrusion and interference that can compromise personal privacy and threaten public safety. Ensuring the security, reliability, resilience, and stability of Internet of Things applications and services is important. Software security controls at the operating system level can be more useful. Internets of Things operations are more secure if security mechanism exists on device and on network level. The intelligence of Internet of Things devices can recognize and defend threats. Unauthorized access and misuse of personal information, attacks on systems and safety problems are potential security risks that can be exploited to harm users of Internet of Things. [7,14]

Securing connected Internet of Things devices is more challenging than securing a computer. Traditional risks of computers and computer networks are enhanced in the Internet of Things. Intruder access and misuse personal information collected by the Internet of Things devices. Device vulnerability is a growing problem. Security vulnerabilities can facilitate attacks on the user's network or initiate attacks on other systems. Increase in connected Internet of Things devices has increased opportunities to exploit security vulnerabilities. Cybercriminals can exploit security vulnerabilities to get unauthorized access to create physical safety risks. Poorly designed/secured Internet of Things devices can cause cyberattacks to disrupt a device to malfunction and can expose user data to theft. Malfunctioning devices can create security vulnerabilities. [13,18]

Global dependence of the highly interconnected Internet of Things devices for essential services, create increased security and resilience opportunities for cybercriminals. Though security measures are evolving along with network evolution, a multi layered security approach is needed. A multi layered approach essentially contains, secure booting, access control, device authentication, firewall, intrusion prevention systems and updates-patches. Secure booting is verifying authenticity and integrity of the software on the device using cryptographically generated digital signatures. Access control is limiting the privileges of device components and applications. Device authentication is done prior receiving or transmitting data. Firewall and intrusion prevention systems are used to control traffic at the device. Updates-patches attempts to eliminate the possibility of compromising functional safety. Weak passwords, poorly protected credentials, can allow cyberattacker to gain access to a device. [1,6,21]

Manuscript received Mar, 2016.
Dr.P.B.Pathak
Assistant Professor and Head,
Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded
Maharashtra, India

II. Internet of Things Definition

The concept of Internet of Things is defined based on different considerations like global implications, applications, technology, and architecture. Though the high importance, technologically advanced, human life transformer, world economy driver, universally accepted definition for the term Internet of Things is not available. The Internet of Things is, extending Internet connectivity and computing capabilities to a variety of objects, devices, sensors, and everyday things. Internet of Things is the ability to connect, communicate, and remotely manage large number of networked, automated devices related to almost every walk of our life, using Internet. [8,17]

The Internet Architecture Board gives the Internet of Things a trend where a large number of embedded smart devices employ communication services offered by the Internet protocols. Internet Engineering Task Force defines Internet of Things as smart object networking, with limited power, memory, and processing resources, or bandwidth. International Telecommunication Union elaborates Internet of Things as a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies. IEEE communications magazine defines the Internet of Things as it is a framework in which all things have a representation and a presence in the Internet that enables the interactions between Things and applications in the cloud. [12,15]

The Oxford Dictionaries states that the Internet of things as the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. The everyday objects are from industrial machines to wearable devices using built in sensors to gather data and take action on that data across a network. The Internet of Things is the future of technology that can make our lives more efficient. The Internet of Things is an increasingly connected future in which regular, everyday items are outfitted with sensors and connected to the Internet to share their data. The Internet of Things will give rise to an entire ecosystem for interconnected devices, objects, systems, and data all working together. Internet of Things is wearable technology and smart appliances, autonomous machines and equipment with sensors, big data and data analytics. [2,5,21]

III. Security Issues and Challenges of Internet of Things

Internet of Things is accelerating globally at an amazing rate raising concerns about security. Commercialization of the Internet is responsible for rapid spread of Internet of Things and expanded security concerns. Accidental or malicious, interference with the controls of Internet of Things devices poses a threat to human life. Security can be seen as inseparable from safety of human life. The vast variety of Internet of Things devices and applications poses an equally vast variety of security and safety challenges. Different implementations Internet of Things present unique security challenges making it difficult full realization of potential benefits. Current fundamental priority is to ensure security in Internet of Things products and services by addressing these challenges. Cyberattacker use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, etc. to gain access to Internet of Things device. Vulnerabilities in Internet of Things devices are in abundance and make it mandatory to have some built in features such as encryption, authentication and the ability to remotely update devices. Poorly secured or unsecured Internet of Things devices and services can be potential entry points for cyberattacks. [4,16]

The reasons for amplified security challenge include very large scale deployment, the ability of devices to automatically connect to other devices, and the deployment of these devices in unsecure environments. A collaborative security approach of developers and users is needed to surface effective security mechanisms in Internet of Things. Privacy, authentication/ authorization, transport encryption, Cloud service/web interface, software/firmware are some security concerns of Internet of Things. Interconnected devices have access to the most sensitive personal data such as name, address, date of birth, health and banking information and can create new opportunities for cybercriminals. Lack of data transport encryption, Lack of requirement of passwords with sufficient complexity and length, vulnerable user interfaces, insufficient authentication and authorization are some prominent Internet of Things device security concerns. Persistent crosssite scripting, poor session management and weak default credentials are particular concern with web interface for devices that offer access to devices and data via a cloud website. [9,19]

The Internet of Things presents a variety of potential security risks that can be exploited to harm users by enabling unauthorized access and misuse of personal information, facilitating attacks on other systems and creating risks to personal safety. Privacy, cybersecurity, and liability are some of the biggest risks for Internet of Things. Rapid evolution, connectivity/interoperability, power management, security/privacy, complexity, data storage, legal, regulatory and rights are some key challenges of Internet of Things. The Internet of Things is continuously evolving with more devices are being added every day. Appropriate standards, reference models, and best practices support greater user benefits, innovation, and economic opportunity. Devices within the Internet of Things require power the challenge is power management of these devices and equipment. Security hardware and use of existing connectivity security protocols is essential to prevent unauthorized use and attacks considering the amount of personal or business data being sent within the Internet of Things. [11,20]

Internet of Things amplifies concerns of increased surveillance and tracking, and the strength of combining data streams from users. Personally identifiable data collected without the consent and knowledge raises serious

privacy Challenge. Routing, capturing, analyzing and using the insights inferred from huge volumes of Internet of Things data in real time and where, how, when the vast amounts of data generated from individual sensors, devices to store are the huge challenges. The challenge is also availability of spectrum and bandwidth for efficient communication. When Internet of Things devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing then legal issues of cross border data flow occurs. Data collected by Internet of Things devices is sometimes susceptible to misuse and potentially discriminatory. Other legal issues with IoT devices include the conflict between law enforcement surveillance and civil rights, data retention and destruction policies, and legal liability for unintended uses, security breaches or privacy lapses. [3,10]

IV. CONCLUSION

Internet of Things has limitless possibilities to cater benefits to the society. Internet of Things technology with embedded sensors, actuators, and traditional low power systems on chips into physical objects transformed lives and made global economic impact. Realization of potential benefits of Internet of Things may be dimmed by significant challenge of security. Internet of Things devices and related data services must be secure from vulnerabilities. Connected devices are growing, security concerns are also exponentially growing. Cloud services, mobile applications increase concerns. The importance of transport encryption rises significantly when sensitive in nature data collected by devices is being passed between the device and the cloud, and a mobile application. Unprotected and unencrypted software and updates download is a big concern.

Every problem Internet of Things solves, there is another problem it creates. Ease of design and development is essential to get more things connected since user must be able to set up and use their devices without a much technical expertise. Full interoperability across products and services is not possible. The challenge is getting the common connectivity standards or protocols for these devices to talk to each other. Vendors, technologies and protocols reduce interoperability in Internet of Things. The full potential of the Internet of Things can only be realized if the security concerns are fully addressed.

REFERENCES

[1] "Reaping the Benefits of the Internet of Things", (2014), http://www.cognizant.com/InsightsWhitepapers/Reaping-the-Benefits-of-the-Internet-of-Things.pdf
[2] Ovidiu Vermesan, Peter Fries, "Internet of Things-From Research and Innovation to Market Deployment", (2014) http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf
[3] White paper on "Realizing the Potential of The Internet of Things: Recommendations to Policy Makers", (2015), https://www.tiaonline.org/sites/default/files/pages/TIA-White-Paper-Realizing_the_Potential_of_the_Internet_of_Things.pdf
[4] Jim Chase, The White Paper on, "The Evolution of the Internet of Things", (2013), http://www.ti.com/lit/ml/swrb028/swrb028.pdf
[5] "The Internet of Things: An Overview-Understanding the Issues and Challenges in More Connected World", (2015), https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf
[6] "The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data", (2014), http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf
[7] White Paper on, "The Internet of Things: Security Research Study", (2015), https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf
[8] Pew Research Center, "The Internet of Things Will Thrive by 2025", (2014), http://www.pewinternet.org/2014/05/14/internet-of-things/
[9] Techopedia, "Internet of Things", (2015), https://www.techopedia.com/definition/28247/internet-of-things-iot
[10] White Paper on, "Security in the Internet of Things-Lessons from the Past for the Connected Future", (2015), http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
[11] "Internet of Things-Privacy & Security in a Connected World", (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[12] Ovidiu Vermesan, Peter Fries, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", (2013), http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf
[13] Daniel Castro & Jordan Misra, "The Internet of Things", (2013), www2.datainnovation.org/2013-internet-of-things.pdf
[14] "The Internet of Things: Evolution or Revolution?",(2015), http://www.aig.com/Chartis/internet/US/en/AIG%20White%20Paper%20-%20IoT%20English%20DIGITAL_tcm3171-677828_tcm3171-698578.pdf
[15] McKinsey Global Institute, "The Internet of Things: Mapping The Value Beyond The Hype", (2015), https://www.mckinsey.de/sites/mck_files/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf
[16] Lopez Research, "An Introduction to the Internet of Things (IoT)", (2013), http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
[17] Essential Guide, "IoT analytics guide: Understanding Internet of Things data" ,(2015), http://searchbusinessanalytics.techtarget.com/essentialguide/IoT-analytics-guide-Understanding-Internet-of-Things-data
[18] Dave Evans, White paper on, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything", (2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[19] Technology & Communications, "The Internet of Things-A Study in Hype, Reality, Disruption, and Growth",(2014), http://www.vidyo.com/wp-content/uploads/The-Internet-of-Things-A-Study-in-Hype-Reality-Disruption-and-Growt....pdf
[20] "The Internet of Things-Research Study", (2015), http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf
[21] P.B.Pathak, "Internet of Things: An Overview of the Emerging Technology", IJNRCSSE, Vol. 3, Issue 1, pp: (167-170), Month: January-April (2016)