International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference "AECD 2018", 9 - 10 March 2018

Development of Authentication and Security Procedures for IoT System

Mr. Amit Jaykumar Chinchawade.
Research Scholar
Dept. Electronics &-Communication Engineering
Suresh Gyan Vinar University, Jaipur, Rajasthan, India.
amitchinchawade@yahoo.co.in.
Dr. O.S. Lamba, Professor,
H.O.D
Dept. Electronics &-Communication Engineering
Suresh Gyan Vinar University, Jaipur, Rajasthan, India.
onkar.lamba@mygyanvihar.com

Abstract— Security and privacy in Internet of Things (IoT) is a major challenge, mainly due to the massive scale and distributed nature of IoT networks. Block chain-based approaches provide decentralized security and privacy, yet they involve significant energy, delay, and computational overhead that is not suitable for most resource-constrained IoT devices. A smart home setting consists of three main tiers namely: cloud storage, overlay, and smart home. Each smart home is equipped with an always online, high resource device that is responsible for handling all communication within and external to the home. Robust authentication and security procedures in IoT is need of time and we propose to achieve such procedures in our research work.

Index Terms- *IOT* (Internet Of Things), Attribute-Based Encryption (ABE), differential power analysis (DPA), ZigBee Light Link (ZLL), low-power wireless personal area networks (LoWPANs), HomeKit Accessory Protocol (HAP).

1. INTRODUCTION

Internet of things is a latest technology which has good number of benefits to its users. It's an emerging technology where we connect daily objects to the internet for sending and receiving data. For an example home automation system, various durable goods, vehicles (cars and trucks) sensors. We can combine all these with internet. We can send and receive information as per user's requirement. IoT is facing security challenges as the devices are providing security to the personal properties like money or intellectual property via automated devices. IoT devices are connected with each other and share information during any haphazard situation. So there are equally more chances for hacking the systems or blocking the services in between transmission. Although fast information exchange is first and foremost requirement so it is not necessary to provide complete security solutions for IoT.

There is need of a dynamic authentication mechanism for mobile users are needed to protect against unauthorized access. To securely exchange information with fast computing speed, symmetric encryption scheme can be used. Although it uses only one secret key for two communicating parties, key agreement protocol to agree on a shared key or key distribution protocol is required. These protocols introduce security requirements such as authentication of parties in key agreement protocol or secure and integrity-assured key distribution to prevent man-in-the-middle attacks and other attacks. Without the use of public-key cryptography, symmetric key scheme is not sufficient to get secure communication features such as confidentiality, integrity, authentication, and non-repudiation.

2. PROBLEM STATEMENT

There is need of robust user authentication and secure device access strategy in IoT. One beneficial aspect in IoT is a big amount of things being related to the Internet, each one supplying data. Searching few paths to reliably store and understanding the masses of data via scalable uses remain a major challenge in technologies. To narration in this section, we will draw a few key challenge areas:

- Access control, Security, Privacy, Management of identity.
- Standardization and Interoperability.
- Data deluge.

.

3. LITERATURE SURVEY

The survey is done by considering the aspects of security and authentication procedures used in IoT

systems. Further survey is categorized based on their approaches.

In multi-receiver scheme [1], users need to generate own key pair to avoid key escrow problem. Although key generation introduces some load on sender, its merit is key escrow problem. In terms of computational cost, the scheme in [1] achieves better efficiency than identity-based multi-receiver encryption scheme proposed in [2] because it reduces one pairing operation not only for encryption but also for decryption. To encrypt messages, the sender uses only the public keys of receivers. Without checking the receivers' public keys for validity and authenticity, the attacker can easily impersonate as the authentic receiver in communication of unknown devices in large and highly dynamic environment. For public key validation, two pairing operations will be required in [1]. For checking the validity of certificate generated by third party, each user will require one pairing operation. In addition to this, the receiver requires one pairing operation to get back the message. Moreover, the scheme does not consider source authentication and replay attack prevention. There are many certificate-less public key cryptography schemes based on computation expensive bilinear pairing [3]. Based on Schnorr's signature scheme, a certificate-less public key encryption scheme without pairing has been proposed in [4] and [5] for single-receiver setting. Existing certificate less multi-receiver encryption scheme has been presented in [6]. In [6], computation expensive pairing operations are used in both encryption and decryption. In addition to this, the scheme does not consider source authentication and replay attack prevention.

In IoT Encryption scenarios Attribute-Based Encryption (ABE), specifically CP-ABE, to securely carry out this sharing, leveraging on the fine-grained access control provided by this scheme. However, these works do not consider the existence of resource-constrained devices, e.g. sensors, as data producers. As it highlighted in [4], such devices present limitations in terms of RAM memory and CPU processing power to perform the CP-ABE operations. To this end, the scientific literature reports plenty of recent studies that examine the feasibility of using CPABE in different types of devices. In [5] the application of ABE schemes is analyzed on current smart phones via the implementation of an ABE library for Android, demonstrating that a suitable performance in these devices can be achieved. However, devices like sensors have more reduced features than smart phones, so it is necessary to look for other solutions which take into account this kind of devices as well as context where data are generated at high rate. On this line, there are different proposals, as [6], which are based on the use of digital wrapper schemes to securely share information.

The security modules in IoT consist of various approaches. A thing is a combination of hardware board, operating system, network stack and applicative layer. The Internet of Things is made with connected devices exchanging messages. Consequently the nodes deal with network stacks including OSI Layers 1 (PHY) and 2 (MAC) and optionally Layers 3 (IP) and 4 (UDP and/or TCP). Messages are processed by upper standardized "application" layers such as HTTP, CoAP [10], MQTT [9], and proprietary protocols like Weave from Google or HomeKit Accessory Protocol (HAP) from Apple. Security features maybe delivered by network layers (typically at MAC frame level) and/or by application layers for example implementing TLS or DTLS stacks.

A. Operating System Security

Operating systems (like Linux, Contiki, Riot, Iotivity, AllJoyn, Brillo, mbed OS ...) implement cryptographic libraries and store the needed keys. Many attacks such as code Smart Cities and IoT Services debugging at runtime, fault injection, glitch, or differential power analysis (DPA) can be used to recover these secret credentials. In some cases [6] the OS code may be altered in order to modify the thing functionality.

In this paper we focus on secure elements benefits, in order to provide trusted and secure (TLS/DTLS) communications. However tamper resistant devices could also enforce secure storage and node integrity checking, i.e. secure booting.

B. MAC Security

Many IoT systems are using the IEEE 802.15.4 [3] radio standard, which supports several security suites, for example the CBC-MAC (CCM, RFC 3610) mode of AES, enforcing at MAC level data privacy and integrity. The ZigBee specification [6] provides mechanisms, based on a Master Key provisioned by off line ways, by which Zigbee devices derive shared secret keys (Link Key). As an illustration the commercial Philips Hue light system [4] is based on the ZigBee Light Link (ZLL) specification [1] in which the same network key is shared by all network nodes for encryption/decryption operations. This unique key is securely distributed thanks to the ZLL master key stored in every bulb. A controller realizes the bridge between the ZigBee mesh networks and the IPv4 world, and includes two radio (IEEE 802.15.4 and Wi-Fi) interfaces. As mentioned in [6] several UDP ports enable the bulbs control, without any security features (such as DTLS), what could be used to create side channel attacks. Therefore the security only relies on a shared link key, and many attacks have been published [5][7] realizing the extraction of ZigBee keys or software injection.

C. TLS/DTLS stacks

Roughly speaking there are two classes of IoT systems, dealing either with IPv6 or IPv4. IPv6 solves the addressing issue in the IoT context, but induces interoperability problems with the legacy IPv4 infrastructure, which are usually solved by the design of an applicative gateway. For example a HTTP/CoAP bridge may proxy incoming HTTP request over IPv4 towards IPv6 mesh network. As an illustration the NEST thermostat [11] powered by the THREAD protocol (see below) has two wireless interfaces, IEEE 802.15.4 with 6loWPAN, and Wi-Fi with IPv4. 6LoWPAN is a set of IETF specifications achieving IPv6 networks over low-power wireless personal area networks (LoWPANs), such as the IEEE 802.15.4. Segmentation/Assembly operations are performed by an adaption layer. Two kinds of routing mechanisms are supported mesh-under (performed in the adaptation layer) and route-over (performed in the IPv6 layer). Security services are delivered by TLS for TCP reliable transport, or by DTLS in the case of UDP datagram mode. Many industrial consortiums such as Open Connectivity Foundation (OCF) [12] or THREAD [13] support 6LoWPAN stacks secured by the TLS or DTLS protocols. The CoAP protocol natively works over DTLS (and soon over TLS , it typically delivers EST services using JSON messages. The MQTT [9] protocol realizes a publish/subscribe messaging paradigm and is secured by TLS. The OCF consortium is pushing an authentication procedure based on password and elliptic curve (J-PAKE) over TLS 1.2. WEAVE [18] is a communication platform from GOOGLE dedicated to IoT devices, and works with a REST protocol over HTTPS. It supports network stacks such as Bluetooth Low Energy (BLE), Wi-Fi, Ethernet and ZigBee WEAVE uses OAUTH 2.0 for authorization and is powered by the BRILLO operating system, a light Android version, requiring at least 30MB of memory. TLS/DTLS stacks are used by OCF or THREAD for authentication purposes. Authorization mechanisms may be also supported by the application layer, like for example access control list (ACL) are available in the OCF framework.

D. Application Layer Security

Another approach is to implement all security operations in the application layer. For example Home Kit is a framework from Apple targeting the management of connected objects, named accessories. It works over two network stacks: Bluetooth Low Energy (using the Generic Attribute Profile - GATT-), and Wi-Fi associated to IPv4 or IPv6; it uses JSON messages over HTTP. The security is fully enforced (i.e. encryption/decryption operations and data integrity procedures) by an applicative protocol named HAP (Home Kit Accessory Protocol), whose initial pairing exchange is based on the Secure Remote Password procedure (SRP, RFC 5054) which deals with a 8 digits PIN code available for every accessory.

4. OBJECTIVE OF THE PROPOSED RESEARCH

1. To develop a protocol to establish end to end security and authentication mechanism.
2. User identity prevention mechanism to improve the protection against threats in the IoT infrastructure.
3. To analyze the performance of developed system by experimentation.
4. Developing test bench for testing purpose.
5. Testing the performances in terms of comparative studies.

5. METHODOLOGY OF THE PROPOSED RESEARCH

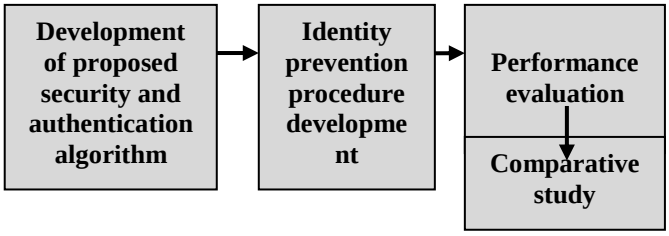

Figure 1: Proposed work flow

The proposed algorithm for authentication and security in IoT systems can be tested using raspberry pi based test bench.

Using open source simulation as well as working libraries in Linux platform environment can be best applicable platforms for the implementation. The testing environment can be consist of open source based simulation tools and libraries for authentication and encryption purpose.

6. EXPECTED OUTCOME OF THE PROPOSED RESEARCH

The developed technique can provide efficient way for IoT system authentication and security in terms of used identity and access.

7. SUMMARY

The Internet of Things (IoT) is one of the so-called disruptive technologies. It has diverse impact margins that can influence our lives, the business world and even the global economy. In utmost synthesis, IoT can be considered a family of technologies whose goal is to enable anything that

can be connected to the Internet even things which do not have any electronic purpose to be monitored and controlled from afar and thus to provide a service to its users. That thing can perform as a sensor, for example, or be enabled to produce information about itself or its surroundings. And that thing can be programmed from a distance, without any specific technologies, but rather through Internet connections. With optimum authentication and security IoT can prove itself as boon to mankind.

REFERENCES

[1] R. Fielding, "Architectural Styles and the Design of Network-based Software Architectures", thesis, UCA, 2000.
[2] Standard for part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (WPAN). IEEE Std 802.15.4, IEEE (2003) .
[3] T. Bray, "JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, 2004
[4] Urien, P. and Dandjinou, M., 2007, in IFIP International Federation for Information Processing, Volume 229, Network Control and Engineering for QoS, Security, and Mobility, IV, ed. Gaiti, D., (Boston: Springer),pp. 75-86.
[5] GEMALTO, GemXpresso R4 E36/E72 PK – Multi App ID 36K/72K -TOP IM GX4 Security Policy, 2009
[6] Federal Office for Information Security, "Certification Report BSI-DSZCC-0555-2009, BSI-DSZ-CC-0555-2009 for NXP Smart Card Controller P5CD081V1A and its major configurations...", 2009
[7] Robert Walsh, "Designing Accessories for iOS and OS X", Session 701,WWDC14,
[8] http://devstreaming.apple.com/videos/wwdc/2014/701xx8n8ca3aq4j/701/701_designing_accessories_for_ios_and_os_x.pdf
[9] A. Banks and R. Gupta, "MQTT Version 3.1.1", OASIS Standard September 2014.
[10] Z. Shelby, K. Hartke, C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014
[11] Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin "Smart Nest Thermostat: A Smart Spy in Your Home", Black Hat 2014
[12] NXP, ZigBee Light Link User Guide JN-UG-3091 Revision 1.3 3 August 2016.
[13] Moazzam Khan, Fereshteh Amini, Jelena Misic, "Key Exchange in 802.15.4 Networks and Its Performance Implications" Mobile Ad-hoc and Sensor Networks Volume 4325 of the series Lecture Notes in Computer Science pp 497-508.
[14] http://www.developers.meethue.com/
[15] Eyal Ronen, Colin O'Flynn , Adi Shamir and Achi-Or Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction", Cryptology ePrint Archive, Report 2016/1047.
[16] E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," 2016 IEEE European Symposium on Security and Privacy (Euro S&P), Saarbrucken, 2016, pp.3-12.doi: 10.1109/EuroSP.2016.13
[17] Colin O'Flynnn, "A light bulb Worm? Details of the Philips Hue Smart Lighting Design", Black Hat USA 2016 White Paper, August1, 2016.
[18] Open Connection Foundation (OCF), https://openconnectivity.org
[19] Thread, http://threadgroup.org
[20] C. Bormann ET al, "A TCP and TLS Transport for the Constrained Application Protocol (CoAP)", IETF draft April 2016
[21] R. Cragie, F. Hao, "Elliptic Curve J-PAKE Cipher Suites for Transport Layer Security (TLS)", draft-cragie-tls-ecjpake-01, June 2016.
[22] Bruce Beare, "Brillo/Weave Part 1: High Level Introduction, Open IoT Summit", April 2016
[23] http://www.eurosmart.com/facts-figures.html
[24] Jurgensen, T.M., et al.: Smart Cards: The Developer's Toolkit. Prentice Hall PTR, Upper Saddle River (2002). ISBN 0130937304
[25] TLS and DTLS Security Modules, draft-urien-uta-tls-dtls-securitymodule-00.txt, June 2015
[26] Chen, Z.: Java Card TM Technology for Smart Cards: Architecture and Programmer's (The Java Series). Addison-Wesley, Boston (2002). ISBN 020170329
[27] Urien, P., "Innovative TLS/DTLS Security Modules for IoT Applications: Concepts and Experiments", IoT 360°, Part I, LNICST169, pp. 1–13, 2016.
[28] Urien, P.; "Innovative DTLS/TLS Security Modules Embedded in SIM Cards for IoT Trusted and Secure Services", IEEE CCNC 2016, January 2016, Las Vegas, NV, USA