Empirical Investigation of Response Time of OTP Techniques in Radius Environment

By

E. A. Adedokun, Yusuf Abdullahi and M. B. Muazu
Department of Electrical and Computer Engineering
Ahmadu Bello University Zaria Nigeria
Email: wale@abu.edu.ng, yusabdu@yahoo.com & mbmuazu@abu.edu.ng

ABSTRACT

The increase in the use of computers in processing, transmission and storage of data by organizations has increase the quest for protection of data from unauthorized access. This has made network security a necessity. To protect sensitive data over the network; many security solutions and protocols have been developed. RADIUS is one of the most popular protocols used in network communication for user authentication. Unfortunately, there are several vulnerabilities in RADIUS network protocol. Researchers have presented number of techniques to reduce the effects of these vulnerabilities. One-time password (OTP) technique is one of the most important techniques which are used to enhance the security of user authentication in numerous environments and to close the potential gap in network security. In this paper, the response time of three OTP techniques, namely Time OTP (TOTP), Hash OTP (HOTP) and Challenge Response OTP (CROTP) were considered, with respect to their operation in a RADIUS environment. TOTP presented the best result with an average response time of 2.5secs, as compared to others.

Keywords: RADIUS, OTP, Remote Authentication, Response Time

INTRODUCTION

Networks are essential parts of our life because they aid communication and information sharing. These networks are used by various organizations; making their security paramount. To secure computer and network systems; components such as confidentiality, integrity, availability, accountability, security assurance and authentication must be put into consideration. Different mechanisms for protecting data over the networks, using various security protocols have been developed. Remote Authentication Dial In User Service (RADIUS) is one of the most common protocols use to secure networks; providing distributed services of Authentication, Authorization, and Accounting (AAA) for dial-up remote access. RADIUS is supported by Virtual Private Network (VPN) servers, wireless access points, authenticating Ethernet switches, Digital Subscriber Line (DSL) access, and other network access types [1].

Currently, RADIUS is the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems [2]. It is widely used in the industry as many hardware vendors support it, and there is also a lot of free and commercial software written in different programming language [3]. RADIUS consistently provides some levels of protection against sniffing and active attacks. Unfortunately, there are several vulnerabilities in RADIUS protocol that are either caused by the protocol or caused by poor client implementation such as: response authenticator based shared secret attack, Denial of Service (DOS) arising from the prediction of the request authenticator, user-password based password attack, offline dictionary attacks, online attack against the PAP (Password Authentication Protocol) and replay attack. These attacks affect the response time of the RADUIS server. OTP (One Time Password) can be used to provide secure access to remote users using different OTP techniques such as Hash OTP [4,5,6,10,11], Time OTP [4,5,8,10], and Challenge Response OTP [7,9,10]. In this paper, the aim is to investigate and analyze different OTP techniques in a RADIUS Environment using response time as the performance metrics. The rest of the paper is arranged as follows: Section 2 details about RADIUS

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

and OTP. Section 3 describes the methodology and the use cases which are implemented. Section 4 discusses about the performance of the different OTP techniques using response time as performance metric. Section 5 provides details about the related work and finally Section 6 concludes the paper.

BACKGROUND

Radius

Remote Authentication Dial in User Service (RADIUS) is a client/server security protocol that enables Network Access Server (NAS) to use shared authentication server for user authentication and authorization [12], while user profiles are stored in a central location, known as the RADIUS server. RADIUS clients communicate with the RADIUS server to authenticate users. The server specifies back to the client what the authenticated user is authorized to do [10]. RADIUS was originally developed by Livingston Enterprises for their Port Master series of Network Access Servers (NAS). RADIUS provides authentication, authorization and accounting (AAA) management for computers to connect. RADIUS is mostly used in the internet or any kind of internal networks which can be wired, wireless networks or integrated e-mail services. These networks may integrate modems, access points, DSL, access points, network ports, web servers or VPN's [9].

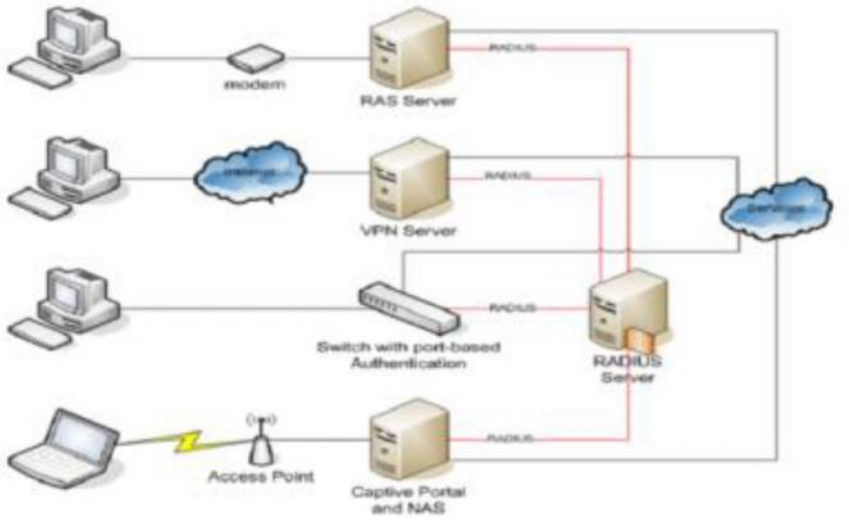

Figure 1: RADIUS Architecture [9].

RADIUS Protocol

The RADIUS protocol was first defined in Request for Comment (RFC) 2058, in January 1997, contains proposed standard of RADIUS protocol. Also, in January 1997, RADIUS accounting was introduced in RFC 2059, status of which is informational. Later in April 1997 these RFCs were obsoleted by RFC 2138 and RFC 2139. Then in June 2000 RFC 2865 defined RADIUS draft standard and obsoleted RFC 2138. RADIUS allows several clients to use one centralized authentication and authorization server for user authentication. User passwords transmitted to the server are encrypted and client can authenticate the server from reply. Replies are also protected from alteration. RADIUS protocol is used for user authentication and authorization and to pass configuration data between two servers. These servers are RADIUS server and Network Access Server (NAS) that acts as client for RADIUS server. NAS sends requests to RADIUS server which replies whether it denies or accepts the request and to pass configuration information concerning the request as shown in Figure 2 [7].

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

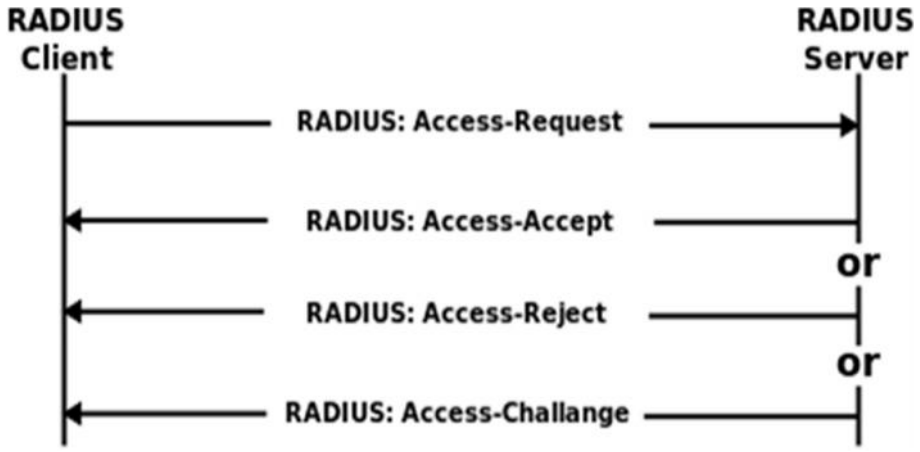

Figure 2: RADIUS Authentication and Authorization Flow [7].

RADIUS Packet and Attributes

RADIUS protocol uses UDP to carry its packets. One UDP datagram contains exactly one RADIUS packet. RADIUS packet consists of five different fields: Code, Identifier, Length, Authenticator and Attributes as in Figure 3. Length of the entire RADIUS packet is 20 octets for the Code, Identifier, Length and Authenticator. In addition to these, various numbers of Attributes can be included, and the total length of the RADIUS packet is in the Length field [14].

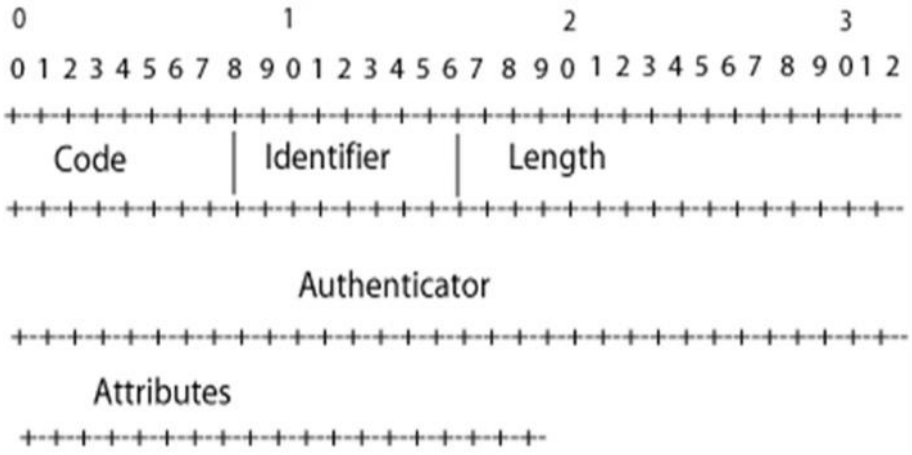

Figure 3: RADIUS Packet Format [14]

First field in RADIUS packet is the Code. It is one octet long. This field determines the type of the RADIUS packet. Second field in RADIUS packet is the Identifier. The Identifier is one octet long. Purpose of this field is to match the requests and replies. The Length field is third field in the RADIUS packet and it is two octets long. For all RADIUS packets have the Code, Identifier, Length and Authenticator fields, the minimum length of the RADIUS packet 20 octets and therefore the minimum value for Length is 20. Maximum value is 4096. Fourth field in RADIUS packet is the Authenticator. This field is 16 octets and the most significant octet comes first. This field is used for two security functions. It authenticates the reply from the RADIUS server to the NAS and is also used in encryption of User-Password attribute. Two different kinds of Authenticator fields are defined [15].

Response Authenticator is the name of the Authenticator field in Access-Accept, Access-Reject

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

and Access-Challenge type packets. The value of the Response Authenticator is calculated by the RADIUS server. For this calculation, the RADIUS server uses the values of the Code, Identifier and Length fields of the response being made, the Request Authenticator of the request, the Attributes of the response being made and the shared secret [9].

These are concatenated in this order and then Message Digest Key (MD5) hash is calculated of this concatenated string. The hash value is the response authenticator and it is expressed as follows: [16]

Response Authenticator = MD5 (Code + Identifier + Length + Request Authenticator + Attributes + Shared Secret) …(1)

In addition to previous four fields RADIUS packet can contain a number of attributes as shown in Figure 3. RADIUS uses attributes to carry additional information such as configuration data, information about the user and service. Standard length for RADIUS attribute is three fields as shown in Figure 4, but some attributes have more fields. These fields are Type, Length and Value [14].

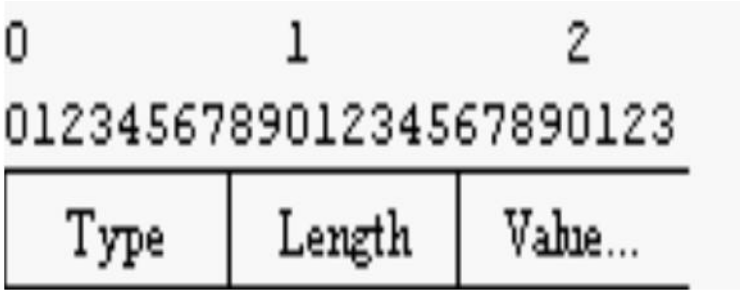

Figure 4: RADIUS Attributes [14].

Table 1: Typical Standard RADIUS Attributes [17]

6	Accounting Status	**30**	New Pin
7	Password Request	**31**	Terminate Session
8	Password Ack	**32**	Password Expired
9	Password Reject	**33**	Event Request
10	Accounting Message	**34**	Event Response
21	Resource Free Request	**40**	Disconnect Request
22	Resource Free Response	**41**	Disconnect Ack
23	Resource Query Request	**42**	Disconnect Nak
24	Resource Query Response	**43**	Change Filters Request
25	Alternate Resource Reclaim Request	**44**	Change Filters Ack
26	NAS Reboot Request	**45**	Change Filters Nak
27	NAS Reboot Response	**50**	IP Address Allocate
29	Next Passcode		

System Architecture

RADIUS protocol is used between two servers. RADIUS server is a shared authentication server that has a list of valid clients. There is a shared secret between the RADIUS server and these clients. This secret cannot be empty, but otherwise it is not defined by the protocol standard how strong it must be. It is only recommended that it is 16 octets minimum. This secret is used to authenticate the RADIUS server to the NAS and to

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

hide the user password. For these purposes the secret is part of value that is hashed and the hash value is sent [18].

RADIUS server also has a database of users containing their passwords, possible other requirements for these users to gain access and configuration data. According to information in this database, the RADIUS server accepts or rejects the request or sends a challenge to user. RADIUS server can also act as a proxy relaying requests to another RADIUS server and to NAS. When acting as proxy RADIUS server replies messages between the NAS and another RADIUS server. There can be many RADIUS servers as proxies between the NAS and the RADIUS server that handles the authentication and authorization of the request [18].

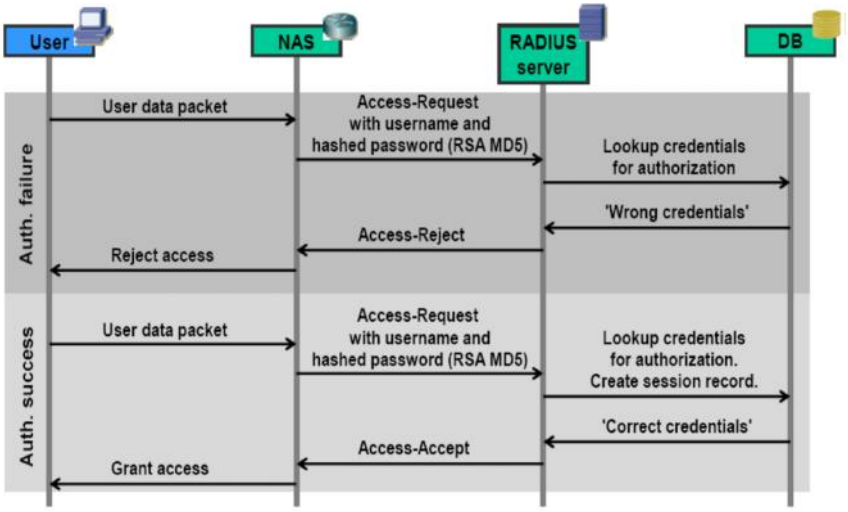

Figure 5: Authentication Flow [13]

One Time Password (OTP)

One Time Password OTP is an instant password, in other words it is a code that change after each use and uses it to authenticate [8]. OTP are passwords that are only valid for a single or small number of transactions. An attacker has a smaller period of time to gain access to resources protected by such password because any previously stolen passwords will likely have become invalid. That means adding some uncertain factors in the procedure of authorization. The information transmitted over network is different, thus the security is improved [9]. OTP has a characteristic making it impossible to predict the next password from the current password; also, they are not vulnerable to replay attacks [19]. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords [8]. OTP is based on a cryptographic algorithm [20].

Cryptogram=f (k) … (2)

Where key k is a cryptographically generated

Computing the cryptogram with factors makes the output random and on time, cryptographic algorithms-based counter also called even and based time (e.g. seconds) with triple factor, f1: key k a cryptographic is generated, f2: T refers to time factor, f3: C refers to counter factor. While f1.i is number of factor, equation (2.1) shows a cryptographic algorithm of OTP. Fig. 2.7 explains OTP generation process.

Cryptogram=f (k, C, T) … (3)

Generation OTP and distribution: The process of the OTP generation consists of

i) Input value.
ii) OTP generation.
iii) OTP extraction.
iv) Time.

The OTP generation algorithm generates an OTP value from an input value (users' strong password and secret key). It is based on hash functions for message digest (MD5) and uses the shared input value between the server and the OTP

Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

generator [20]. The generation algorithm uses a time value, a counter value and a challenge value as the key and data. The extraction algorithm of the OTP value extracts the real OTP value from the output value of the OTP generation algorithm.

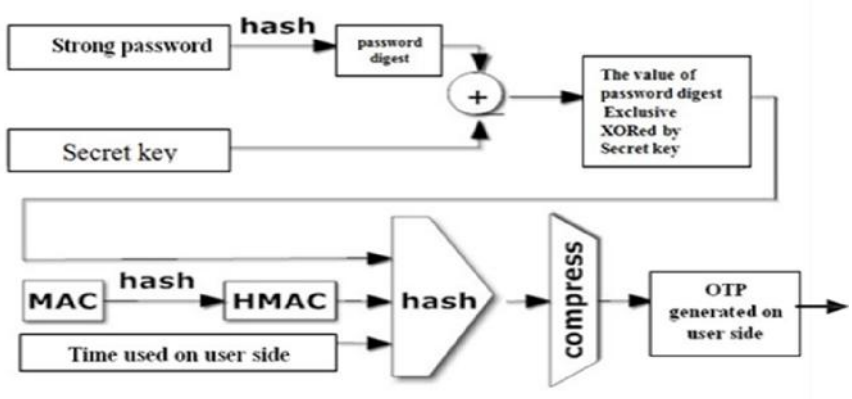

Figure 6: OTP Generation [10]

Approaches for the generation of OTP

There are three major technique used for generation of OTP [15]:

(1). TIME SYNCHRONIZATION

In this technique, both the client and server will have synchronous time clocks. In this approach time is used as a changing factor which changes every 3 minutes. The generation time must be synchronized with the authentication server time. If the authentication server and the user do not keep the same time, then the expected OTP value won't be produced and the user authentication will fail [15]. With time-synchronized OTPs, the user typically must enter the password within a certain period of time before it is considered expired and another one must be generated [21]

(2). EVENT SYNCHRONIZATION

In this technique, both the client and server will typically have a counter value. Whenever client wants to login, it generates OTP from the counter value and any other input Personal Identifier Number (PIN) and updates the counter. User submits the generated OTP to server. Server also generates the password using the counter. If password match, the server authenticates the user and updates the counter (increment/ decrement the counter), it may happen that the counter on client and server may drift (due to passwords generated by client but not submitted, passwords submitted by client but does not reach to server due to network failure, etc.). [15]

(3). CHALLENGE – RESPONSE TECHNIQUE

In this technique, a random number (PIN) chosen by the authentication server is sent to a user, the user enters PIN value then sends response to the server. This technique based on a challenge response. [6]

Types of OTP techniques

The following are the different types of OTP techniques:

(1). HASH ONE TIME PASSWORD (HOTP) TECHNIQUE

The HOTP technique is based on an increasing counter value. Both the client and server will typically have a counter value. Server generates the password to use the counter. If passwords match, the server authenticates the user and updates the counter increment/ decrement the counter), it may happen that the counter at client and server may drift (due to passwords generated by client but not submitted, or passwords submitted by client but does not reach to server due to network failure, etc.) [8]. In this case it will respond to server with denial service. The steps in generation of HOTP technique is shown in Table 2 [5].

Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

Table 2: Steps in Generation of HOTP Technique [5]

Steps	Description
1.	The user enters the username and password in the login screen. The password should contain more than six characters.
2.	The system sends user data to the RADIUS server to authenticate the user.
3.	The RADIUS server verifies the username and password and sends a response either accept or reject.
4.	The user opens the OTP application and enters the PIN.
5.	The OTP application provides the generated OTP for the system user.
6.	The user enters the PIN and the generated OTP through the system.
7.	The system sends a request to the AS to check the last OTP, the PIN and the secret key of the system user.
8.	The AS verifies user OTP and sends a response to system either accept or reject.

(2). TIME ONE TIME PASSWORD (TOTP) TECHNIQUE

The TOTP technique [7] that is a time-based OTP. Time dynamism is an OTP generation principle widely utilized in two factor authentication schemes; two factor authentications based on PIN identification as first factor and OTP generation (different password) as second factor to increase security. Different password is needed for different time to prevent number of attacks, this schema depends on two periods, static period is designed for user to input the OTP into the login form upon receipt of the dynamic period password, and the length of which can always be customized by the client [10]. The steps in generation of TOTP is shown in Table 3 [22].

Table 3: Steps in Generation of TOTP [22]

Steps	Description
1.	The user enters the username and password in the login screen. The password should contain more than six characters.
2.	The system sends user data to the RADIUS server to authenticate the user.
3.	The RADIUS server verifies the username and password and sends a response either accept or reject.
4.	The user opens the OTP application and enters the PIN.
5.	The OTP application provides the generated OTP for the system user. This OTP is expired after 3 minutes.
6.	The user enters the PIN and the generated OTP through the system.
7.	The system sends a request to the AS to check the last OTP, the PIN and the secret key of the system user.
8.	The AS verifies user OTP and sends a response to system either accept or reject.

(3). CRYPTOGRAPHY ONE TIME PASSWORD (CROTP) TECHNIQUE

CROTP [6] is a generalization of HOTP with variable data inputs that based on an incremented counter and secret key values [8]. It is used in several network protocols such as RADIUS, Kerberos and digest access authentication. The definition of CROTP requires a cryptographic function, a key K and a set of data input parameters [23]. Instead of a shared counter value, a challenge is issued from the validation server to the user. The user would then input this challenge to receive the OTP value: [23]

CROTP=CryptoFunction (K, DataInput) **…** (4)

Where K represents a shared secret key,

Data-input function represents input data values; cryptofunction represents functions that perform the CROTP. In details Inputs that are based

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

on challenge response (CR) authentication mechanism consists of the server which presents the user with an unpredictable challenge every time the user attempts to authenticate. For every challenge, there is an associated response that allows the user to be authenticated. [6]

Table 4: Steps for Generation of CROTP Technique [24]

Steps	Description
1.	The user enters the username and password in the login screen. The password should contain more than six characters.
2.	The system sends user data to the RADIUS server to authenticate the user.
3.	The RADIUS server verifies the username and password and sends a response either accept or reject.
4.	The system provides a random PIN to challenge the user
5.	The user opens the OTP application and enters the system random PIN.
6.	The OTP application provides the generated OTP for the system user.
7.	The user enters the generated OTP through the system.
8.	The system sends a request to the AS to check the last OTP, the random PIN and the secret key of the system user.
9.	The AS verifies the user OTP and sends a response to system either accept or reject.

METHOD

The methodology adopted is based on the designed, configurations and simulations of a campus network to identify the response time on the three variants of OTP in a RADIUS environment, using captive portal, GNS3 and virtualbox. Simulation software's were used to configure the network devices and the installation of the Linux operating system with free RADIUS 2.0, with firewall on the virtualbox environment, the Network Access Server which provides the captive portal was also installed on the virtualbox.

The Campus Network

The routers in the topology were configured to run using Mikrotik router operating system to simulate the real live campus network design and configuration. The authentication server uses Ubuntu server 14.0 with firewall and FreeRadius2 installed on it, the three OTP variant will also be implemented on this server together with the OTP generator. While the windows machine is used as the user's machine which are connected to the virtualbox using the GNS3 simulator**.**

Captive Portal Implementation

The captive portal was implemented on the Network Access Server (NAS) which also resides on the Ubuntu Linux server, the captive portal is developed using the PHP programming language. The captive portal is the screen that appears when user accesses resources on the network, it consists of fields such as the login, password, self-registration, and drop-down button to select different types of OTP technique.

OTP Generation Scenarios

This sub-section describes the OTP generation scenario to show how the user OTP is generated through OTP application. The OTP application is developed using a PHP developed script. After the user is authenticated (sign-in process) by RADIUS server, the system transmits the user to the OTP page which is an important page in the login process in the captive portal. The user must open the OTP application and enter the PIN and then get the OTP which is generated by one of the three OTP variants. Finally, the user takes the OTP and enters the PIN and OTP in the OTP page of the system. After that the user can login to the system if the matching process is verified and certified ok by the authentication server.

Obtaining Usernames, Pin and OTP

The user can register self on the server from the captive portal, and then the user is prompt

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

to select desired PIN. Then, the user will generate the desires OTP from the three techniques using the developed OTP generator.

User Login Scenario

The user login scenario offers a set of cases for login process in the RADIUS server. In section 3.5, each case passes the system user in several stages in order to login to the network. These cases are mentioned as follows:

Case 1: The valid user

a) A user login to the network by providing username and password.
b) The RADIUS server sends a response accepting the credentials.
c) The system redirects the user to OTP page; the user provides PIN and OTP.
d) The system sends the PIN and OTP to authentication server (AS) which checks PIN, last OTP and secret key and then AS sends an acceptance response to the system.
e) The authentication result in this case is successful and the user can login to network.

Case 2: The missing user name

a) A user attempts to login to the network without providing username.
b) The RADIUS server sends a rejection response.
c) The system prevents this user from login to the network.

Case 3: Invalid password

a) A user login to the system by providing valid username and invalid password.
b) The RADIUS server sends a rejection response.
c) The system does not response to user

Case 4: Invalid OTP

a) A user login to the network by providing username and password.
b) The RADIUS server sends a response accepting the credentials.
c) The system redirects the user to the OTP page; the user provides valid PIN and invalid OTP.
d) The system sends the PIN and the invalid OTP to AS which verifies PIN, last OTP and secret key and then AS sends a rejection response.
e) The authentication result of this case is failed.

Case 5: Invalid PIN

a) A user login to the server by providing valid username and password.
b) The RADIUS server sends a response accepting the credentials
c) The system redirects the user the OTP page, and the user enters invalid PIN and valid OTP.
d) The system sends the PIN and the OTP to AS which verifies PIN, last OTP and secret key and then AS sends a rejection response.
e) The authentication result of this case failed.

Hardware Requirements

The simulated ABU network environment using GNS3 was adopted and configured on a live server, using the following devices:

1) Dell power edge server with 8GB of RAM, 500GB of Hard disk drive and 2.3GHz processor with Linux operating system, FreeRadius 2.0 and Firewall were installed on the server.
2) Mikrotik router with router operating system version 6.35
3) Cisco switches 3750 and 2960

RESULTS

The modeled campus network in GNS3 modeler environment is simulated for ten users averagely to represent a response time for each user using the three variants of OTP. To measure the server response time, ten different cases are offered for each of the three OTP techniques. These cases show the server response time for each request by the system user. Table 5 shows the user request time and its response time by the server, for the three OTP techniques.

The Unix time stamp is a way to track time as a running total of seconds. This count starts at the Unix Epoch on January 1st, 1970 UTC. The Unix time stamp is merely the number of seconds between a particular date and the Unix Epoch. For example, the user request time for case 1 is equal to 1447419898 as timestamp. This case is equal to 13/11/2015, 3:04:58pm as current date using a timestamp converter.

From the Table 5, the average response time for TOTP 2.5sec., HOTP is 5.7s and CROTP is 5.2sec. These results were obtained when the OTP generators and the RADIUS servers were

Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

separated. From these results, it can be concluded that the TOTP has the least response time, while the HOTP has the highest response time. These values are higher than the recommended response time for a captive portal in a RADIUS environment which is approximately 1000ms.

Table 5: Server Response Time for Three OTP Variants

Case	Request time	Response time	Technique Type	Drift Second
1	1447419892	1447419895	TOTP	3
2	1447420040	1447420044	TOTP	4
3	1447510055	1447510056	TOTP	1
4	1447510225	1447510226	TOTP	1
5	1447510511	1447510517	TOTP	6
6	1447510737	1447510738	TOTP	1
7	1447513402	1447513404	TOTP	2
8	1447514101	1447514106	TOTP	5
9	1447514384	1447514385	TOTP	1
10	1447514696	1447514697	TOTP	1
11	1447505190	1447505196	HOTP	6
12	1447504833	1447504837	HOTP	4
13	1447505111	1447505119	HOTP	8
14	1447505521	1447505525	HOTP	4
15	1447505981	1447505988	HOTP	7
16	1447506642	1447506650	HOTP	8
17	1447507060	1447507068	HOTP	8
18	1447507511	1447507516	HOTP	5
19	1447507873	1447507878	HOTP	4
20	1447508422	1447508425	HOTP	3
21	1447578601	1447578619	CROTP CROTP	8
22	1447578922	1447578930	CROTP CROTP	8
23	1447579244	1447579246	CROTP	2
24	1447579532	1447579538	CROTP	6
25	1447579869	1447579873	CROTP	4
26	1447580235	1447580241	CROTP	6
27	1447580739	1447580744	CROTP	5
28	1447581432	1447581437	CROTP	5
29	1447581927	1447581932	CROTP	5
30	1447582628	1447582631	CROTP	3

CONCLUSION

In this paper the RADIUS protocol was implemented on the three OTP techniques in a RADIUS environment with captive portal. This work is aimed at providing remote authentication on a network using RADIUS, by evaluating the three variants of OTP techniques with the aim of selecting and adopting the one that has the best response time for further improvement. The result obtained is lower than the recommended response time of a RADIUS server in a captive portal environment, which is 1000ms. The TOTP technique is the recommended technique to adopt having the lowest response time.

REFERENCES

[1] Hashmathur Rehman1. Govardhan T. Venkat Narayana Rao, "Design and Implementation of RADIUS A Network Security Protocol", Global Journal of Computer Science and Technology, P a g e 48 Vol. 10 Issue 7 Ver. 1.0 September 2010.

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)

[2] Ji Cao," AAA Functionality for Handheld Systems", master thesis 2005.

[3] Havard Raddum, Lars Hopland Nestas, and Kjell Jrgen Hole," Security Analysis of Mobile Phones Used as OTP Generators ", page 324-331, IFIP International Federation for Information Processing 2010.

[4] Andrew Y. Lindell,"Time versus Event Based One-Time Passwords", the foundation of information security, white paper, 2002.

[5] Bellare, Hoornaert, Naccache," HOTP: An HMAC-Based One-Time Password Algorithm" ,RFC4226, 2005

[6] Bellare, Hoornaert, Naccache, "CROTP: OATH Challenge-Response Algorithm", RFC4226, ISSN: 2070-1721, 2011.

[7] D. M'Raihi," TOTP: Time-Based One-Time Password Algorithm", Internet Engineering Task Force (IETF), 2011.

[8] Sung-Jae Lee, Jae Seong Lee, Mun-Kyu Lee, Sang Jin Lee, Doo-Ho Choi, and Dong Kyue Kim,"Low-Power Design of Hardware One-Time Password Generators for Card-Type OTPs", ETRI Journal, Volume 33, Number 4, August 2011.

[9] Trupti Hemant Gurav1, Manisha Dhage2,"remote client authentication using mobile phone ", International Journal of Scientific and Research Publications, Volume 2, Issue 5, May 2012, page 5549-5555, ISSN 2250-3153.

[10] Xuguang Ren, Xin-Wen Wu，and Kun Tang, " TSPass: A Dynamic User Authentication Scheme Based on Time and Space", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.10, October 2012.

[11] Balkis Hamdane y, Ahmed Serhrouchni y, Adrien Montfaucony, Sihem Guemara," Using the HMAC-Based One-Time Password Algorithm for TLS Authentication", page 1-8 2011 conference IEEE.

[12] madhuri and ramana lakshmi "attack patterns for detecting and preventing ddos and replay attacks", international journal of engineering and technology vol. 2(9), page 4850-4859, 2010.

[13] Chii-Ren Tsai, "Non-Repudiation in Practice", Citigroup Information Security Office 2003.

[14] Rigney, C. S. (2007). Remote Authentication Dial in User Services (RADIUS). Internet Engineering Task Force (IETF).

[15] Namrata, T. V. (2013). An Approach of Authentication in Public Cloud using Two Step Verification Code. International Journal of Emerging Research in Management &Technology, 2(5).

[16] Mikko, S. (2004). Legacy User Authentication with IPSEC. Retrieved from http://www.tml.tkk.fi/Publications/Thesis/msaarinen.pdf

[17] Hassel, J. (2003). Securing Public Access to Private Resources RADIUS (First Edition ed.). (J. Sumser, Ed.) California CA: O'Reilly & Associates, Inc.

[18] Jaakko, T. (2014). Overview, details and analysis of Radius protocol. Retrieved from Cisco how radius works, Authentication, Authorization and Accounting: http://www.cisco.com/image/gif/paws/12433/32.pdf

[19] Gagan, D. N. (2013). replay attack prevention in Kerberos authentication protocol using triple password. International Journal of Computer Networks & Communications (IJCNC), 5(2).

[20] Himika Parmar, Nancy Nainan and Sumaiya Thasee," Generation of Secure One-Time Password Based on Image Authentication, Computer Science & Information Technology (CS & IT), 2012, pp. 195–206,

[21] Binod, V. (2013). HOTP-Based User Authentication Scheme in Home Networks. IJCSNS International Journal of Computer Science and Network Security, 1-10.

[22] Amna. (2014). Implementing and Comprising of OTP Techniques (TOTP, HOTP, CROTP) to Prevent Replay Attack in RADIUS Protocol using ELSBOT. Retrieved from http://library.iugaza.edu.ps/thesis/113489.pdf

[23] Alan, H., (2013). A Methodology for Analyzing the Performance of Authentication Protocols. IEEE, 5(10).

[24] Kun Tang. (2014). A Dynamic User authentication based on time and space. IJCSNS International Journal of computer science and network security, volume 15(13).

 Copyright © 2017 JOSTE. All Rights Reserved (www.atbuftejoste.com)