International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Modified Kerberos for IoT by Dynamic Expansion

Nilesh B. Korade,B. Veeramallu
Abhijeet R. More,Vasudha S. Potey
Snehal G. Langhe
Computer Science & Engineering Department KL University
Guntur, Andhra Pradesh,
India
PCETS
Pimpri Chinchwad College of Engineering and Research,
Ravet, Pune,
Maharashtra, India,
nileshkorade9@gmail.com,
bvmallu@gmail.com
abhijeet.r.more@gmail.com
vasudha.potey@gmail.com
snehallanghe23@gmail.com ,

May 24, 2018

Abstract

The future it is! IoT. IoT is deepening its roots in every field and has an enormous impact. The control has been dispersed all over the world as the decentralized network approach has come into picture. With the transfer of data over such networks, comes greater risks of data theft, server manipulation, device manipulation, data manipulation, etc. Thus, we require an efficient and secure protocol to protect the user privacy and sensitive data. The existing

Kerberos is vulnerable as the main components- Authentication Server (AS) and Key Distribution Centre (KDC) can be jeopardized by any attack. When compared with the traditional network, IoT has vast communication between the nodes where the block of bytes is small but, strongly encrypted. So, by extending the traditional Kerberos we put forth the idea of separating the modules of Kerberos and distributing it on multiple nodes autonomously. We also include third party cloud service.

***Key Words*:**Kerberos, Authentication Server (AS), Key Distribution Centre (KDC), Ticket Granting Ticket (TGT), Expanded Kerberos.

1 Introduction

The Internet of Things is a system of connected physical objects; including mobiles, electronic appliances, connected security systems, cars, lights in household and commercial environments, speaker systems that are accessible through the internet. These objects collect useful data and then autonomously flow the data between other devices, for example smart home devices such as the control and automation of lighting, ventilation, heating, air conditioning systems that use Wi-Fi for remote monitoring. IoT brings huge opportunities for consumers and businesses in the areas of warehousing, healthcare, logistics and transportation. IoT application

handles a lot of sensitive data; hence developers face whole new challenges to make sure that IoT applications are well secured.

Increasing the number of devices is the fundamental security weakness of Internet of Things. Years ago, we had to worry only about protecting our computers and smartphones but now we have to worry about protecting our home appliances, car, wearable devices, etc. We have heard how hackers potentially remotely control and accelerate or decelerate the car. Not only a car but, hackers could even use seemingly unimportant devices like baby monitors or your thermostat to uncover private information or just ruin your day. The consequences may be big or small but surely non-beneficial.

IoT security is concerned with protecting networks and the devices connected to it. A lot of personal user data is collected by

these devices and is shared with other devices on the network for communication.

IoT experts argue there is not enough been done to build confidentiality, stability and security in IoT. To manifest their statement, they have compromised a host of devices like automated lighting, baby monitors, smart refrigerator, as well as the systems which are city wide such as traffic signals. As more connected devices pop up around the globe, cyber-attacks are also a growing threat. Hackers could penetrate people's homes, critical infrastructure and even connected cars. Several tech companies are paying attention on cyber security in order to secure the safety and privacy of all this data.

Following are the key challenge for making IoT safer:

IoT authentication: In IoT authentication, we provide user authentication for an IoT device which may range from normal password to more robust mechanism such as two-factor security, digital certificate and biometrics. In existing system, the user authentication process involves user entering username and password as their credential whereas, many IoT authentication scenarios are based without user interference.

IoT encryption: Data processing and data retrieval is integral part of the IoT environment where IoT applications collect tons of data. Most of this collected data is confidential and personal and needs to be protected through encryption. While sending data from one device to another device, the transferring data should be converted into cipher text and key used in encryption algorithm should be managed securely to prevent potential exposure to the outside.

Kerberos

Kerberos protocol is used to establish a strongly secured network-based communication as it provides strong authentication for client as well as server. Kerberos is a network authentication protocol available in many commercial products. The currently used protocols are not secured. Hence, the credentials are shared over the unsecured channel like internet and thus can be extremely vulnerable to attacks. Kerberos protocol was designed by MIT which provides solution to network security problems that helps in providing identity of client to the server.

Kerberos Authentication Dialogue

The Kerberos protocol allows a client to repeatedly be authenticated to multiple servers assuming that there is a long-term secret key shared between the client and Kerberos infrastructure. The client long-term secret key was generated using the client's password. A simplified overview of the Kerberos actions is shown in Figure 1. Exchange between the client and the Kerberos AS (Authentication Server) in step 1 and 2 are used only when the user first logs in to the system. In step 3 and 4, communication takes place between client and Kerberos TGS (Ticket Granting Server) whenever a user authenticates to a new server. Step 5 is conductedevery time user authenticates itself to a server. And finally, step 6 is the mutual-authentication response by the server.

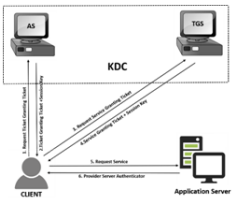

Fig1.Kerberos

2 Related Work

To make our lives more comfortable, easier and convenient smart homes filled with connected products. Securing IoT for smart home system is one of the key challenges. As the number of IoT devices are increasing, the security risk of an IoT system also increases. With the observation of1 the author listed the security requirements of the smart home services includes authentication, unauthorized access, protection of user confidential data, etc.

In research article2, the authors presented systemic approach for IOT security. There are four nodes present in model namely intelligent object, person, technological ecosystem and process. These nodes interact through tensions; the tensions represent dynamical character of model which can be identification, privacy, trust, safety, responsibility, reliability and auto-immunity. In research article3 the authors examine authentication issues and schemes pertinent to the IoT. Verifying intelligence or authentication of smart devices, plays important role in the realization of IoT. They have designed a

network testbed to emulate the IoT for authentication study. The research article4 demonstrated that both industrial and commercial IoT devices are vulnerable to IoT related attacks. While building modern IoT devices the security parameter should be considered because these devices are of limited protection.

In the research article5, authors proposed 3-level secure Kerberos authentication for smart home system. The security on server side has been increased by using 3 level Kerberos authentication. The home automation scheme proposed in this paper include online server which provides secure authentication through Kerberos technology, smart central controller which includes main controller, modem, GSM/GPRS modem and last part includes small microcontroller having RF and switch module. In the research article6 the authors presented Secure Multi-Hop Routing Protocol (SMRP), which enable IoT device to authenticate before joining an existing network or forming a new network. The proposed SMRP merges the Authentication and routing process to form a secured IoT network and produces a secured multi-hop IoT communication network without performance degradation.

In the research article7 the authors show that Telnet-based attacks that target IoT devices have increased since 2014. To analyze Telnet-based attacks on various IoT devices they have proposed IoT honeypot and sandbox. IoT require that, approaches to IoT security should be dynamic. To simulate real defense environment of IoT security, the researcher8 adopts Artificial Immune System principal and mechanism in IoT security. The proposed approach captures and analyses original data to identify whether it contains security threats. With rapid growth in wearable and mobile device technology we are seeing devices increasingly becoming a method of authentication (e.g. RFID enabled cards, smartphones).

The author9 proposed user authentication based on digital memories for mobile devices. Using personal digital memories for authentication eliminates many risk that are associated with remembering password, phishing, shoulder surfing and brute force. The author9 described a discovery framework that can be used to secure IoT based smart home system. Basic security mechanisms that are related to thing authentication and access control are discussed to ensure privacy in IoT. The author10 introduced some changes to Kerberos authentication protocol. The traditional Kerberos is vul-

nerable to password guessing attack. The modified Kerberos version is no longer vulnerable to password guessing attack because the modification to KDC database will enhance the performance of protocol and the secret key will be independent on user password.

3 Proposed System

In the presented design, the system would have N (N1, N2, N3, , Nn) number of IoT nodes. When we consider the traditional Kerberos system, one of these N nodes, assume Ni, will act as the Authentication Server (AS) and another node, assume Nj, will act as the Key Distribution Center (KDC); the variables i and j can take any values from 1 to n. In the proposed system, Authentication server and the Key Distribution Center functions the same as that in the traditional Kerberos. The significant difference is that, in the traditional Kerberos there is only one system on which Authentication server and Key Distribution Centre functions; whereas in the extended Kerberos there are n-number of ASs and n-number of KDCs which keep switching their roles with the help of random algorithm after specified period of time. The AS and KDC would work anonymously i.e. the nodes on which AS and KDC would be working unknowingly.

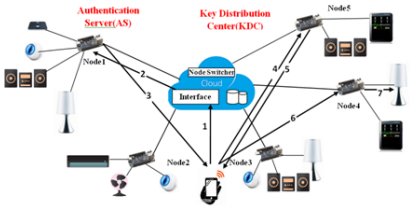

Fig2. Architecture of Proposed System

The security of traditional Kerberos is endangered completely if AS or KDC get discredited by any attack. All IoT nodes (N1, N2, N3, , Nn) are capable of being AS and KDC hence the probability that the node getting hacked is either AS or KDC is 1/2n as a whole and 1/n individually for AS and KDC, this makes the system n times less vulnerable. Also, the probability of nodes getting attacked and the node being AS/KDC, decreases with the increase in number of nodes in the IoT network. As we are using cloud-based

service to store sensitive data so, while switching between AS and KDC there is no overhead.

Procedure:

Assume that there are N=10 clients in the IoT network (Client A to Client J). At start of time t=1, Client A is AS and Client E is KDC and their information is stored on the cloud. Other Clients get to know about AS and KDC as their information is stored on the cloud. Also, both the AS and KDC get information about all clients in IoT through cloud.

If Client H wants to communicate with Client G (resource), then Client H will request AS i.e. Client A for Authentication.

Once AS (Client A) authenticates Client H to be legitimate, it will send a packet to Client H.

Consecutively, Client H will request KDC to grant the Tickets and Keys for communicating with Client G (resource) by sending the packet received from AS which would prove Client's identity.

Once KDC (Client E) receives the approval Packet from Client H, it will grant ticket to Client H and thus then Client H further sends packet to Client G (resource). Thus Client G would provide service to Client H.

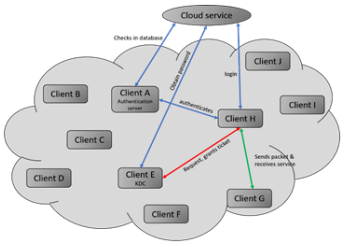

Fig3. System overview.

After n clocks, at time t=1+n, randomly two nodes are selected by making use of random algorithm. These two randomly selected nodes are assigned as AS and KDC respectively.

Suppose that, now Client I become AS and Client C becomes KDC. Client A and Client E become normal Clients in the IoT.

During the transferring of AS and KDC, no new communications can be established and only the existing handshakes can work. After the new AS and KDC are selected, only then new connections can be established between and among the Clients in IoT.

This process of task transferring of AS and KDC takes place after every n clock and thus, attack on AS and KDC can be minimized.

4 Mathematical model and Algorithm

Let S be the proposed Kerberos system

S={ Ni, C, A, K, Res, R, CT}

where, Ni= $\{N_1, N_2, \cdots, N_n\}$ Nodes in network C,A,K, Res N

C $\in N_c$,Client node c= 1 to n

Client

client(){

Step 1: Login to Webpage.

Step 2: Send Request to AS.

Step 3: Listen till AS responds.

Step 4: Accept the Tokens TGT and TGSSK Sent by AS.

Step 5: Decrypt TGSSK with Client Password.

Step 6: Encrypt Tokens.

Step 7: Send Tokens to KDC

Authenticator (Encrypted with TGS session key)

TGT (Accepted from AS)

Step 8: Listen till KDC responds.

Step 9: Accept the Tokens HTTPSSK and HTTPT.

Step 10: Decrypt HTTPSSK with HTTP session key.

Step 11: Encrypt Authenticator with HTTP Session Key.

Step 12: Send Tokens to resource

HTTPT (Accepted from KDC)

Authenticator ((Encrypted with HTTP Service Session key)

Step 13: Listen till Resource responds.

}

Authentication Server

A $\in N_i$, Authentication server (AS) node at time= t, i =1 to n and i!=j

AS() {

Step 1: Listen // for new client request.

Step 2: Accept the Plaintext from Client.

Step 3: Check if resource is present.

Step 4: Send Tokens to Client

TGT (encrypted with TGS Secret key)
TGSSK (encrypted with Client Secret key)
Step 5: Listen // for new client request.
}
Key Distribution Center
$K \in N_j$,Key Distribution Center (KDC) node at time= t, j=1 to n and j!=i
KDC(){
Step 1: Listen //Till client responds
Step 2: Accept the Tokens from Client.
Token 1: TGT
Token 2: Authenticator
Step 3: Decrypt Tokens
Step 4: Check if resource is present.
Step 5: Encrypt Tokens (HTTPT, HTTPST).
Step 6: Send Tokens to Client
HTTPT (encrypted with TGS Session key)
HTTPST (encrypted with HTTP Service Secret key)
Step 7: Listen //For new client request.
}
Resource
Res $\in N_r$,Resource node at time = t, r=1 to n
Resource () {
Step 1: Listen //Till client responds
Step 2: Accept the Tokens from Client.
Token 1: HTTPT
Token 2: Authenticator
Step 3: Decrypt Tokens
Step 4: Compares both token
Step 5: Encrypt Authenticator Token(encrypted with HTTP Service Session Key).
Step 6: Send to Client.
Step 7: Listen //For new client request.
}
Random Function
R= RandomFunction()
{ Run following query:
SELECT column_name FROM table_name ORDER BY RAND() LIMIT 2

Check if new node is equal to previous
if new node equal to previous node
go to step 1
else
change AS and KDC to new nodes.
}
At current time, CT=A, K
where, $A \in N_x$Current AS node at time = t+1, x=1 to n, x!=y & x!=i
K$\in N_y$ Current KDC node at time =t+1,y=1 to n, y!=x & y!=j
After random function, CT=A, K
where, $A \in N_a$Current AS node at time = t+2, a=1 to n, a!=b & a!=x $K \in N_b$Current KDC node at time =t+2,b=1 to n, b!=a & b!=y

5 Experimental result

Designed system is more secure since we have made use of Dynamic and Expanded Kerberos authentication. User feels secured to use the services. The secured authentication is shown in the Fig4. In the first step, the user/client who wants to access a resource needs to login with his username and password.Now, the user gets authenticated by the authentication server and is then redirected to the resource access page where user is given options to select services which are shown in Fig5. At this point, the actual implementation of Dynamic and Expanded Kerberos is not in picture.

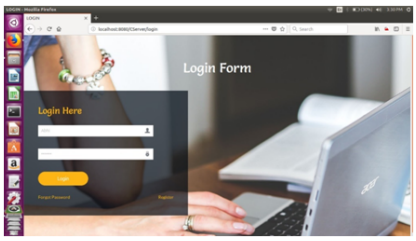

Fig4. Login page

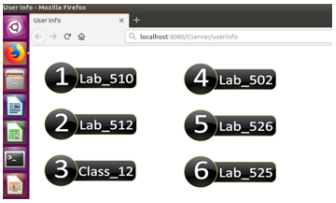

Fig5. Access Resources Page

In the second step, the user now needs to select a service from the options provided. For example: If user wants to get access of the camera and capture photos securely of Lab510, then he/she would select the button1 which is Lab510. Once the user selects the service, the actual process comes into picture. The proposed system authenticates, encrypts, decrypts, contacts cloud services and provides requested services to the user. At the end of this process, user gets access to the resource and further is able to control and manage the resource according to his/her manner. By using this protocol user can communicate securely. According to the graph (Fig6.), as the number of IoT nodes increases, the security in proposed system also increases whereas; in traditional system, with the increase of IoT nodes, security remains constant. The probability of server getting compromised decreases with the increase in number of nodes which can be seen in Fig7. The proposed system is highly scalable.

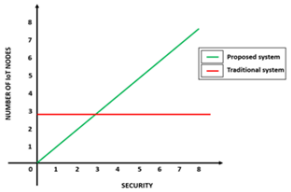

Fig6. Security increased with increase in node

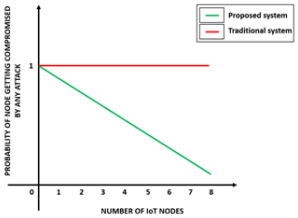

Fig7. Probability of node getting compromised by any attack is decreased

6 Conclusion

The IoT has some special security requirements, hence traditional models of security cannot be applied in IoT security directly. The proposed approach segregates the AS and the KDC adding to it Expanded-Kerberos. As there are a number of nodes present in the network, the chances of AS and KDC getting compromised by an attacker are reduced because, attacker wont be able to find AS and KDC. By the time attacker gets to know regarding AS and KDC, the nodes performing roles would change. The proposed architecture is made more resistant to attacks and is time and space efficient to handle the IoT demands. The whole process of IoT Security is distributed.

References

[1] J. H. Han, Y. Jeon and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment,", 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 1116-1118. doi: 10.1109/ICTC.2015.7354752.

[2] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou and A. Bouabdallah, "A Systemic Approach for IoT Security,", 2013 IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, 2013, pp. 351-355. doi: 10.1109/DCOSS.2013.78.

[3] M. A. Crossman and Hong Liu, "Study of authentication with IoT testbed,", 2015 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2015, pp. 1-7. doi: 10.1109/THS.2015.7225303.

[4] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi and Y. Jin, "Security analysis on consumer and industrial IoT devices," 2016 21st Asia and South Pacific Design Automation Conference

(ASP-DAC), Macau, 2016, pp. 519-524. doi: 10.1109/ASP-DAC.2016.7428064.

[5] P. P. Gaikwad, J. P. Gabhane and S. S. Golait, "3-level secure Kerberos authentication for Smart Home Systems using IoT,", 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015, pp. 262-268. doi: 10.1109/NGCT.2015.7375123.

[6] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication,", 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 428-432. doi: 10.1109/WF-IoT.2014.6803204.

[7] Yin Minn Pa Pa , Shogo Suzuki , Katsunari Yoshioka , Tsutomu Matsumoto , Takahiro Kasama , Christian Rossow, IoTPOT: analysing the rise of IoT compromises, Proceedings of the 9th USENIX Conference on Offensive Technologies, p.9-9, August 10-11, 2015, Washington, D.C.

[8] . Liu, Y. Zhang and H. Zhang, "A Novel Approach to IoT Security Based on Immunology," 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 771-775. doi: 10.1109/CIS.2013.168.

[9] Shone, Nathan Chelsea Dobbins, William Hurst and Qi Shi, Digital Memories Based Mobile User Authentication for IoT 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (2015), pp. 1796-1802.

[10] S. K. Datta, "Towards securing discovery services in Internet of Things," 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2016, pp. 506-507. doi: 10.1109/ICCE.2016.7430707.

[11] Eman El-Emam, Magdy Koutb, HamdyKelash, Osama S. Faragallah, An Authentication Protocol Based on Kerberos 5, International Journal of Network Security, Vol.12, No.3, PP.159-170, May 2011. DOI: 10.6633/IJNS.