Security Concerns of Internet of Things (IoT)

P.SAI CHAITANYA
ASSISTANT PROF ,KITS(S)
ECE DEPARTMENT

N.KARTHIK
ASSISTANT PROF ,KITS(S)
ECE DEPARTMENT

P.CHAITANYA
ASSISTANT PROF KITS(S)
ECE DEPARTMENT

Abstract: The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders .Internet of Things (IoT) has been a major research topic for almost a decade now, where physical objects would be interconnected as a result of convergence of various existing technologies. IoT is rapidly developing; however there are uncertainties about its security and privacy which could affect its sustainable development. This paper analyzes the security issues and challenges and provides a well defined security architecture as a confidentiality of the user's privacy and security which could result in its wider adoption by masses.

Keywords - internet of things; security; privacy; confidentiality.

Introduction:
As the Internet of Things (IoT) continues to gain traction and more connected devices come to market, security becomes a major concern. Businesses are increasingly being breached by attackers via vulnerable web-facing assets1 ; what is there to keep the same from happening to consumers? The short answer is nothing. Already, broad-reaching hacks of connected devices have been recorded2 and will continue to happen if manufacturers do not bolster their security efforts now. In this light, Vera code's research team examined six Internet-connected consumer devices and found unsettling results. We investigated a selection of always-on consumer IoT devices to understand the security posture of each product. The result: product manufacturers weren't focused enough on security and privacy, as a design priority, putting consumers at risk for an attack or physical intrusion.
Building upon the concept of Device to Device (D2D) communication technology of Bill Joy [1], Internet of Things (IoT) embodies the concept of free flow of information amongst the various embedded computing devices using the internet as the mode of intercommunication. The term "Internet of Things" was first proposed by Kevin Ashton in the year 1982 [2]. With the aim of providing advanced mode of communication between the various systems and devices as well as facilitating the interaction of humans with the virtual environment, IoT finds its application in almost any field. But as with all things using the internet infrastructure for information exchange, IoT to is susceptible to various security issues and has some major privacy concerns for the end users. As such IoT, even with all its advanced capabilities in the information exchange area, is a flawed concept from the security viewpoint and proper steps has to be taken in the initial phase itself before going for further development of IoT for an effective and widely accepted adoption.

Generic Architecture:
Generally, IoT has four main key levels as shown

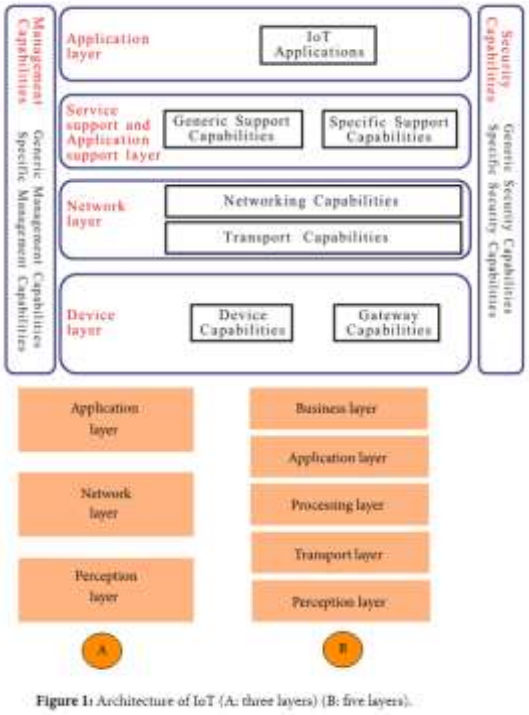

Figure 1: Architecture of IoT (A: three layers) (B: five layers).

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers.

SECURITY GOALS

The major security goals of IoT are to ensure proper identity authentication mechanisms and provide confidentiality about the data etc. The Security triad or CIA triad, a distinguished model for the development of security mechanisms, implements the security by making use of the three areas which are Data confidentiality, integrity and availability as shown in the Fig. 2. A breach in any of these areas could cause serious issues to the system so they must be accounted for. The three areas are described below:

Data Confidentiality

Data confidentiality is identical to providing freedom to user from the external interference. It is the ability to provide confidence to

user about the privacy of the sensitive information by using different mechanisms such that its disclosure to the unauthorized party is prevented and can be accessed by the permitted users only. There are many security mechanisms to provide confidentiality of the data including, but not limited to, Data Encryption in which the data is converted into cipher text form which makes it difficult to access for the users having no proper authorizations, the Two step verification, which provides authentication by two dependent components and allows the access only if both the components pass the authentication test and the most common Biometric Verification in which every person is uniquely identifiable. For the IoT based devices, it ensures that the sensor nodes of the sensor networks don't reveal their data to the neighbouring nodes; similarly the tags don't transmit their data to an unauthorized reader .

Data Integrity

During the communication, data could be altered by the cybercriminals or could be affected by various other factors that are beyond human control including the crash of server or an electromagnetic disturbance. Data Integrity refers to the protection of useful information from the cybercriminals or the external interference during transmission and reception with some common tracking methods, so that the data cannot be tampered without the system catching the threat [13]. The methods to ensure the accuracy and originality of data include methods like Checksum and Cyclic Redundancy Check (CRC) which are simple error detector mechanisms for a portion of data. Moreover, continuous syncing of the data for backup purposes and the feature like Version control, which keeps a record of the file changes in a system to restore the file in case of fortuitous deletion of data can also ensure the integrity of data such that the data on IoT based devices is in its original form when accessed by the permitted users.

Data Availability

One of the major goals of IoT security is to make data available to its users, whenever needed. Data Availability ensures the immediate access of authorized party to their information resources not only in the normal conditions but also in disastrous conditions. Due to dependency of companies on it, it is necessary to provide firewalls to countermeasure the attacks on the services like Denial of service (DoS) attack which can deny the availability of data to the user-end. Data Availability also ensure the prevention of bottleneck situations which prevent the flow of information. The Redundancy and Failover backup methods provide duplication of the system components in conditions of system failure or various system conflictions to ensure reliability and availability of data.

Security Threats in the Smart Home

Threats Although the Smart Home is a very different environment, the overall nature of security threats is similar to other domains. Confidentiality threats are those that result in the unwanted release of sensitive information. For example, confidentiality breaches in home monitoring systems can lead to the inadvertent release of sensitive medical data. Even seemingly innocuous data, such as the internal home temperature, along with knowledge of the air conditioning system operation parameters, could be used to determine whether a house is occupied or not, as a precursor to burglary. Loss of confidentiality in things such as keys and passwords will lead to unauthorized system access threats. Authentication threats can lead to either sensing or control information being tampered with. For example, unauthenticated system status alerts might confuse a house controller into thinking that there is an emergency situation and opening doors and windows to allow an emergency exit, when in fact allowing illicit entry. One issue that will be raised later is automated software updates—if these are not appropriately authenticated problems can arise. Access threats are probably the greatest threats. Unauthorized access to a system controller, particularly at the administrator level, makes the entire system insecure. This can be through inappropriate password and key management, or it could be by unauthorized devices connecting to the network. Even if control cannot be gained, an unauthorized connection to a network can steal network bandwidth, or result in a denial of service to legitimate users. Since many Smart Home devices may be battery operated and wirelessly networked with a low operational duty cycle, flooding a network with requests can lead to an energy depletion attack—a form of denial of service.

Some Existing Security Support for IoT

Due to their low cost, IoT computing devices generally are not as powerful as traditional desktop and laptop computers. Most IoT devices are low energy, use a low-end microcontroller and have limited memory. Such controllers are well-matched to the requirements of standalone controllers in a washing machine or air conditioner. However, these characteristics have made the move to networked IoT controllers more challenging as the existing Internet protocols are not typically designed for these embedded devices. Several Internet Engineering Task Force (IETF) working groups have been created to tackle these problems. IETF standardization work on IoT has played a vital role in the establishment of the necessary light-weight communication protocols for constrained environments over the existing IP network. These include IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN: RFC 6282) [20], IPv6 Routing Protocol for Low power and Lossy Networks (RPL: RFC 6550) [21] and Constrained Application Protocol (CoAP: RFC 7252) [22]. Figure 2 shows the comparison between IETF IoT and TCP/IP protocol stacks. Once devices are connected to the Internet, any of the security threats on the Internet could also compromise the security and privacy of IoT. In the following sections we review the current security implementations for these standard IoT protocols.

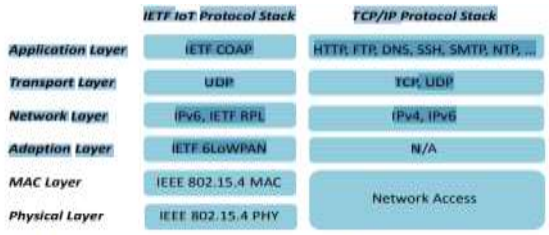

Figure 2. The comparison between IETF IoT and TCPIP protocol stacks.

6LoWPAN and Security:

Electrical and Electronics Engineers (IEEE) has defined the 802.15.4 standard for wireless personal area networks (WPANs). IEEE 802.15.4 defines how the physical and media access control layers should operate under the low-bandwidth, low-cost, low-speed and low-energy conditions typical of these networks. As such, 6LoWPAN is a light-weight protocol designed by the IETF to allow IPv6 packets to be transferred over IEEE 802.15.4 wireless networks.

RPL and Security

Routing protocols are a core component of conventional networks, and this also applies to 6LoWPAN networks. RP is an optimized

IPv6 routing protocol designed by IETF especially for Low power and Lossy Networks (LLNs) and is primarily used by 6LoWPAN networks. RPL is a distance-vector routing protocol, and its mapping topology is based on a Destination-Oriented Directed Acyclic Graph (DODAG) structure. A generic topology authentication scheme called Trust Anchor Interconnection Loop (TRAIL) for RPL has been presented in [26]. TRAIL can prevent the topological inconsistency attacks from spurious nodes by discovering and isolating the forged nodes. A round-trip message has been used by TRAIL to validate upward path integrity to the root node and help the nodes in the tree get genuine rank information. The innovation of TRAIL is that each node in the tree can validate its upward path to the root and detect any fake rank attacks. In the DODAG tree, it is essential for nodes to select their correct parent nodes, since every node except the root must have a parent node. The RPL rank is used to describe a node's position in the tree topology. In [27], the authors present a secure selection scheme to help a child node to choose an authentic parent node. In its selection algorithm, a node's threshold value will be calculated based on average and maximum rank values from its neighbour nodes to exclude spoofing nodes from becoming its parent. So existing solutions can ensure secure routing table generation in Smart Home networks.

CoAP and Security

CoAP [22] is a HTTP-like application layer protocol designed for constrained device networks. As there are some special requirements such as group communications in IoT networks, CoAP provides multicast support which HTTP does not have. To better suit the low-bandwidth connections and low-computational-power device environments, the User Datagram Protocol (UDP) protocol is adopted by CoAP. UDP is a simpler, low-latency and connectionless transport layer protocol compared with its counterpart Transmission Control Protocol (TCP). CoAP is a stateless protocol and is based on the client-server architecture model. It uses request/response-style operations to exchange messages between the client and server. Similar to HTTP, CoAP is also based on a representational state transfer (REST) model, where each resource on the server has its own Uniform Resource Identifier (URI), a client can access a resource by making a request to the server, and the request can be one of these four methods: GET, POST, PUT and DELETE

A Suitable Smart Home Architecture for Security

There have been many different proposals for Smart Home architectures, each of which have particular security issues. Three of the most important and popular architectures are middleware, cloud and gateway architectures. The next sections investigate the security issues and implementation difficulties for these architecture styles. 6.1. Middleware Architectures and Security Middleware is a software layer that sits between the low-level layer of devices and the high-level application layer. It usually provides a common interface and a standard data exchange structure to abstract the complex and various lower-level details of the hardware. When the middleware receives a request from a higher-layer application, it converts the high-level standardized resources access request to the corresponding device-specific methods. When the device responds back to the application, the middleware processes the low-level methods and data transformations, and then sends the related abstract commands and data back to the application. The application does not need to know the underlying details of the different implementations of the hardware, it can just simply invoke the commands and functions provided by the middleware. Security and privacy protection should be considered at all levels of the middleware, from the lower hardware interaction level to the higher common interface level. VIRTUS Middleware [30] is a middleware solution based on the open eXtensible Messaging and Presence Protocol (XMPP) protocol. It adopts the Simple Authentication and Security Layer (SASL) protocol for authentication and the Transport Layer Security (TLS) for data security and privacy. Secure Middleware for Embedded Peer-to-Peer systems (SMEPP) [31] is a middleware focusing on providing peer-to-peer security communication between smart nodes. Before a device can communicate with others, it needs to join a group by providing a valid credential. There are three different security levels, but only level 1 and level 2 take up the security mechanisms. There is no security implementation under level 0. SMEPP implements pre-shared key cryptography under level 1 and public-key cryptography under level 2 for group admission. On the other hand, SMEPP adopts authentication under level 1 and authentication together with encryption approach under level 2 to protect data security. While middleware has been extensively used in corporate systems with desktop-class machines to manage complex heterogeneous networks, currently proposed IoT middleware solutions require substantial additional complex software layers and cryptographic routines to be implemented on devices which have neither the memory nor the computational power to host them.

Cloud Architectures and Security

Collaboration between devices is an important aspect of IoT. Such interoperable functions require high processing power which most IoT devices are not capable of. To solve the performance problem of IoT devices, researchers have proposed cloud-based solutions for IoT. The cloud has the resources to monitor, collect, store and process data from IoT devices. By analyzing this data, the cloud can trigger actions according to user-defined policies to achieve complex Smart Home control. The cloud-based architecture of IoT is also known as the Cloud of Things (CoT).

Gateway Architectures

An IoT gateway is a relatively resource-rich network processor working on the same LAN with the other IoT endpoints. It can not only be a central management point to deal with the coordination of IoT devices, but it can also improve interconnection and interoperability between smart devices from different manufacturers. In addition, it can act as a bridge to connect the local IoT infrastructure to the cloud. Since the gateway has more computing power and resources, high computation and memory-rich tasks can be offloaded from IoT devices to the gateway. In terms of security, the gateway can centralize user authentication and apply access control to guard against unauthorized access or modification of restricted data. It also acts as a firewall to protect the smart devices and privacy from cyber threats, and to reduce the attack surface.

CONCLUSION AND FUTURE WORK

The only hurdle that stands in the way of the IoT development is the security and privacy issues. Security at all the levels of IoT is expository to the functioning of IoT. Luckily, there already have been many research achievements in the IT security concerns and for effective implementation of a security infrastructure for IoT, these achievements must need to be further expanded instead of focusing the attention towards seeking the new possible security solutions, to make IoT able to provide services to the futuristic data-hungry billions of devices with the ability to thwart the adversaries.

So the adequate privacy and security measures through substantial researches must be made and the answers for the number of open questions in this research field must be provided, before it gets deployed in the society. This paper discussed the security goals and possible security challenges and issues of the IoT system. Then a well-defined architecture for the IoT security was presented. In the future, more authentications, risk assessment and intrusion detection techniques in each architectural layer must be explored in parallel to the implementation of the security infrastructure using existing IT security features. Moreover, legal frameworks, proper regulations and policies must be devised to ensure stable development of the secure technologies.

REFERENCES:

[1] Kevin Ashton, That Internet of things thing, It can be accessed at: http://www.rfidjournal.com/articles/view?4986

[2] D. Singh, G. Tripathi, A.J. Jara, A survey of Internet-of Things: Future Vision, Architecture, Challenges and Services, in Internet of Things (WF-IoT), 2014 .

[3] Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717

[4] Rolf H. Weber, "Internet of Things - New security and privacy challenges," in Computer Law and Security Review (CLSR), 2010, pp. 23-30

[5] Rodrigo Roman, Pablo Najera and Javier Lopez, "Securing the Internet of Things," in IEEE Computer, Volume 44, Number 9, 2011, pp. 51-58

[6] Friedemann Mattern and Christian Floerkemeier, "From the Internet of Computers to the Internet of Things," in Lecture Notes In Computer Science (LNCS), Volume 6462, 2010, pp 242-259

[7] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, Security in the Internet of Things: A Review, in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651

[8] Ying Zhang, Technology Framework of the Internet of Things and Its Application, in Electrical and Control Engineering (ICECE), pp. 4109-4112

[9] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, A Multilayer Security Model for Internet of Things, in Communications in Computer and Information Science, 2012, Volume 312, pp 388-393

[10] Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, pp. 257-260

[11] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013.

[12]. Fleming, B. Advances in automotive electronics (automotive electronics). IEEE Veh. Technol. Mag. 2014, 9, 4–19. [CrossRef]

[13]. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Commun. Surv. Tutor. 2011, 13, 584–616. [CrossRef]

[14]. Attaran, M. Critical success factors and challenges of implementing RFID in supply chain management. J. Supply Chain Operat. Manag. 2012, 10, 144–167.

[15]. Zou, Z.; Chen, Q.; Uysal, I.; Zheng, L. Radio frequency identification enabled wireless sensing for intelligent food logistics. Philos. Trans. R. Soc. Lond. A Math. Phys. Eng. Sci. 2014, 372. [CrossRef]

[16.] Ricquebourg, V.; Menga, D.; Durand, D.; Marhic, B.; Delahoche, L.; Loge, C. The Smart Home Concept: Our Immediate Future. In Proceedings of the 2006 1st IEEE International Conference on E-Learning in Industrial Electronics, Hammamet, Tunisia, 18–20 December 2006; pp. 23–28.

[17] Alam, M.R.; Reaz, M.B.I.; Ali, M.A.M. A Review of Smart Homes—Past, present, and future. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) 2012, 42, 1190–1203. [CrossRef]