International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Accustoms of IOT and Security Concerns

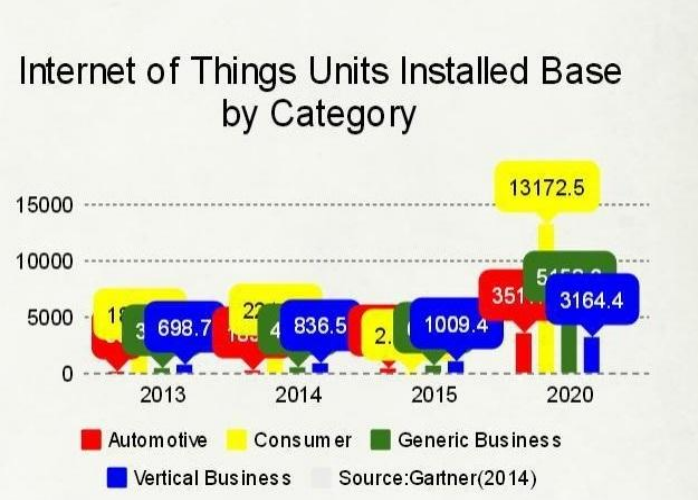
Raxit Solanki

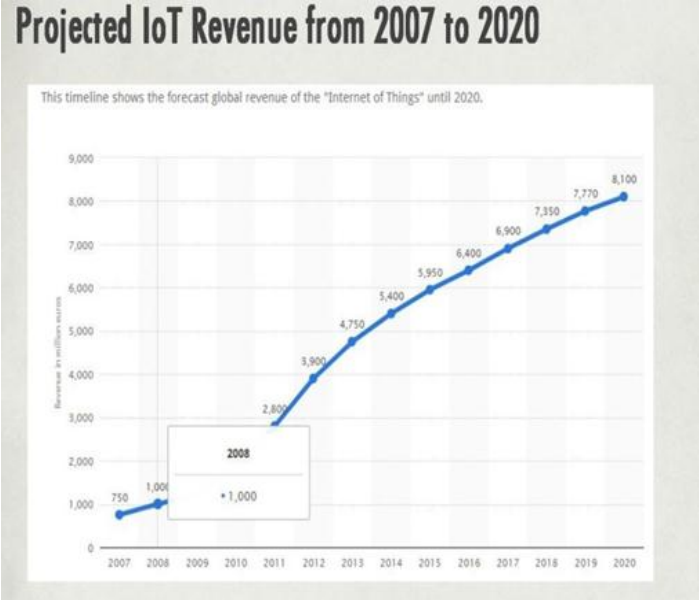
B.tech Information Technology, U.V.Patel College of Engineering.

Abstract – *IOT(Internet of things) is rapidly burgeoning field of modern era of computing. IOT products can be classified broadly into five different categories: smart wearable, smart home, smart city, smart environment, and smart enterprise. The IOT products and solutions in each of these markets have different characteristics, which will be further explained in quotidian manner. Security vulnerabilities are explained in accordance with results of survey of Gartner, Inc. (NYSE: IT) which is information technology research and advisory company, and solicitous to deliver the technology-related insight. In addition, few of the upshots are from Forbes as well.*

1.INTRODUCTION

A formal definition for IOT could be "network of physical devices, vehicles, buildings and other items embedded with sensors, software, actuators and network connectivity, enabled those devises or objects to exchange or collect data" IOT provides instance of generalization of cyber physical systems, which also encompasses technologies such as smart grids, smart phones, intelligent transportation, smart cities etc., and it is expected to provide wide variety of services that goes beyond just machine to machine communication, and covers a wide variety of protocols, domains and applications. Interconnection of automation will be engendered in nearly all fields. In, IOT, we can refer to wide variety of devices, like heart monitoring implants, bio chip transponders on farm animals, electric clams in coastal waters, automobiles with built in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist firefighters in search and rescue operation. one can view IOT as inextricable mixture of hardware, software, data and services. Expansion of Internet-connected automation into a plethora of new application areas, IOT is also expected to generate large amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IOT is one of the platforms of today's Smart City, and Smart Energy Management Systems. According to Gartner, Inc. there will be nearly 20.8 billion devices on the internet of things by 2020, where as ABI Research estimates that more than 30 billion devices will be wirelessly connected to the internet of things by 2020, which has a potential transformational effect on the data center market, its customers, technology providers, technologies, sales and marketing models, and it is predicted by Gartner that the revenue growth will be incremented drastically.





2. Inception

As of 2013, the vision of the internet of things has evolved due to a convergence of multiple technologies, ranging from wireless communication to the Internet and from embedded systems to micro-electromechanical systems (MEMS). This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the internet of things. The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IOT. In 1994 Reza Raji described the concept in *IEEE Spectrum*as "movement of small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The concept of the internet of things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Center) as a prerequisite for the internet of things at that point. If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the *tagging* of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital water making.

3. Evolvement of security

Security controls have evolved in parallel to network evolution, from the first packet-filtering firewalls in the late 1980s to more sophisticated protocol- and application-aware firewalls, intrusion detection and prevention systems (IDS/IPS), and security incident and event management (SIEM) solutions. These controls attempted to keep malicious activity off of corporate networks and detect them if they did gain access. If malware managed to breach a firewall, antivirus techniques based on signature matching and blacklisting would kick in to identify and remedy the problem. Later, as the universe of malware expanded and techniques for avoiding detection advanced, whitelisting techniques started replacing blacklisting. Similarly, as more devices started coming onto corporate networks, various access control systems were developed to authenticate both the devices and the users sitting behind them, and to authorize those users and devices for specific actions. More recently, concerns over the authenticity of software and the protection of intellectual property gave rise to various software verification and attestation techniques often referred to as trusted or measured boot. Finally, the confidentiality of data has always been and remains a primary concern. Controls such as virtual private networks (VPN) or physical media encryption, such as 802.11i (WPA2) or 802.1AE (MACsec), have developed to ensure the security of data in motion.

4. Apprehension of IOT

Gartner has identified the following potential challenges in IOT as whole,

Security — The increasing digitization and automation of the multitudes of devices deployed across different areas of modern urban environments are set to create new security challenges to many industries.

Enterprise — significant security challenges will remain as the big data created as a result of the deployment of myriad devices will drastically increase security complexity. This, in turn, will have an impact on availability requirements, which are also expected to increase, putting real-time business processes and, potentially, personal safety at risk.

Consumer Privacy — As is already the case with smart metering equipment and increasingly digitized automobiles, there will be a vast amount of data providing information on users' personal use of devices that, if not secured, can give rise to breaches of privacy. This is particularly challenging as the information generated by IOT is a key to bringing better services and the management of such devices.

Data — the impact of the IOT on storage is two-pronged in types of data to be stored: personal data (consumer-driven) and big data (enterprise-driven). As consumers utilize apps

and devices continue to learn about the user, significant data will be generated.

Storage Management — the impact of the IOT on storage infrastructure is another factor contributing to the increasing demand for more storage capacity, and one that will have to be addressed as this data becomes more prevalent. The focus today must be on storage capacity, as well as whether or not the business can harvest and use IOT data in a cost-effective manner.

Server Technologies — the impact of IOT on the server market will be largely focused on increased investment in key vertical industries and organizations related to those industries where IOT can be profitable or add significant value.

Data Center Network — Existing data center WAN links are sized for the moderate-bandwidth requirements generated by human interactions with applications. IOT promises to dramatically change these patterns by transferring massive amounts of small message sensor data to the data center for processing, dramatically increasing inbound data center bandwidth requirements.

IOT threatens to generate massive amounts of input data from sources that are globally distributed. Transferring the entirety of that data to a single location for processing will not be technically and economically viable. The recent trend to centralize applications to reduce costs and increase security is incompatible with the IOT. Organizations will be forced to aggregate data in multiple distributed mini data centers where initial processing can occur. Relevant data will then be forwarded to a central site for additional processing.

Wind River published a white paper on IOT security in January 2015, and the report starts off with a sobering introduction. Titled Searching For the Silver Bullet, it summarizes the problem in just three paragraphs, which can be further condensed into a few points as:

- Security must be the foundational enabler for IOT.
- There is currently no consensus on how to implement security in IOT on the device.
- A prevalent, and unrealistic, expectation is that it is somehow possible to compress 25 years of security evolution into novel IOT devices.
- There is no silver bullet that can effectively mitigate the threats

U.S. Federal Trade Commission (FTC) chairwoman, Edith Ramirez, addressed the Consumer Electronics Show in Las Vegas, warning that embedding sensors into everyday devices, and letting them record what we do, could pose a massive security risk. Ramirez outlined three key challenges for the future of IOT:

- Ubiquitous data collection.
- Potential for unexpected uses of consumer data.
- Heightened security risks.

5.Security Concerns

In a quotidian pattern we can simulate and exemplify the security concerns in following types.

Unauthorized access: it is one of the most challenging security concern in IOT, as there are a number of reported issue of security breach by unauthorized access. There are reports showing that insulin pumps can be hacked remotely to deliver deadly doses of the medicine in question or skip scheduled injections. Moreover, a series of experiments has proven that a car's internal computer network can be accessed through a built-in telematics unit without even physically touching the car. Another example is of innocuous USB wall chargers that crack Microsoft wireless keyboard and then send the data wirelessly to the attacker's device. As one HP study proves by revealing 250 security defects in ten commonly utilized IOT appliances—such as web cameras, TVs, home alarms, door locks, and thermostats—security features embedded in IOT devices are not good enough. Some of them have weaker factory-made authentication features that immediately expose them to security threats. In fact, either 8 out of 10 of these "things" failed to set up stronger password authentication than "1234" or the password given by the manufacturer by default is never changed at all. Passwords are the lowest hanging fruit when it comes to authentication, and many IOT devices rely on it. Most of the IOT devices, moreover, have a limited user interface, with no keyboards or screens, which in turn makes the implementation of password authentication system weak by default. That is why smart appliances can be susceptible to brute-force or dictionary attacks

Encryption : In 2014, an Israeli security firm uncovered a critical vulnerability in a telematics device developed by Zubie – a U.S.-based connected-car startup. The research team found that Zubie's hardware, which tracks a car's performance to provide drivers with instructions on improving driving efficiency, did not encrypt

communications between the device and server. Researchers were able to demonstrate how hackers could exploit this weakness to send malicious updates to the device, steal data on the car's location and performance, and even unlock doors remotely. Another study of nine video baby monitors, conducted by Rapid7 senior security consultant Mark Stanislav, identified several common security issues and 10 new vulnerabilities: a lack of encryption for communications and data storage, the availability of a command-line interface on a network port and backdoor accounts with weak passwords, backdoor credentials, cross-site scripting, authentication bypass, and privilege escalation. A couple of researchers from Florida International University who proved in 2013 that the Fitbit fitness tracker was vulnerable to various security attacks, and even unsophisticated toolkits could eventually capture data from any such fitness device within 15 feet, simply because the device was not created with security in mind (it used plain HTTP in its communications). In short, because of the small size, low power and computational incapacity of such devices, it is difficult to add security measures like encryption. The U.S. Federal Trade Commission (FTC) chairwoman, Edith Ramirez, who addressed the Consumer Electronics Show in Las Vegas earlier this year, likewise confirmed that "the small size and limited processing power of many connected devices could inhibit encryption and other robust security measures." Processing power is needed to support more secure measures for data transmission, such as encryption. To explain this point, The Article 29 Data Protection Working Party, a prominent advisory organization in the EU (henceforth "the Working Party"), announced that most sensors today "are not capable of establishing an encrypted link because of the priority given to the physical autonomy of the device or to cost control."

Updates and patches : Connected devices need to be updated on a regular basis in order to remain immune at least to extremely unsophisticated cyber-threats. The risk of cyber-attacks increases if patches are not updated frequently. Most of the companies provide remote updates for their smart devices. One of the potential reasons for that, one is lack of economic incentives to give continuous support, due to which the companies will leave the IOT product unsupported and with numerous security vulnerabilities. For some instance the underlying issue is the lack of communication channel for company to remotely deliver the security patches, because it is more convenient for the companies to let the user download and install the consumers download and update security patches manually. Seen from the consumers' point of view, however, this may not work well for them because some of them experience difficulties installing the updates, or may not be at all aware of their existence in the first place. another weakness in the presence of unpatched vulnerabilities is that they can be indexed by specialized search engines. Even when customers are familiar with the existence of vulnerabilities, they may not be able to access the vendor's updates due to hardware limitations or technologies that are out of date and prevent the device from providing support to software updates. This is why automated firmware update on every device is a chronic issue.

Lack of experience : Designing secure IOT products requires a bundle of multiple skills that would consider the app, device, and entire infrastructure, without leaving out the communication channel of security. The shortage of experienced security experts specializing in IOT tech trends is the main obstacle in creating secure environment for all those elements enumerated above, according to 35% of the respondents in a study. New entries may not have the experience to cope with security problems in IOT, but it is also possible that experienced IOT manufacturers may find it hard to keep up with the rapid tempo of the new digital revolution. As a result, security concerns are overlooked by current IOT manufacturers.

6. Conclusion

Considerably, there weren't that many security debacles reported by IOT, and in turn it is also a fact that we don't see that many headlines about security fiasco of IOT in news or any means of communication source. There are humongous numbers of android wear available in consumable market, how many security breach headlines we have heard about them, only a few. IOT is burgeoning at lightning speed, indeed it is a fact that there are few loopholes related to security in most common IOT technology, but manufacturers have become more solicitous regarding the security concerns, and will be able to troubleshoot sooner or later in future. Possible consideration are likely to be, Methods for secure by design IOT, Methods for IOT security analysis and audit, Privacy techniques in IOT, Secure cloud of things, Trust management architectures, Lightweight security solutions, Authentication and access control in IOT, Identification and biometrics in IOT, Liability and policy

enforcement in IOT, Virtualization and auto-immunity of smart objects, Security of Big data in IOT, Cyber physical systems security, Cyber attacks detection and prevention, Ethics and legal considerations in IOT.

REFERENCES

[1] AFCEA (2015). The security implications of the Internet of Things Available at http://www.afcea.org/mission/intel/documents/InternetofThingsFINAL.pdf

[2] Drozhzhin, A. (2015). Internet of Crappy Things. Available at https://blog.kaspersky.com/internet-of-crappy-things/7667/

[3] inch, B., Polidora, R., Meyer, C., Lutz, L. & Shecter, P. How to Fail in the Internet of Things. Available at http://www.pillsburylaw.com/siteFiles/Publications/AlertFeb2015PrivacyHowtoFailintheInternetofThings.pdf

[4] O'Brien, D. (2014). The Internet of Things: New Threats Emerge in a Connected World, SYMANTEC. Available at www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world

[5] Wired.com (2014). The Internet of Things Is Wildly Insecure — And Often Unpatchable. Available at http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

[6] White paper of, Wind River Systems, SECURITY IN THE INTERNET OF THINGS, Available at http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf