SPIoT: Security & Privacy Concerns on Internet of Things

Parth I Patel
Department of Computer Engineering
Vadodara Institute of Engineering, Vadodara, India

Abstract— IoT can interconnect billions of devices (such as smartphones, sensors and alternative networking devices), to speak with one another. The IoT is the collection of devices, people and services to interconnect and exchange information and useful data. IoT may be a system wherever objects embedded with detector technology to act with one another over wireless communication medium to come up with, exchange and transfer knowledge without human interaction. This interconnection is relevant in many ways like timely coordination with many simple devices and due to open and heterogeneous nature of these networks; they are highly prone to vulnerable attacks. As IoT systems will be ubiquitous and pervasive, a number of security and privacy issues will arise. So privacy and security is the biggest concern in this technology. It covers privacy and security concerns in different segments like web interface vulnerabilities, device connections, spamming, data storage issues, IoT network related problems and many privacy preserving mechanisms. The goal of this paper to present the privacy and security problems that IoT environment is facing and existing mechanisms to protect it. For Internet of Things, credible, economical, efficient and effective security and privacy are required to ensure exact and accurate confidentiality, integrity, authentication, and access control, among others.

Key words: Internet of Things, Sensors, Attacks, Security, Privacy

I. INTRODUCTION

The Internet of Things will consist of billions of individuals, individual devices, and services that can interconnect to exchange data and useful information. Moreover, IoT represents a broader move to the vision of pervasive or universal computing [2].Current industrial trends aim to "connect the unconnected". Presently crucial applications such as modern vehicles and latest infrastructures are the interconnection of devices [3].It is estimated that by 2020 IOT environment will comprise of 26 billion devices [4]. IoT is a platform to interconnect the network of several objects such as radio frequency identification (RFID) tags, sensors, actuators, mobile phones, thermometers and other similar devices [5].In Over the past few years, domain of production engineering, automation and intelligent computational systems has integrated into Internet of Things[3].However, several systems at their initial stages are aiming at this wider vision. The large number of insecure IoT devices with heterogenous nature and high computational power make them an easy and attractive target for attackers seeking to compromise these devices Safety is the major concern in the IoT business opportunities.

There is an alarming rise of hacks and breaches contributing to the vulnerabilities within the IoT. [6].In November, Symantec researchers discovered the Linux.Darlloz worm, which exploited a PHP vulnerability to propagate to IoT devices such as home routers,TV set-top boxes, security cameras, printers, and industrial control systems. In January2014, a variant of the worm was found to include a cryptocurrency mining tool etc. [7].In September 2016, a Mirai-based attack against the French webhost OVH broke the record for the largest recorded DDoS attack—at least 1.1Tbps, and perhaps as large as 1.5Tbps [8]. Hackers also use Distributed Denial of Service Attacks (DDoS) attacks in order to prevent legitimate users from accessing the service of a provider.The primary objective of this attack is to flood the network with false service requests of the server, thus depriving the service to the legitimate requests [9].An IoT botnet built from the Mirai malware— perhaps the largest botnet on record—was responsible for a - 600 Gbps attack targeting Brian Krebs's security blog (krebsonsecurity.com) [10]. According to a survey conducted by Capgemini, 71% of respondents in the survey agreed that security concerns has influenced customers' decision for purchasing IoT products.

The IoT vision is to revolutionize the Internet, to create networks of billions of wireless identifiable objects and devices, communicating with each other anytime, anyplace, with anything and anyone using any service. The increasing enhanced processing capabilities of RFID technologies, wireless sensor networks (WSNs) and storage capacity at lower cost may create a highly decentralized common pool of resources interconnected by a dynamic system of networks [11].

II. PRIVACY AND SECURITY THREATS IN IOT

The three core issues with the IoT are privacy for humans, confidentiality of business processes and third-party dependability. It is acknowledged that in the IoT setting, there are four interconnected, interacting components (people, objects, software and hardware) that communicate over public, untrusted networks. These are bound to be confronted with security, privacy and open trust problems. Therefore, questions regarding users, servers and trusted third parties, as discussed in [25] must be addressed. In such situation, security can be defined as an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures required to protect individual system assets as well as the system as a whole against any deliberate or unintentional threat. All these interactions must also be secured by one means or another, to ensure data and service provisioning of all significant parties and restrict the amount of incidents that will influence the entire IoT. Data diversity and data volume are two factors that characterize the IoT technologies. In order to preserve privacy economical algorithmic schemes and protocols has to be implemented, in numerous devices, and in a very nice range of applications. Firmware tampering is run above the hardware and it is made usable.

A. IoT Architecture

Implementing IoT necessitates an open architecture based on several layers to maximize interoperability among heterogeneous systems and distributed resources. There are various research articles on studies of different IoT architecture instances. The application layer is responsible for data utilization in applications. In another example, in [14] Chen and others indicated that IoT architecture can be primarily divided into three layers: the perception layer, which assumes information collection, the network layer, for information transmission, and the application layer to realize recognition and perception between objects and objects, and people and objects, and to perform an intelligence function[11].

B. IoT Web Interfaces

Most of the IoT devices might have web interfaces that have to be connected to information servers [16]. One among the most important security threats for such systems is SQL injection and cross website scripting that may impact the web interfaces.SQL injections (SQLi) happens when a hacker enters SQL code in a field (like an symbol, a countersign or just about something which will be processed by a SQL database) which will later be used – unchanged – by the application's SQL engine. This can cause privileges escalations, account enumerations, etc[17,18].A Cross website Scripting (XSS) is that the executes a vulnerable script – that originated from the hacker and was sent back by the application – by the web browser of the victim. Such attack is accustomed send the victim to a different website, and force the victim participate in a DDoS attack or pirates the user's session. [19].

C. Attacks on user privacy

Eavesdropping and passive monitoring: This is most common and easiest form of attack on data privacy. If messages are not protected by cryptographic mechanisms, an adversary could easily understand the content. Traffic analysis: In order to effectively attack privacy, eavesdropping should be combined with traffic analysis. Through effective traffic analysis, an adversary can identify certain information with special roles and activities in IoT devices and data. Data mining: This enables attackers to discover information that is not anticipated in certain databases. This could be a security and privacy issue in IoT[11].

D. IoT Network Services

IoT device network services are another way to attack these systems. Inability to use the legitimate requests is the main root of Distributed Denial of Service attack (DDoS).This attack can be launched using botnets. A botnet is a robot network of compromised machines, or bots, that run malicious software under the command and control of a botmaster. These machines have a wide range of nefarious purposes including email spam delivery, distributed denial -of-service (DDoS) attacks, password cracking, key logging, and crypto currency mining.

E. Security and Privacy Challenges in the IoTs

The Internet of Things is a multi-domain environment with a large number of devices and services connected together to exchange information. Each domain can apply its own security, privacy, and trust requirements. In order to establish more secure and readily available IoT devices and services at low cost, there are many security and privacy challenges to overcome. Among those challenges are:

1) User privacy and data protection: Privacy is an important issue in IoT security on account of the ubiquitous character of the IoT environment. Things are connected, and data is communicated and exchanged over the internet, rendering user privacy a sensitive subject in many research works [10, 41]. Although an abundance of research has already been proposed with respect to privacy, many topics still need further investigation. Privacy in data collection, as well as data sharing and management, and data security matters remain open research issues to be fulfilled [42].
2) Authentication and identity management: Authentication and IdM are a combination of processes and technologies aimed at managing and securing access to information and resources while also protecting things profiles. IdM uniquely identifies objects, and authentication entails validating the identity establishment between two communicating parties [43]. It is essential to consider how to manage identity authentication in the IoT, as multiple users and devices need to authenticate each other through trustable services. Many such open research issues have been presented, for instance in [17]. In order to identify all things uniquely, an efficient identity management approach should be defined. Mobility, privacy, pseudonimity, and anonymity aspects require deeper analysis and research [42].
3) Trust management and policy integration: When a number of things communicate in an uncertain IoT environment, trust plays an important role in establishing secure communication between things. Two dimensions of trust should be considered in IoT: trust in the interactions between entities, and trust in the system from the users perspective [34]. In order to gain user trust, there should be an effective mechanism of defining trust in a dynamic and collaborative IoT environment.

The main objectives of trust research in the IoT framework are the following: first, the conception of new models for decentralized trust; second, the implementation of trust mechanisms for cloud computing; third, the development of applications based on node trust (e.g., routing, data aggregation, etc.) [42]. Trust evaluation must be automated and preferably autonomous. There are many proposals for automated trust evaluation, and one of the more interesting is the reputation-based Subjective Logic (SL) approach [44]. The SL approach even permits negative trust (distrust), which is a useful abstraction when communicating trust with human users. Within managed IoT systems it is anticipated for the IoT management entity to be a trust hub for all managed devices. Trust may be transitive between systems but needs to be subject to agreements. One model that potentially works out is the roaming agreement model found in cellular systems, whereby a subscriber can use services in other networks provided that the operators have a roaming agreement in place. Trust will ultimately necessitate a foundation, one element of which is trustworthiness. In our context, a trust device must be able to avoid subversion. The

paper "Reflections on Trust in Devices"[45] further investigates trust in devices from a human perspective and provides critical analysis on the limits of trust in software and hardware. In a post-Snowdon context, this provides food for thought. A good policy framework is desired to incorporate the evaluated trust level and current threat level prior to decision making.

4) Authorization and access control: Authorization enables determining if the person or object, once identified, is permitted to have the resource. Access control means controlling access to resources by granting or denying according to a wide range of criteria. Authorization is typically implemented through the use of access controls. Authorization and access control are important in establishing a secure connection between a number of devices and services.
5) End-to-End security: Security at the endpoints between IoT devices and Internet hosts is likewise important. Applying cryptographic schemes for encryption and authentication codes to packets is not sufficient for resource-constrained IoT. For complete end-to-end security, the verification of individual identity on both ends, protocols for dynamically negotiating session keys and algorithms must be securely implemented.

In IoT with end-to-end security, both ends can typically rely on the fact that their communication is not visible to anyone else, and no one else can modify data in transit. Correct and complete end-to-end security is required, without which, many applications would not be possible.

6) Attack resistant security solution: There are diverse types of devices with different amounts of memory and limited computation resources that are connected to the internet of things. Since these devices are susceptible to attacks, there should be attack-resistant and lightweight security solutions available. Mitigation planes should be provided on devices to tackle external attacks, such as denial-of-service, flood attacks, etc.

III. Cryptographic approaches

Current cryptographic models and security schemes are based on widely adopted encryption algorithms, and privacy standards. Confidentiality is guarded in most of the cases with Advanced Encryption Standard (AES) [35]. The asymmetric algorithm RSA serves for asymmetric encryption, digital signatures, as well as for key management. This is designed for general purpose uses, and their functionality is based on significant processing power, good memory resources, and power availability. Since the applicability of these cryptographic models and security schemes is a little bit unclear, detailed analysis is needed, in order to be assure that they can be implemented in the specified resources of IoT In order to achieve better results, research is still in progress for more flexible cryptographic approaches. Special interest has been attracted by the security schemes of combined mode, that supports probably encryption and authentication [36].Nowadays, more suitable encryption algorithms are under investigation each time, based on the available resources of IoT devices.

IV. A longer term IOT security strategy

Defenses against botnets can be broadly categorized into preventing, monitoring and response. Preventing bot infections is the most effective defense. This can be accomplished through antivirus software complemented by intrusion- prevention systems, firewalls, content filtering and inspection technologies, and application whitelisting. User awareness is also critical, as malware often spreads because of user mistakes, such as clicking on email attachments. However, machines can become infected despite the use of security techniques. It's therefore critical to monitor network and device behaviour for anomalous events or trends that might indicate the presence of a threat. Network behaviour analysis (NBA) programs—which can be installed and operated by administrators or provided by third-party service continuously monitor data flows from routers and other sources and flag departures from established baselines for traffic volume, bandwidth use, protocol use, and other metrics. If signs of a potential DDoS attack or infected machine are detected, a prompt response is critical to minimize damage and prevent the malware from spreading. Responses can vary from simple actions such as disconnecting a suspect machine from the network to tracking, analyzing, and taking down botnets [20].

V. Conclusion

The main goal of this paper was to provide an explicit survey of the most important aspects of IoT with particular focus on the vision and security challenges involved in the Internet of Things. IoT is an emerging technology and significant progress that has been made in the standardization of the technology. Yet understanding the combination of techniques and tools should be used to protect Iot systems. IoT systems include heterogenous data spread across different system boundaries. The paper, reviews the major privacy challenges in Iot by identifying different areas which are sensitive to security attacks. Later the discussion is about the recent privacy preserving techniques. As future perspective to protect IoT, better security frameworks are required to be developed which can address the privacy issues across all boundaries. Further research is required to develop and design appropriate security mechanisms that are resilient to different types of attacks. So users, organizations and developers have to come under one roof and find a prominent solution for a secured IoT environment. Numerous difficulties and challenges related to IoT are still being faced. Challenges like assuring interoperability, attaining a business model in which hundreds of millions of objects can be connected to a network, and security and privacy challenges, such as authentication and authorization of entities are introduced.

References

[1] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, David Eyers,"Twenty Security Considerations for Cloud-supported Internet of Things"IEEE Internet of things Journal,Vol 3,No 3, June 2016.
[2] M. Weiser, "Ubiquitous computing," Computer, vol. 26, no. 10, pp. 71– 72, 1993.

[3] Ahmad-Reza Sadeghi1, Christian Wachsmann2; Michael Waidner1,3,"Security and Privacy Challenges in Industrial Internet of Things" DAC '15, June 07 - 11, 2015, San Francisco, CA, USA Copyright 2015 ACM ACM 978-1-4503-3520-1/15/06 ...$15.00 http://dx.doi.org/10.1145/2744769.2747942
[4] Gartner.com, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", December 2013.
[5] Sudip Misra,P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena, Mohammad S. Obaidat,2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing"A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things".
[6] Capgemini Consulting and Sogeti High Tech Interview,www.capgemini-consulting.com.
[7] S.K. Bansal, "Linux Worm Targets Internet-Enabled Home Appliances to Mine Cryptocurrencies," The Hacker News, 19 Mar. 2014; thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html.
[8] US Computer Emergency Readiness Team, "Heightened DDoS Threat Posed by Mirai and Other Botnets," alert TA16-288A, 14 Oct. 2016 (revised 30 Nov. 2016); www.us-cert .gov/ncas/alerts/TA16-288A.
[9] Peeha Machaka,Antoine Bagula,Fulufhelo Nelwamondo,"Using Exponentially Weighted Moving Average Algorithm to Algorithm to Defend Against DDoS Attacks" in 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech) Stellenbosch, South Africa.
[10] D.Goodin,"Record-Breaking DDoS Reportedly Delivered by >145K Hacked Cameras," Ars Technica, 28 Sept. 2016; arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest -ddos-ever.
[11] Mohamed Abomhara, Geir M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues", IEEE, 2016.
[12] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," IEEE Commun Surveys Tuts, Vol 11, no. 2, pp. 52–73, 2009.
[13] S. K. R. H. R. S. O. Garcia-Morchon, S. Kumar, "Security considerations in the ip-based internet of things draft garcia-core-security-06," https://tools.ietf.org/html/draft-garcia-core-security-06, Sep. 2013.
[14] The OWASP Foundation, "Owasp internet of things top ten project," https://www.owasp.org/index.php/OWASP Internet of Things Top Ten Project.
[15] "ISO/IEC 27000:2014 – Information technology – Security techniques – Overview and vocabulary."
[16] "How safe are home security systems?" Mar. 2015.

