A Novel Approach to reduce Vulnerability on Router by Zero vulnerability Encrypted password in Router (ZERO) Mechanism.

Tejendra DS, Varunkumar C.R, Sriram S.L, Sumathy .V, Thejeshwari .CK
dept. Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India
tejads01@gmail.com, crvkche@gmail.com, srisls217@gmail.com, sumathy.v@rajalakshmi.edu.in, thejeswari.ck@rajalakshmi.edu.in

***Abstract*—As technology is developing exponentially and the world is moving towards automation, the resources have to be transferred through the internet which requires routers to connect networks and forward bundles (information). Due to the vulnerability of routers the data and resources have been hacked. The vulnerability of routers is due to minimum authentication to the network shared, some technical attacks on routers, leaking of passwords to others, single passwords. Based on the study, the solution is to maximize authentication of the router by embedding an application that monitors the user entry based on MAC address of the device, the password is frequently changed and that encrypted password is sent to a user and notifies the admin about the changes. Thus, these routers provide high-level security to the forward data through the internet.**

***Keywords*—Vulnerability,Authentication,Encryption,Security.**

I. Introduction

From our school days, we have inspired by the area of systems networking and environment, so we began to find out about it. At a point, we were admired on observing a networking gadget named Router. We came to realize that it transmits the information or packets to a gadget wirelessly. Are we were supposing how it is conceivable to send packets wirelessly to a specific gadget? , then we began to find out about it. Also, we came to knew it has a low authentication level. A Router doesn't think about the users. It, for the most part, confirms a user with a solitary passphrase. This is the principle explanation behind the powerlessness of routers. However, it is called as a backbone of networking it has numerous security issues.

So it is good to have an application that will be embedded inside a router and it is programmed to monitor the users and security levels of a router. The application which is embedded inside the router maintains storage which stores the related information of devices and the application has right to grant and revoke the permission to or from the user with an acknowledgement to the admin. This approach may possibly authenticate the user by their MAC address authentication and use some encryption techniques and one time keys are used which may reduce the vulnerability in a router and provides highsecurity.

What IsRouter

A wireless router is an electronic device that works as a router means it sends data from the internet cable to a device and as a wireless access point so this data can be shared through radio signals instead of cable. These radio signals are shared among multiple devices in order to make wireless establishment between router and devices. When devices connected to the router, devices can access the service provided by the router.

II. Literature Survey

[5] Security dangers against steering in MANETs are ordered into either detached or dynamic assaults. The reason for an aloof assault is for the most part to listen in on steering correspondence and to recover data from observed information bundles. In an aloof assault, a malignant system hub attempts to recognize correspondence parties and the substance of their correspondence. This can open up potential outcomes to dispatch further security assaults. The assault is uninvolved since the typical system correspondence isn't modified. In a functioning assault, a vindictive hub endeavors to intrude, irritate, as well as change the steering usefulness in a MANET.

[3] In this paper, we present a confined convention, which mitigates inner assault through trust-based basic leadership. We utilize area mindfulness, a typical component of numerous sensor organize applications and got flag quality in the approval of area data. Our notoriety based trust demonstrate is dynamic, that is, trust measurements are continually being invigorated.Notoriety in our work is a probabilistic appropriation comparable in nature. Crucial to our methodology is the capacity of hubs to screen the traffic going all through their neighbours.

[8] Giving secure directing in WSN turning into a testing assignment, consequently many research works have been introduced, still, there is a vacuum for research in the steering convention for WSN. The absence of a consistent system network turns into the perceptible specialized issue in WSN. In WSN demonstrating a steady an interface between the

978-1-5386-9371-1/19/$31.00 ©2019 IEEE

facilitate the steering process.

[4] The router is the key device to connect the network in the Internet world, whose security plays a crucial role. However, attacks on routers have never been ceased. According to the U.S. National Vulnerability Database (NVD) statistics, the prevalence of router vulnerabilities is growing up the proportion of vulnerabilities' severity. Previous research on router security is mostly about the technology of exploiting known flaws of routers or debugging routers. How to effectively and automatically discover router vulnerabilities becomes an urgent problem to be solved, especially protocol vulnerabilities. Fuzzing is an effective automatic technique to find vulnerabilities.However, current Fuzzing tools on network protocols are not or partly not suitable for testing router protocols, whose methods of monitoring and debugging targets are different from routers.

III. Need For Security On Routers:

Routers are more Vulnerable nowadays due to low authentication level means there is only one password to connect to the router. The main reason for vulnerability on router is leaking of passwords to the neighbours or others. Once they get the password from admin they can access the router without the knowledge of the admin of the router. Another way is through hacking the routers using tools and some intelligent methods such as decryption, packet replay, TCP connection hijacking, HTTP content injection and others. So we need to find the solution to this issue. When we do not change the password for long period of time when they found the Wi-Fi signal after some period also they will be easily connected to the router.

IV. Real World Analysis

A survey says that more than 40 millionrouters are Vulnerable and India holding 3rd place in the list having 2 million vulnerable routers. There are no datasets available regarding security on routers, so we started to collect the data from the people who are using the wireless networks. Based on the analysis made on the acquired real-world datasets it is observed that more than 70%of people are using these wireless networks which is described in the below graph.

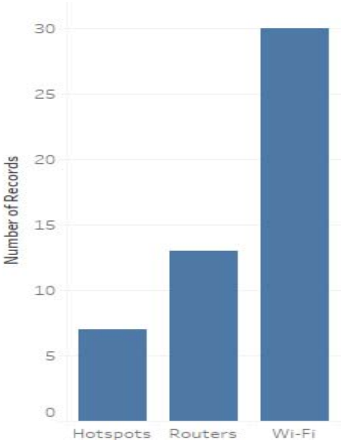


Fig.1. Describes the number of people accessing different modes of wireless networks.

From the real world analysis that we made most of the people stick on to the wireless networks rather than wired networks that too Wi-Fi are mostly using in all the places. Even though Wi-Fi used at most of the places, we don't know that they are secured or not. An analysis from the real world stated that more than 80% of people having the passwords not more than 8 characters. If the lengths of these passwords are low then obviously those wireless networks will have poor security.

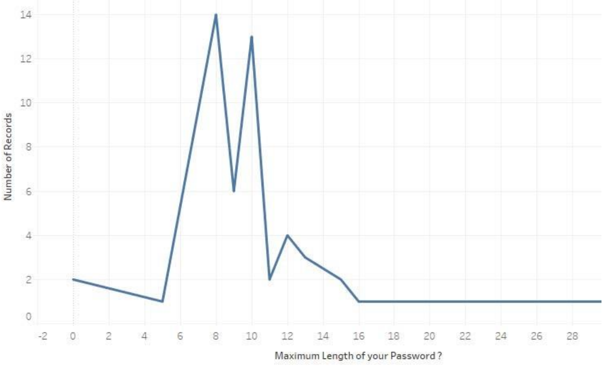


Fig.2. Describes about length of passwords versus the number of users.

The above graph depicts about the number of users in over the length of the password of the users. From the graph the peak value describes only 14 users having length of password only 8 characters and the rest of them are less than 8 characters and only few are using greater than 8 characters.

V. Proposed Model

Generally, when the user detects the Wi-Fi signal they try to connect to a router using the password to access the services provided by the router is happening now. This methodology is insecure because even if an unauthorized person gets the password and entered the password, it provides access to the unauthorized one. In our proposed model the methodology differs from the traditional one. In our approach the user had to an explicit request containing the mobile number to the router in order to access, then the router sends OTP to the requested device to establish an encrypted session between the router and the intended user. The Router process the request with data stored un the database. The database will have MAC address of the device, mobile number, IP address of the device. These router connected to both centralized and built-in database. The built-in database will contain a list of connected users who are connected to the router only. The centralized database holds all the users who are accessing the routers that are located in many places. When the users are authenticated they will acquire an encrypted password. These encrypted passwords are generated using Triple DES algorithm having 3-Keys. These three keys are like one-time pad where for each user request a 3keys are generated. The size of each key is 56 bit. So it takes more than 2100 combinations to break the process. Moreover, the keys are not static it will be difficult to break. When the requested user enters the encrypted password, if the allowed to access the router else the user will not able to access the network. These passwords will be valid until the user connected to the network. Once the users have disconnected from the network the keys and the password will be invalid. These passwords are used to dynamically authenticate the end-users. These generated passwords will not be regenerated to any other users.

TABLE1:
MEMORY STORAGE INSIDE ROUTER.

REGULAR USER	TEMPORARY USER	ERRANT USER
04:00:ff:ff:ff:d0	ec:1a:59:61:07:b	00:15:17:5f:d2:80
04:00:ff:ff:ff:a6	90:59:af:3d:6d:bc	53:ff:24:d5:e3:9k
3c:97:oe:48:22:12	00:18:31:87:8f:bo	
4c:72:b9:7c:bb:7e		

Then after storing, the router sends an encrypted password to the user through the mobile number, and then the user needs to use the password to connect to the router. The encrypted password is valid for only one user and one time only. The same password cannot be used by some other user also. The encryption is faster for every requests connection the bits are encrypted at a rate of 12bits per second. Then after getting connected to the router he/she can access the services provided by the router. All this above has to do in a minute, otherwise, the users are timed out and did not get the connection to access the router. If some errant user keeps trying to access the router their details are stored in router and admin can block them permanently then he/she didn't access the router. In case if the router cannot able to communicate with admin the router takes the decision by Machine learning process, if the requested user Ethernet address or mobile number are stored in the storage of permanent users list then router grants permission automatically without requesting the admin or in case of if the requested user is a temporary user then it router look back into databases, and calculate how much amount of time need to provide for the temporary user based on his/her previous usages. The database in the router is accessed only by the admin of the router with authentication of original passphrase of the router and along with few predefined queries set by the admin.

Incase if the person in the middle (Attacker/Hacker) captured the packet and if the person tries to connect he/she will not be connected due to the following reasons. When the router replies a packet to a user each of the packets contains Internet Control Message Protocol (ICMP). This protocol used when a message not reached at the destination it sends a reply message to a source that packet not reached the destination. Since this mechanism works based on MAC address, the attacker will not have the same MAC address for the device as same as requested user MAC address. In case a person sends a malicious packet to the router it again forwards a packet to the personal device itself.

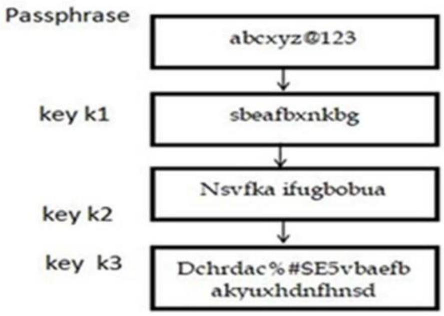


Fig.3. Working of Encryption.

.

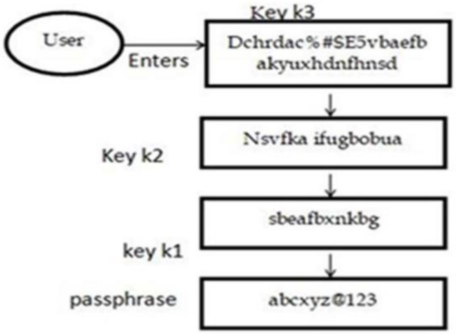


Fig.4.Working of Decryption

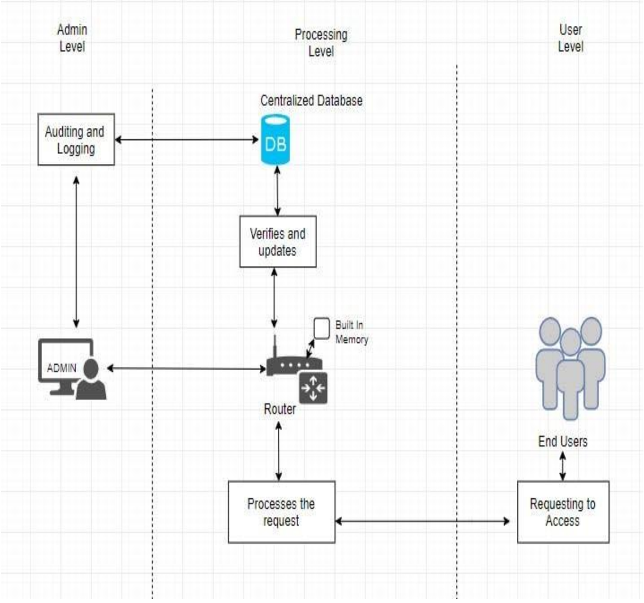


Fig.5. Working of Proposed Model.

VI. Results:

By using our proposed system we had developed the working code which accepts the users with specified MAC address and only if the encrypted passwords are matched. If they are matched then users are allowed to access the network else no longer they unable to access the network.

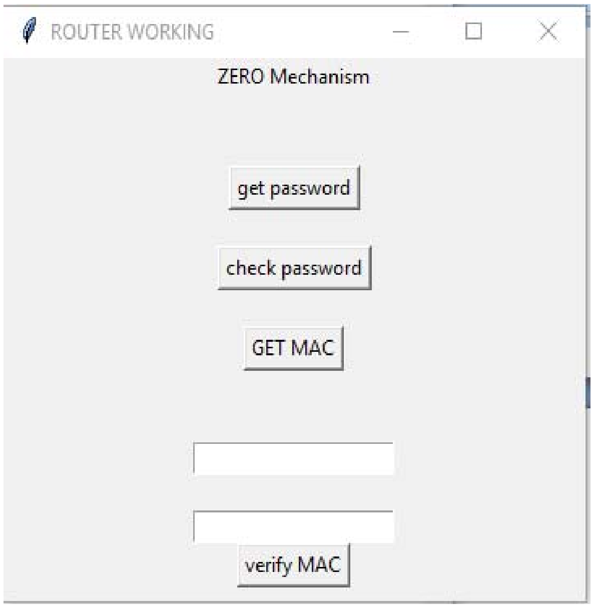
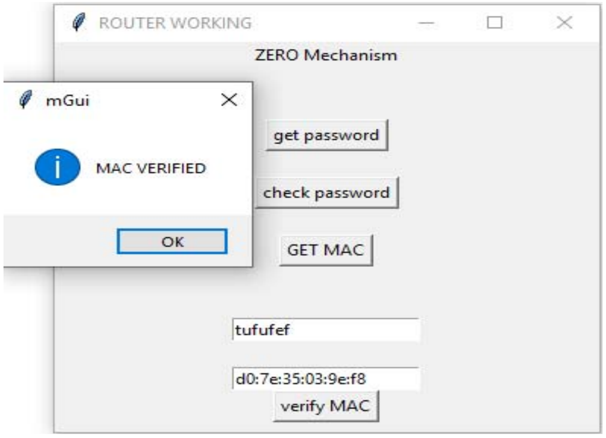


Fig.6. Describes the Graphical User Interface of our proposed system.



MAC VERIFIED

tufufef

d0:7e:35:03:9e:f8

Fig.7.Describes the working of authentication and authorization of end-users.

The above diagram describes about the working of the proposed model where we can see two entry text boxes were first textbox describes Encrypted password received from router and the second text box contains MAC address of the requested device. If the both values are correct then the permission will be granted and allowed to access the network.

VII. Merits

- The Security level of the router will be high.
- These kinds of routers can be used in Top level secured areas.
- These kinds of routers are unbreakable.
- This approach can overcome attacks like Brute Force, TCP hijacking and few more attacks.

VIII. Future Enhancement

- This approach will be used in high level secured areas where any data is highly confidential.
- In future Digital Certificates (X.509) are used in order to authenticate the end-users.
- By this mechanism, the errant users find out easily with their Geo-locations.

X. Conclusion

This approach takes few seconds for user authentication also it improves security on the router and as it monitors the users who are connected to the router, there is high-level authentication so any unknown persons can connect to the router without the knowledge of admin of the router.

REFERENCE

1.Seungwon Shin, Haopei wang, Guofei Gu, "A First Step Towards Network Security Virtualization: From Concept To Prototype", IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2236-2249, 2015.

2. Mohammed Salman Arafath ; Khaleel Ur Rahman Khan,"A survey on privacy and secure routing"2nd International Conference on Anti-Cyber Crimes (ICACC),2017.

3.G. Crosby, N. Pissinou, and K. Makki, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks", International Journal of Network Security, vol. 12, no. 2, pp. 107–117, 2011.

4. Zhiqiang Wang ; Yuqing Zhang ; Qixu Liu, "A research on vulnerability discovering for router protocols based on fuzzing", 7th International Conference on Communications and Networking in China

5. Jonny Karlsson ; Laurence S. Dooley ; Göran Pulkkis, "Secure Routing for MANET Connected Internet of Things Systems", IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud),2018

6. Fengjiao Li ; Luyong Zhang ; Dianjun Chen, “Vulnerability mining of Cisco router based on fuzzing”, 2nd International Conference on Systems and Informatics (ICSAI 2014).

7. LI Shuming, XIAO Van, LIN Qiaomin, QI Zhuzhu, "A Novel Routing Strategy to Provide Source Location Privacy in wireless Sensor Networks",wuhan University Journal of Natural Sciences, vol. 21, no. 4, pp. 298-306,2016.

8. S. Karthick ; E. Sree Devi ; R. V. Nagarajan, “Trust-distrust protocol for the secure routing in wireless sensor networks”,International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET),2017.