INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Security Tools for Internet of Things: A Review

Amandeep Singh[1],Dr. Charanjit Singh[2]
[1,2] Department of Electronics and Communication Engineering, Punjabi University, Patiala
singh.amandeep183@gmail.com[1]

Abstract

In today's communications, the main challenging facet is Security of LTE systems in terms of various areas such as mutual authentication, key management, forward and backward secrecy, use of efficient security tools, etc. For proper key management, the generation and distribution of random keys is of main concern which can be done with the help of dynamic security tools. In this paper, main features of security tools like, Docker, Java Cryptography Architecture (JCA), Token-based authentication have been reviewed. Docker provides containerized environment based on application virtualization and also lighter than virtual machines. To define cryptographic concepts and algorithms, JCA cites design patterns and an extensible framework for Java platform. Token-based authentication method or system is used to provide secure user access to server using a token, like smart cards.

Keywords: Docker, JCA, Key Management, Mutual Authentication, Token-based Authentication.

1. Introduction

In today's world, almost all devices have been attached to Internet, as they can be operated from all over the world through Internet. So, Internet of Things (IoT) plays vital role to fulfil the needs in present human life. The backbone of IoT is Artificial Intelligence that makes the system smart [1]. Besides the pros of IoT like mitigation of human intervention, more processing speed and accuracy; there are some of cons of IoT like vulnerability to attacks in terms of security issues. Cryptography can be used to provide confidentiality, mutual authentication, integrity, and other security services. Mutual Authentication is a security feature in which a client must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection [2].

Various cryptography tools are available to ratify the security issues in terms of authentication for users by using appropriate key management. By using public and private keys, one can authenticate the user's identity rather than requiring secret passwords from user. Password or secret key authentication is more vulnerable to dictionary and man-in-the-middle attacks. A pair of asymmetric keys is assigned to each user for authentication using server's pubic key encryption and client's private key decryption [3]. Git Bash and PuTTYgen tools can be used to generate asymmetric keys for Windows platform. A longwith key management, token-based authentication can be used as an additional protective measure electronically. Security tokens are tools used to verify user's identity by which they can access a particular service. Security tokens may be in the form of authentication tokens, cryptographic tokens, hardware or software tokens, USB tokens, or key fobs [4]. Java Cryptography Architecture (JCA) is based on conventional public key cryptography and does not support group-oriented cryptography. JCA uses provider architecture and contains a set of Application Programming Interfaces (API) for digital signatures, key generation and management, and certificates [5]. Java Security API is set of packages, such as java.security, java.security.interfaces, etc., to develop secure applications in Java. JCA also supports famous algorithms like AES, DES, 3DES, Blowfish, and Twofish etc. By using Docker application, the user can set up programs in sandbox packages called containers having all required dependencies. For more scalable and secure environments, demand for virtual technologies has been increased dramatically. Container-based virtualization (Docker) and hypervisor-based virtualization are the two methods available for virtualization solutions that provides their services at software level and hardware level respectively. Docker is an open source container technology with the ability to "build, ship, and run distributed applications" [6]. It is commonly used in some popular applications, such as Spotify, Yelp, and Ebay. Docker application consists of two major components: Docker engine, which is an open source solution and lightweight packaging tool depends on container-based virtualization and Docker Hub, which is a Software-as-a-Service platform. Docker provides the user the ability to start the processes in a container with a different SELinux type, through the '–security-opt parameter' leading to an increase of security in Docker. Docker's security relies on three components, i.e., isolation of processes at userspace level managed by the Docker daemon, enforcement of this isolation by the kernel, and network operations security [7].

2. Literature Survey

In 2013, Wu-Chuan Yang and Jian-Xun Lee proposed a method for developers to write and maintain any stream cipher algorithm in Java Cryptography Algorithm (JCA). An abstract class, namely CipherSpi, has been developed and implemented included by 14 abstract methods for block cipher and stream cipher encryption. The stream cipher service is proved better than block cipher service for Java platforms [8].

In 2014, Alexandre Melo Braga, Eduardo Moraes de Morais described about the construction of cryptographic library for Android devices in terms of design decisions and implementation issues of standard as well as non-standard algorithms both. The cryptographic library for Android platform has been designed based on standard cryptographic API for Java, Java Cryptography Algorithm (JCA) and its design principles. The performance of Java programs has been evaluated in terms of elapsed time to process a single block of data [9]. In 2016, Jeeva Chelladhurai et al. discussed about security of Docker containers by avoiding DoS attacks. Containers are highy vulnerable to DoS attacks due to direct communication with host kernel. A novel security approach has been proposed to improve the safety of Docker containers against threat of DoS attacks [10]. In 2016, Alexandre Braga and Ricardo Dahab discussed about squandering of cryptography by software developers in online forums about security aspects. Data mining technique Apriori has been implemented to determine cryptography misuse in terms of cryptography-based security and cryptographic programming. Three programming forums, namely Oracle Java Cryptography (OJC) using Java Cryptographic Architecture (JCA), Google Android Developers (GAD) using Android programming, and Google Android Security Discussions (GASD) have been analysed as they all are share the same Java-based API for cryptography [11].

In 2017, Babak Bashari Rad et al. presented an introduction to Docker and also analysed its performance by surveying literature of various authors. Docker Client and Server, Docker Images, Docker Registries, and Docker Containers are fundamental components of Docker. In comparison to virtual machines, it is far more advantageous to use Docker in terms of more speed, easily portable, scalability, higher density, etc [12].

In 2017, Minhaj Ahmad Khan and Khaled Salah surveyed and reviewed major security issues about IoT layered architecture and its protocols. Besides providing many advantages like controlling of appliances at home, predicting weather conditions, etc.by IoT; there are some flaws also, like more vulnerability to attacks, threat to confidentiality, authentication and integrity of data. Various issues regarding IoT at different layers have been discussed in this paper and suggestions to improve these issues using blockchain have been presented. [13]

In 2017, Quanqing Xu et al. discussed about vulnerability of docker images towards Denial-of-Service (DoS) attack and provided solutions by decentralizing the Docker Content Trust (DCT). Two approaches have been suggested, in first approach InterPlanetary File System (IPFS) has been used which is similar to BitTorrent. In second approach, Blockchain based technology has been used. [14] In 2017, Adhitya Bhawiyuga et al. proposed a design to secure Message Queue Telemetry Transport (MQTT) using token based authentication in constrained devices. Publisher, subscriber, MQTT broker and JSON Web Token authentication server are prime components of the proposed design. As a result, the proposed design has been performed efficiently by authenticating valid and expired tokens in very less time [15]. In 2017, Huseyin POLAT and Saadin OYUCU developed an M2M (Machine-to-Machine) platform using token-based authentication method with RestFul web services and NoSQL database. Token-based method has been used for session control and ID authentication. In the developed M2M platform, web services have been tested using a Google Chrome plug-in, namely, Advanced Rest Client [16]. In 2018, Seo Yeon Moon et al. described security issues in the form of threats to IoT technology. Proper and secure authentication among devices is the main aspect in IoT alongwith effective key management. With an application of lightweight encryption technology and reliable integrity process, the security of IoT devices can be enhanced appropriately. [17]. In 2018, Mohammed Ali Al-Garadi et al. suggested about implementation of Machine Learning (ML) and Deep Learning (DL) to enhance the security measures of IoT. Consequently, ML/DL methods have been used to analyse the behaviour of devices (normal/abnormal) within IoT environment. Moreover, these methods are also helpful in predicting new unknown attacks by learning from existing examples. The applications of ML/DL methods have also been analysed at various IoT layers and reviewed [18]. In 2019, Cihan Atac and Sedat Akleylek provided comparison for IoT security in terms of authentication, integrity and vulnerability to various attacks. Several countermeasures have also been discussed in order to improve issues related to cybersecurity in IoT. By implementing appropriate and effective methods, threats to attacks can be avoided significantly [19]. In 2019, Marco De Benedictis and Antonio Lioy presented a solution, named as Docker Integrity Verification Engine (DIVE), for integrity of cloud environment employing Docker containers. The proposed method has covered wide spectrum of lightweight virtual technologies as it has been based on Linux kernel and has not any dependency at any specific container runtime. The main advantage of DIVE is its behaviour of detecting compromised container, so that it be stopped and replaced as early as possible without refreshing the whole system. It has also improved Remote Attestation efficiency and verified using OAT core tool [20]. In 2019, Yongfeng Yin et al. proposed an experimentation platform architecture design to analyse the effectiveness of cyber security based on Docker. In this method, various experimental environments and network topologies with flexible monitoring and faster test environment has been deployed for larger cyber simulation. Additional functions of cyber security have been further improved by using the proposed method [21].

In 2019, Mohammadreza Hazhirpasand et al. discussed about investigation of cryptographic APIs used by developers in terms of 2324 Java projects using CogniCrypt tool and GitHub for exploitation of Java Cryptographic Architecture (JCA). GitHub API (Application Programming Interface) search method has been deployed to check about the usage of crypto classes, by any project, specified in the CogniCrypt rule set. Without any API misuse, a project is said to be secure and not demented. The Java projects have been analysed in terms of four parameters, API diversity, number of projects, JCA commits, number of days committed by developer [22]. In 2019, Abid Omar et al. implemented a Docker technology based platform for cyber physical production system to pre-process data using Fog computing method. The proposed method has implemented through Raspberry cards alongwith combination of Docker technology in terms of virtualization kubernetes in terms of container composition for improvement interoperability and scalability of Industry 4.0. Containers have been preferred over virtual machines as the containers are lighter and share the same operating systems among other containers. The proposed method has been proved to be efficient as the response time is less than 100 ms and flexible computation complexity [23].

Conclusion

Nowadays, cryptography is used to protect sensitive information of many applications. Various encryption techniques and security tools are used for mutual authentication and key management, so as to avoid vulnerabilities among data transfers. This paper has reviewed some of security tools such as JCA, Docker and Token-based authentication provided by several authors for proper authenticity and integrity of M2M devices using security tools.

References

[1] S. Gusmeroli, S. Piccione, D. Rotondi (2013). A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling 58 (5) 1189.

[2] W. Diffie and M. Hellman. New Directions in Cryptography. IEEE Transaction on Information Theory, Vol. IT-22**,** 1976, pp. 644-654**.**

[3] Randall K. Nichols, Panos C. Lekkas. Wireless Security: Models, Threats, and Solutions. McGraw-Hill, 2002.

[4] Kai Zheng and Weihua Jiang (2014). A Token Authentication Solution for Hadoop Based on Kerberos Pre-Authentication. Data Science and Advance Analytics (DSAA). Shanghai, pp. 354 – 360.

[5] J. Knudsen. Java Cryptography. O’Reilly. 1st edition. 1998.

[6] J. Fink (2014). Docker: a software as a service, operating system-level virtualization framework. Code4Lib Journal. Vol. 25.

[7] C. Anderson. Docker (2015). IEEE Software, Vol. 32, No. 3.

[8] Wu-Chuan Yang and Jian-Xun Lee (2013). Implementation of Stream Cipher Service in JCA. IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26. Kaohsiung, Taiwan. pp 557-561.

[9] Alexandre Melo Braga, Eduardo Moraes de Morais (2014). Implementation Issues in the Construction of Standard and Non-Standard Cryptography on Android Devices. SECURWARE 2014: The Eighth International Conference on Emerging Security Information, Systems and Technologies. pp 144-150.

[10] Jeeva Chelladhurai, Pethuru Raj Chelliah, Sathish Alampalayam Kumar (2016). Securing Docker Containers from Denial of Service (DoS) Attacks. IEEE International Conference on Services Computing. pp 856-859.

[11] Alexandre Braga and Ricardo Dahab (2016). Mining Cryptography Misuse in Online Forums. IEEE International Conference on Software Quality. Reliability and Security Companion, pp 143-150.

[12] Babak Bashari Rad, Harrison John Bhatti, Mohammad Ahmadi (2017). An Introduction to Docker and Analysis of its Performance. IJCSNS International Journal of Computer Science and Network Security. Vol.17 No.3. pp 228-235.

[13] Minhaj Ahmad Khan and Khaled Salah (2017). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems. pp 1-32.

[14] Quanqing Xu, Chao Jin, Mohamed Faruq Bin Mohamed Rasid, Bharadwaj Veeravalli and Khin Mi Mi Aung (2017). Decentralized content trust for docker images. IoTBDS. pp. 431–437.

[15] Adhitya Bhawiyuga, Mahendra Data, Andri Warda (2017). Architectural Design of Token based Authentication of MQTT Protocol in Constrained IoT Device. IEEE.

[16] Huseyin POLAT and Saadin OYUCU (2017). Token-based authentication method for M2M platforms. Turk J Elec. Eng. & Comp. Sci. (25). pp 2956-2967.

[17] Seo Yeon Moon, Jin Ho Park, Jong Hyuk Park (2018). Authentications for Internet of Things Security: Threats, Challenges and Studies. Journal of Internet Technology

Vol. 19. No.2, pp 349-358.

[18] Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani (2018). A survey of machine and deep learning methods for Internet of Things (IoT) security. [Online]. https://arxiv.org/abs/1807.11023.

[19] Cihan Atac and Sedat Akleylek (2019). Survey on Security Threats and Solutions in the Age of IoT. European Journal of Science and Technology. pp 36-42.

[20] Marco De Benedictis and Antonio Lioy (2019), Integrity verification of Docker containers for a lightweight cloud environment. Future Generation Computer Systems. Elsevier 97. pp 236–246.

[21] Yongfeng Yin, Yuyan Shao, XueFeng Wang, Qingran Su (2019). A Flexible Cyber Security Experimentation Platform Architecture Based on Docker. IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). pp 413-420.

[22] Mohammadreza Hazhirpasand, Mohammad Ghafari, Stefan Krüger, Eric Bodden, Oscar Nierstrasz (2019). The Impact of Developer Experience in Using Java Cryptography. ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM) IEEE.

[23] Abid Omar, Bouzarkouna Imen, Sahnoun M'hammed, Brik Bouziane, Baudry David (2019). Deployment of Fog Computing Platform for Cyber Physical Production System Based on Docker Technology. The 3rd International Conference on Applied Automation and Industrial Diagnostics (ICAAID). 25-27 September 2019. Elazig. Turkey. European Union.