ISSN: 2455 - 5630
International Journal of Scientific Research and Modern Education
Impact Factor 7.137, Special Issue, March 2020 – Conference Proceedings
International Conference on Rise of Disembedded Unilateral Economy: InnoVision in the Era of Deglobalization (KRUPACON 2019) On 8th & 9th November 2019 Organized By
Krupanidhi Group of Institutions, Bangalore, Karnataka

SECURITY FOR END TO END COMMUNICATIONS IN INTERNET OF THINGS

Bhargavi K* & Chithra S**
* Krupanidhi Group of Institutions, Bangalore, Karnataka
** Krupanidhi Degree College, Bangalore, Karnataka

Cite This Article: Bhargavi K & Chithra S, "Security for End to End Communications in Internet of Things", International Journal of Scientific Research and Modern Education, Special Issue, March, Page Number 12-15, 2020.

Abstract:

This paper attempts to present a multi-layered approach to ensure data transportation from a mobile internet link to a host by way of a mobile network. This approach uses several safety measures that present a verysafe communication solution when completely implemented.

Key Words: Internet of Things, Security, Communication

Introduction:

The exponential development of IoT clarifications leads to biggerworry about safety concerns related to the multitude of computers. The growth of the Internet of Things connected devices is expected to reach 20 trillion by 2020. Many of these solutions use wireless networking to connect to each other. Poor architecture cellular networking can help overcome future security problems. A highly protected architectural solution needs alargely architectural plan for the interface, stretching from the border system to the target host for processing, storage and use in a multi-layered protection approach. Mobile networking strategies provide solutions that can use Ethernet or wireless Wi-Fi and focus on community Internet for information transportation from the host's edge apparatus. There are a variety of vulnerability flaws in these alternatives. The autonomous design of an IoT solution i.e. a system that separately interacts with a host that does not need human intervention and control by definition – provides the rationale for remote observation and monitoring of all useful IoT solutions. Since the essence of data transport is not continuously controlled or triggered by human feedback, interference can arise without human realizing that it does not work as planned with a wireless handheld computer. In particular, there have been many recent security breaches, using a loophole connected to Wi-Fi over the public Internet as a means of accessing data streams and manipulating or changing the features of the IoT system. The multi-level approach discussed here offers a secure wireless link using bundled data as used in 3G and above cellular carrier technologies to create a clear connection between the IoT unit and the bidirectional host. There are a variety of practical components in this technique interlocking, which are explored in this article. Including:

- SIM-based authentication and key agreement,
- Encryption of the radio communication network,
- Custom Access Point name (APN),
- Private non-routing addressing of TCP/IP,
- Tunnel routing scheme which is non-split,
- Point to point data transport host,
- Tracking of host router,
- No direct device to device communication,
- Confirmation and alerting of the SIM toolkit IMEI
- SIM PIN lock

Architectural System Description:

An encrypted radio access network links the IoT cellular infrastructure to a nearby serve cell tower. The local tower is tightly connected to the mobility data centre of the home carrier. The host is linked via an encrypted point-to-point connection.
This architecture has two inherent benefits: 1) the use of standards-based elements so that the solution can be extended to IoT devices off-the-shelf and 2) end-to-end authentication which is obtained without cost-effective over-the-top device host data encryption. When the data stream is encrypted until the edge system is left and the host does not encrypt it offers a more protected layer, this normally costs a higher data output which is calculated per byte or kilobyte in the cellular room. The architecture mentioned in this paper offers the necessary protection without improved safety encryption data payload.This approach allows TCP or UDP data to be shipped in plain texts for several groups of Internet Stuff applications, and its protected architecture offers a suite of practical security elements which can properly connect together to avoid unwanted data access.

The Interlocking Functional Elements:

Each security functional element available in the architecture is briefly described in this section.

A. SIM-Based Authentication and Key Agreement:

The subscriber identification module (SIM) [1] is the first essential feature in the safe architecture. The basic feature of the SIM is to avoid compromise of authentication keys. The SIM is a microprocessor with a variety of hardware security capabilities to avoid destruction by chemical decomposition, x-rays or reverse engineering attempts. In order to avoid forced external irregularities to make the SIM vulnerable to hacked, security processes are added to the SIM I/O pins. The SIM I/O Circuit tracks and disables the SIM if the TX and the RX pins have higher or lower voltages in regard to the supply and ground to allow the I/O Circuit to latch or go in an unpredictable state. In addition, the SIM is being shielded from anomalous feedback and clocking [2]. The on-board microprocessor cannot provide direct access to SIM through the cellular radio module [2] alone. Contact with the SIM is only conducted via the built-in radio stack layer. In this case, the antenna is automatically programmed to search the available Radio Band and to catalogue potential wireless carriers to connect to[3] when the mobile phone, in this case

an Internet of Things unit, is turned on. This method chooses a cellular tower that first fits the mobile network code of its own carrier (MNC). This is achieved by pointing out the radio bands search for radio transmittal codes that fit the IMSI (IMSI) code of the SIM. If a matching operator, including the SIM house carrier, is not found, the radio checks for others and compares it to a list of favorite roaming partners that is revised.

B. Radio Access Network Encryption:

Another safety factor is that the radio connection layer between the node and cell tower of the system is encrypted 128-bit and using the previous key from the regular GSM protocol for 3G and above transmission [4] as part of the overall data transport protection technique.

C. Custom Access Point Name (APN):

The micro processor will launch a TCP/IP data session inside the Things Internet system after authentication of the Internet of Things device with the service cell carrier. The command collection is an extension of a.k.a. AT+ command in the Hayes modem. A radio module is supplied with the AT command, which includes the access point name (APN) that the application needs to use [10], through some variables. The APN module on consumer phones, the APN is a general generic term for any telephone used by the home provider to route consumer information from telephones and tablets to the public Internet. These data packets are normally routed to the public internet through a port address translation (PAT) and then a stateful firewall. While this standard practice is good for user solutions needing access to the wider internet, the Internet of Things architecture poses security vulnerability. A custom APN is allocated to any company client using IoT devices, because of its stable IoT architecture. This personalized APN is exclusive to the organization that produces and operates IoT products. The custom APN requires such a company (and only such company) to permit an IoT computer to access the custom data transport APN of that company.

The following additional authentication function is provided by the use of a special custom APN. While a malicious party could find or speculate the company's customary name for the APN, clearly requiring the APN use the AT command does not permit such a custom APN to be supplied and authenticated. The authorization transfers are based on the process used to ensure that an IoT device requesting the custom APN will use the custom APN in their data transmission. At this stage of the setting up of the data infrastructure, the Gateway GPRS support node (GGSN) or the packet data network gateway is the serving feature of the home carrier network (PDN-GW). GGSN/PDN-GW serves as the broker for data session and features through the link from the IoT system to the mobile data centre and the GGSN/PDNGW portion through the Radio Network. The GGSN/PDNGW path from the Mobility Data Center is also mapped and managed by tailored APN parameters, in which the routing of TCP/IP data packets will go straight from the Mobility Data Center to the Destination Host (to receive, store, etc instead of going to the public internet (user experience). See the following pages for more information.

D. Private Non-Routable TCP/IP Addressing:

The use of private IP addressing, usually a class B 10.x series, is one of the main protected methodologies used to pick and set a personalized APN build. During the data link between the IoT module and the mobility information centre, the GGSN/PDNGW assigns the class B IP address. From the accessible IP addresses, the APN build specifies the dynamically allocated private IP address. The 10.x unroutable IP address for the radio link is retained in the packet, along the path between the IoT radio module and the GGSN/PDN-GW so as to prevent any Network address translation (NAT) or port address translation (PAT). The Private IP address scheme would not route to the public Internet due to the existence of the overall architecture. Given the unfamiliarity of the IP addressing, even though the malicious packet was going to escape" the pipe into the protected pipe, or one IP packet, the first router hop automatically lowered the pipe due to its unfamiliar IP address.The inherent protection of the non-routable IP addressing scheme and the fact that a personalized APN can be developed and supplied only by the intended business offers a highly protected approach that avoids mismanagement with or between data traffic. The program cannot access data accessible via the public internet by using a non-routable IP addressing. For example, an IoT system may have to look at an external information sources in a commercial water sprinkler, for example weather information. The IoT controller will request a weather forecast to decide whether it needs water on a certain day. This IP packet produced as a request outbound by the IoT controller microprocessor would have an IOAA URL that provides an electrically readable meteorological feed. This text would include the protected scheme architecture to the customer's router in the data centre via the device. The packet is addressed to the public destination. After going via the business router and firewall, this public-IP-addressed packet will then be assisted into the public internet.

E. Non-Split Tunnel Routing Schema:

Poor architecture implementations often have an APN slicing the data packet tube. This means that while private data packets of 10.x are sent directly to corporate customers according to previous explanation, public destination packets are routed to the public Internet directly from the mobility data centre. This may be architecture, but it breaks this protection approach, since an IoT system now has a way to the public Internet and is not regulated by the company user.

F. Pointto Point Data Transport between Cellular Carrier and Host:

The points-by-point link between the mobility data centre and the target host may be an IPsec VPN tunnel or an MPLS or frame relay, as well as a variety of secure point-to-point online networking options that the outbound side of the carrier service might provide. The most popular is the IPsec VPN which typically uses both the carrier and the host data sites with Cisco VPN firewalls. Combining all functional elements provided by the customized APN and IPsec VPN tunnels, a closed protected pipe can be created, originating from a radio module throughout the entire tower and via a modified off-the-Internet secure pipe transiting the mobility data centre through the GGSN/PDN-GW.

G. No Direct Device to Device Communication:

It is important to remember that Machine to Machine (M2M) is a standard term for IoT and causes a misconception that IoT machines are communicating with each other directly. Direct device-to-device communication via the carrier or host client is excluded from the technique as defined herein. In reality it's just the application layer that administers IoT solutions in the backend host that receives IoT devise correspondence. In situations where data interchange between IoT device A and IoT device B is needed and required, this purpose can be accomplished via the application layer on the backend server rather than through direct data exchange between the two devices.

This technique, though theoretically feasible, violates the authentication methods mentioned above, while an APN can be designed for device-to-device routing by the carrier's data centre.If IoT devices must connect directly with the operator's data centre, this would not cause the customer's router or backend host system to log or have a footprint. The machines will speak back and forth in other words, without the company customer having registered or seen traffic on an M2M computer, therefore unable to test the traffic for malicious behavior.

H. Destination Host Router Monitoring:

Another intangible advantage of this safe routing system is that the customer's router goes through all the data packets to and from the IoT unit. Deep consumer packet inspection can detect irregular data actions on the IoT devices in real-time, which can suggest illegal or harmful practices. Automatic warning is then used to uninstall the IoT unit and alert technical interference with the supply mechanism. Of the commercially routed data packets were tunneled on the carrier site and then those packets with the 10.x will go into the customer's business router. The customer's host data centre has a holistic vision of all traffic from and through IoT systems, supplying any packet through its customer business router. It can forensically track fraudulent activity.

I. SIM Toolkit IMEI Validation and Alerting:

Once a protected link between your radio module and your backend service host has been created, more physical protection is provided. One already mentioned method of securing cryptographic keys inside is the physical hardware protection found in the SIM feature. The only serial number found inside the radio chipset is a second hardware element. The IMEI or international mobile device identifier is called this. Each wireless system manufacturer is allocated its own specific IMEI range for its product after conducting the necessary PTCRB approval testing. The serial number of the IMEI is 15 digits long, with the manufacturer / commodity code known as the form allocation code in six of the digits representing the special serial number and the corresponding eight digits (TAC). The IMEI will therefore recognize up to 1,000,000 specific units.The IMEI numbers are reported for the members of the PTCRB body in a searchable database.

The make and model of an IoT system can be easily detected by an IMEI code that is contained inside a radio chipset by cellular carriers. The combination of the IMEI and the International Telephone Subscriber Identification (IMSI), the serial number of the SIM, are part of the records that are interchanged between the IoT system radio module and the service provider in authentication. If deceptive conduct is identified with these components, the carrier may use all codes to authenticate, authorize or reject communication services, and to decide if the system is a trustworthy device with the carrier and industry specifically accredited to obtain its exclusive IMEI code chain.

Another special safety feature of the SIM is available. As a microprocessor with executable code space, the SIM runs a variety of protection method programs known to the carrier only. In this paper the technique explains a series of SIM programming that the IMEI of the radio module directly linked to when powered up queries. [2] The SIM is a protected storage space and has either obtained or discovered a first-run copy of the attached IMEI computer. The IMEI(s) are stored in non-volatile memory on the SIM and the SIM asks the same on the radio module and compares the IMEI given on the stored IMEI on the SIM. In the case that all of these are paired, the SIM expects that the equipment should be fitted with the authorized serial number of the hardware, which is safely maintained.

If the SIM notices another IMEI, it could conclude that a suspicious action has taken place and that the physical SIM is taken off the trustworthy device and replaced in the potential malignantappliance. The SIM warns the host mobility data centre that there is a fault in power up and the organization will take urgent action to deactivate the SIM or block data flows before the problem is examined. This note is applied to the business practices of the enterprise client, which provide a strong sign that a SIM has switched to another IoT unit.

J. PIN Locking of SIM:

The IoT system uses the SIM's normal PIN locking mechanism as a security tool [5]. Inside the hardware of the device processor that is operated by hardware, such as the IMEI, a safe hacking algorithm is developed, which allows a specific 4-digit integer. The unlocking key is coded into a locked condition during mounting by the SIM connected to the computer with the special 4 digit code. Using the radio terminal to the computer system, the SIM demands the unlock code. The firmware performs a 4-digit decrypt code hash algorithm and moves into the SIM. The SIM would be allowed for service when the code suits the SIM. If the pin is not aligned after three tries, the SIM will not be used or blocked.

This approach avoids the withdrawal of a SIM from an IoT and its incorporation into a consumer handset.After three unsuccessful attempts the SIM is no longer available, and this pin is demanded in the phone interface by the malicious user. The unblocking series with a coding that is 8-digit, only identified to the vendor of devices that can unblock SIM, becomes indefinitely unworkable if it is improperly administered 10 times [5].

Conclusion:

This article has proposed a multi-stage approach to safely set up TCP/IP Internet end-to-end cellular networks based on UMTS/LTE networking systems. This approach consists of standard-based interlocks of usefulessentials in a firmarchitecture carrier system supplying the internet of devices and applications with a secure end-to-end communication path.

Acknowledgement:

The authors express gratitude towards the assistance provided by The Management, Krupanidhi Group of Institutions (KGI) and Krupanidhi Research Incubation Centre, KGI in completing the research. We also thank our Research Mentors who guided us throughout the research and helped us in achieving the desired results.

References:

1. 3GPP TS 11.113rd Generation Partnership Project; Technical Specification Group Terminals Specification of the Subscriber Identity Module - Mobile Equipment (SIM- ME) interface
2. 3GPP TS 22.022 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Personalisation of Mobile Equipment (ME); Mobile functionality specification
3. 3GPP TS 23.122 3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions relatedto Mobile Station (MS) in idle mode
4. 3GPP TS 33.102 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture
5. 3GPP TS 21.111 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)