Performance Analysis of Microsoft Network Policy Server and FreeRADIUS Authentication Systems in 802.1x based Secured Wired Ethernet using PEAP

Farrukh Chughtai[1], Riaz UlAmin[1], Abdul Sattar Malik[2], and Nausheen Saeed[3]
[1]Department of Computer Science, Balochistan University of Information Technology Engineering and Management Sciences, Pakistan
[2]Department of Electrical Engineering, Bahauddin Zakariya University, Pakistan
[3]Department of Computer Science, Sardar Bahadur Khan University, Pakistan

Abstract: *IEEE 802.1x is an industry standard to implement physical port level security in wired and wireless Ethernets by using RADIUS infrastructure. Administrators of corporate networks need secure network admission control for their environment in a way that adds minimum traffic overhead and does not degrade the performance of the network. This research focuses on two widely used Remote Authentication Dial In User Service (RADIUS) servers, Microsoft Network Policy Server (NPS) and FreeRADIUS to evaluate their efficiency and network overhead according to a set of pre-defined key performance indicators using Protected Extensible Authentication Protocol (PEAP) in conjunction with Microsoft Challenged Handshake Authentication Protocol version 2 (MSCHAPv2). The key performance indicators – authentication time, reconnection time and protocol overhead were evaluated in real test bed configuration. Results of the experiments explain why the performance of a particular authentications system is better than the other in the given scenario.*

Keywords: *IEEE 802.1x, Microsoft NPS, FreeRADIUS, PEAP, MSCHAP2, performance analysis, RADIUS.*

Received May 28, 2016; accepted May 29, 2017

1. Introduction

802.1x is an IEEE standard that provides a reliable solution for network access/admission control through port-based authentication in enterprise networks. It is widely implemented in wired and wireless networks to secure and isolate network for servers, computers, internetworking devices, peripherals and users' owned mobile devices. By keeping Wireless Local Area Network (WLAN) secured, and physical ports unprotected, many network administrators expose their network to serious threats that may result in performance degradation to total loss of services.

The research community has paid little attention to wired security and left most of the work up to the vendors to introduce new protocols and services. Availability of various proprietary and open source authentication systems gives freedom to the implementers to adopt technology according to their environment, while leaving them on their own to determine the impact on network performance. Careful examination is required while implementing 802.1x authentication in largescale networks where even small traffic overhead may lead to a considerable degradation in network performance especially when there are a large number of concurrent users on the network.

This research focuses on the performance analysis of two commonly used authentication systems in802.1x deployment i.e., Microsoft Network Policy Server (NPS) and Remote Authentication Dial in User Service (FreeRADIUS).

Extensible Authentication Protocol (EAP) as defined in Internet Engineering Task Force (IETF) Request For Comments (RFC) 3748 [1, 2] is a layer 2 protocol that works with IEEE 802 networks without requiring IP; thus, making it the best choice for network authentication. Protected Extensible Authentication Protocol (PEAP), an extension to EAP, was evaluated for its performance on the two authentication systems keeping the authenticator and the supplicants (clients) unchanged.

Microsoft NPS and FreeRADIUS were setup in real testbed environment i.e., no simulator was used and PEAP was evaluated for its performance using MSCHAPv2 over the 802.1x network as per predefined performance matrix that include authentication time for successful and failed authentication, reconnection time and packet overhead in successful, failed and reconnected authenticated sessions. The performance evaluation is critical for large networks where a small difference in performance indicators can result in considerable effect on the network due to large number of concurrent 802.1x sessions.

Ethernet has revolutionized the world of Information Technology (IT). Inheriting its basic

design of being flexible, decentralized and cost effective, it not only proved to be a practical networking solution for businesses, government offices and large enterprises, but also provided a solid infrastructure for the globally used "Internet". The last decade saw a major advancement in the field of wireless networking that emerged as a foundation for mobile computing. Despite having flexible wireless networks and their widespread usage in all fields, wired LANs are still considered to be at the core of every small to large scale network. It is an established fact that the academic research community paid little attention to the architectural security in the wired Ethernet and left most of the work to the equipment manufacturers while giving more emphasis on the higher level protocols and wireless networks [13].

Physical access ports to the wired Ethernet are found in almost every network and majority of them lack security on the network access. This drives the attention of the network professionals to implement a technique of Network Access Control (NAC) also referred to as Network Admission Control by different equipment manufacturers.

The prime objective of having NAC in place is to validate the connecting entity prior authorizing it for a network resource; so that only authenticated users/ devices can participate over the network and acquire services according to the established access policies [11, 17]. If the user is successfully authenticated, the appropriate network access is granted, otherwise the port itself is isolated from the LAN so that no communication could be made to any part of the network. In some cases, it is possible to implement remediation strategy to make the newly connected computer/ device policy compliant to the minimum standards set by the network administrator, and once the policy requirements are met, access to the network is granted to the newly connected device.

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard for port-based network access control. It is a layer 2 protocol utilizing Extensible Authentication Protocol or its variants to authenticate user or machine accounts against an external authentication system over a wired network [10, 19]. It was originally designed for wired networks but also gained its popularity for the wireless networks by providing a framework for authentication in the form of a user name / password or a cryptographic key in the form of a digital certificate. It gives a solid foundation to implement guest access control in a corporate network also incorporated with Bring Your Own Device (BYOD) environments [15].

802.1x provides connectionless secured services at Logical Link Control (LLC) sub layer of the Data Link Layer [4] to various standards in 802 family for local and metropolitan area networks including Ethernet, Token Ring and 802.11 wireless networks.

The structure of 802.1x protocol is comprised of 3 major components:

1. Supplicant System-The client side software, installed on the user's computer/ device requesting network access. It utilizes Extensible Authentication Protocol over LAN (EAPoL) to initiate the authentication process. The supplicant system is nowadays an integral part of the wired (802.3, 802.5) and wireless (802.11) connection suites on almost every Operating System and can easily be activated if not done by default.
2. Authenticator System-A device supporting 802.1x protocol that resides in the middle of the supplicant system and the authentication system. Switches and Wireless Access Points are the most common examples of an authenticator system. The authenticator utilizes a dual port model to facilitate the authentication process using Controlled and Uncontrolled ports. These ports should not be confused with physical ports; in fact, these are two different logical states of a physical port of a manageable Layer 2 switch. The Uncontrolled port is always open and is used to facilitate the supplicant (authenticating device/user) to contact the appropriate authentication services available on the network by allowing the EAPoL traffic only. The Controlled port remains down until the supplicant is successfully authenticated via uncontrolled ports. The authenticator system then opens the controlled port for the authenticated device and allows access to the LAN resources.
3. Authentication Server-Usually a RADIUS server and Authentication, Authorization and Accounting (AAA) protocol to authenticate users [8] by storing user information such as User names IDs and Password, schedule of network usage and type of service allowed for the supplicant. It is also possible to integrate a certificate authority with 802.1x system and use external user accounts repository like Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) instead of the credentials stored on the RADIUS server. A RADIUS server can easily be implemented on common server operating systems using built-in components such as Microsoft RADIUS services or installing an open source produce like FreeRADIUS. The following adapted Figure 1 describes the authentication framework based on the 802.1x infrastructure.

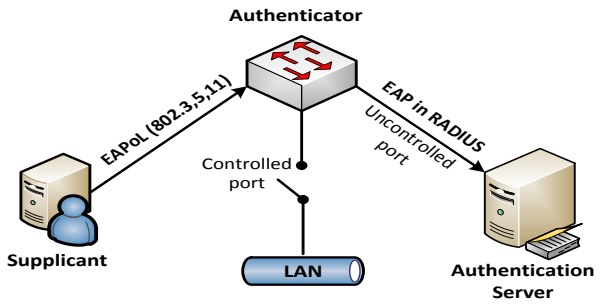

Figure 1. Components of 802.1x framework.

When a new device connects to an 802.1x network, the authenticator challenges the user for its identity. The switch ports will simply deny the network access if the supplicant is not installed or running on the connecting device. The connecting device, using its supplicant, passes the network credentials or the certificate to the authentication server using EAPoL over the uncontrolled port of the authenticator (switch or access point). If the authentication is successful, the controlled port opens for the connecting device and traffic is allowed over the LAN. Otherwise, the controlled port remains down and no direct connection to the LAN can be made. It is mandatory for both supplicant and the authenticator to support 802.1x features.

2. Literature Review

2.1. Extensible Authentication Protocol

EAP is an authentication framework running on data link layer such as Point to Point Protocol (PPP) or IEEE 802 without requiring Internet Protocol and supports multiple authentication methods [1]. EAP can be used on dedicated links as well as switched circuits over wired and wireless medium. It can be used at a variety of lower level layers including Point-to-Point Protocol PPP, Layer 2 Tunnelling Protocol (L2TP), Point-to-Point Tunnelling Protocol (PPTP), IEEE 802 wired networks (IEEE-802.1x) and wireless technologies like IEEE 802.11 (Wireless LAN or Wi-Fi) and IEEE 802.16 (Broadband Wireless Access or WiMAX).

EAP provides the flexibility to select a specific authentication mechanism configured at the backend authentication system instead of requiring an authenticator to support all authentication methods or without pre-negotiating a pre-defined mechanism.. The use of backend authentication system also helps implementing organizational policies for different access rights, credentials management and network isolation using dynamic VLAN tagging.

2.2. Protected Extensible Authentication Protocol

PEAP was originally designed by Microsoft [14] as an extension to the Extensible Authentication Protocol to provide an additional layer of security during password negotiation phase of 802.1x connections. It combines the features of TLS and standard EAP authentications by establishing a TLS session by using a server side certificate before actually validating the credential supplied by the supplicant.

PEAP messages (32 bits in length) are transported from supplicant to authenticator over a lower-layer protocol such as 802.1x or PPP whereas RADIUS takes care of the PEAP communication between the authenticator and the authentication system. The following adapted Figure [14] labelled as Figure 2 presents a typical deployment of PEAP.

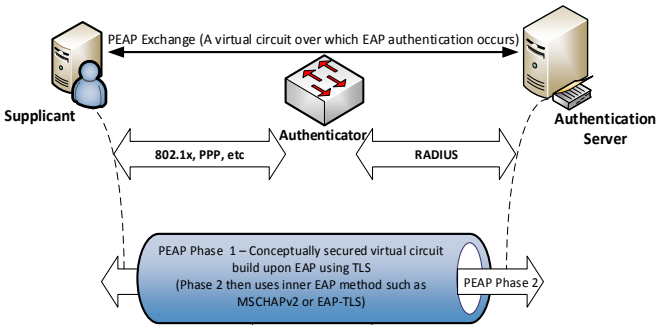

Figure 2. Typical deployment of PEAP.

PEAP offers a number of advantages over other EAP methods (EAP-MD5, EAP-TLS, etc) such as:

- PEAP utilizes TLS channel to secure the password based credential.
- PEAP supports all kinds of EAP types including certificates, MSCHAPv2, passwords, users, machines identities, etc.
- PEAP hides the user identity and the methods used in the tunnel during mutual authentication, that helps avoiding an attacker inject packets between the authenticator and the supplicant.
- PEAP does not require certificate to be deployed to every supplicant. It can easily be deployed in the environments lacking Public Key Infrastructure (PKI) or Certificate Authority (CA) and can be used with a variety of access methods such as dial-up connections, wired or wireless Ethernet, Virtual Private Network (VPN), and Point to Point Protocol over Ethernet (PPPoE).
- PEAP supports TLS session resumption, therefore it is a suitable protocol for delay sensitive traffic in roaming environments.
- Since PEAP is an open standard, more and more vendors are adding its support to their products including proprietary and open source products.

2.3. 802.1x Authentication Procedure

The following Figure 3 summarizes the steps involved in 802.1x authentication [16].

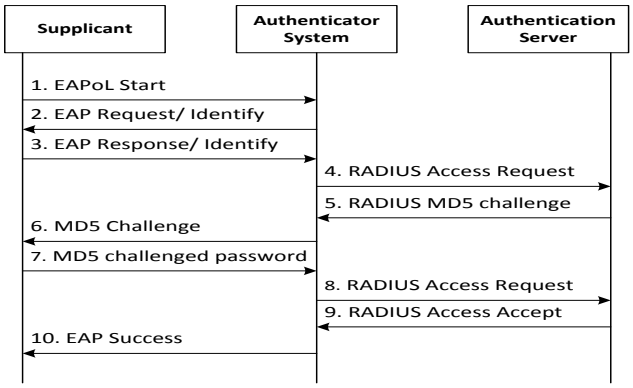

Figure 3. 802.1x Authentication process.

The Start and Success EAP messages are not acknowledged, therefore they are not retransmitted by the authenticator. MD5 is the simplest authentication algorithm in EAP; one can use different authentication algorithms (MD5, LEAP-TLS, EAP-TTLS, PEAP, etc.,) to match the required level of encryption. Only a single authentication algorithm or EAP method is allowed in one conversation. The following Table 1 [5, 6] summarizes the common EAP methods:

Table 1. Common EAP methods.

EAP Method Name	Features					
	Authentication Attributes	Deployment Difficulties	Dynamic Re-Keying	Require Server Certificates	Require Client Certificates	Tunnelled
MD5	Unilateral	Easy	No	No	No	No
LEAP	Mutual	Easy	Yes	No	No	No
TLS	Mutual	Hard	Yes	Yes	Yes	No
TTLS	Mutual	Moderate	Yes	Yes	No	Yes
PEAP	Mutual	Moderate	Yes	Yes	No	Yes

EAP-TLS provides the highest level of security but is hard to implement because of the involvement of certificates both at server and client end. In this research scenrio, only server-side certificate will be used, therefore EAP-TLS and EAP-TTLS are the available choices. EAP-TTLS has the advantage of broader compatibility and support of legacy protocols, but PEAP supports newer operating systems and authentication mechanisms such as MSCHAPv2. PEAP provides a balance between the best security and ease of implementation, therefore the experiments in this research will be carried out using MSCHAPv2.

Access to the network is regulated by using the feature of Virtual LAN (VLANs) on the authenticator. A VLAN, by its nature, reduces the broadcast traffic and allow us organizing LANs logically instead of physically thus improving scalability, security and traffic control [3]. The controlled port can be regulated in such a way that an unauthenticated device may be put in to a restricted VLAN by allowing some services, such as allowing Internet traffic but no access to internal application servers or can be put into a VLAN of blocked ports with no access to the LAN [10, 17].

2.4. Remote Authentication Dial In User Service (RADIUS)

IEEE 802.1x by design does not require a central implementation of Authentication, Authorization and Accounting (AAA) [7] but keeping in mind the scale of implementation in enterprise networks, a backend deployment of AAA is highly desirable and most of the authenticators will act as RADIUS clients.

RADIUS implements an AAA model as defined in [5] and uses elements called “Attributes” to depict the data regarding to authentication, accounting and authorization events. In general, Authentication is to validate the identity of the contacting user or machine, Authorization is to make sure that the contacting endpoint is matched against the predefined set of rules to make sure it is permitted to use the requested resource, such as a network, a VLAN or a service; while accounting components records all relevant information about the authorization decision and information about the activities of the authorized sessions.

2.5. RADIUS Attributes

RADIUS attributes are classified into three major categories

1. Vendor specific attributes–these are usually not interoperable with other vendors.
2. Industry specific attributes–interoperable with other vendors in the same industry.
3. Internet specific attributes–interoperable with other vendors, platforms and technologies in multiple industries.

These attributes are used authenticate users, authorize users for difference services or changes in services and account them for the network activities through logging mechanism.

The following Table 2 summarizes few commonly used RADIUS attributes along with their function:

Table 2. Common RADIUS attributes.

Number	Radius Attribute	Description
1	User-Name	Specifies the username to be matched to the user database of authentication system
2	User-Password	Password of the user in response of Access challenge
3	NAS- IP Address	IP address of network access server, requesting authentication
5	NAS-Port	Physical port number of the network access server
6	Service Type	Type of service requested or provided such as login, framed, call-back login, authenticate only
7	Framed Protocol	Predefined framing to be used such as PPP, SLIP
8	Framed IP Address	IP to be assigned to the user (Dynamic)
11	Filter-ID	To define network access policies based on type of connection request such as type of user etc.
61	NAS-Port Type	Type of physical port or media such as Ethernet wired or wireless, Token Ring, ISDN, virtual etc.
64	Tunnel Type	Type of Tunnel such as layer-2 forwarding, L2IP, VLAN etc.

2.6. MSCHAPv2

Microsoft Challenge Handshake Authentication Protocol v2 as defined in RFC2759 is an authentication method used in EAP framework RFC 3748 [1]. It is used to enable authenticated and authorized users and devices to access the network locally (wired or wireless) or remotely via Virtual Private Network (VPN). MSCHAPv2 allows the client and server authenticate each other using shared authentication.

The successful authentication mechanism is described below:

1. The supplicant and the authentication server establish an EAP session.
2. Both negotiate for the EAP method to use; MSCHAPv2 is selected once PEAP is configured as the as the authentication method.
3. The endpoints try to authenticate each other by exchanging MSCHAPv2 messages encapsulated in a lower level protocol such as 802.1x, PPP, EAP, PEAP or RADIUS. This is described in the Figure 4:

MSCHAPv2 Payload
Extensible Authentication Protocol
Transport (PPP, IEEE 802.1x, RADIUS)

Figure 4. MSCHAPv2 Encapsulation.

By default, MSCHAPv2 support is natively available for Microsoft and other proprietary and open source operating systems including Unix and Linux variants.

3. System Design

In this research, PEAP was in real test bed scenario. A quantitative performance analysis was carried out to compare the performance of PEAP using MSCHAPv2 on Microsoft Network Policy Server and FreeRADIUS. The key performance indicators are given below:

3.1. Authentication Time

It can be defined as the total time required to complete an end to end authentication in an 802.1x communication. By closely observing the packet format and the traces captured during communication, authentication time can be defined using following Equation.

$$TA = (TRQ - TST) + (TSX - TRI) \quad (1)$$

Where:
TA= Authentication Time
TRQ = Time of Request Identity
TST = Start time
TSX = Success time and
TRI = Time of Response Identity.

3.2. Re-Authentication/ Reconnection Time

The EAP sessions expire after a predefined time for better security and freeing up network resources. The active sessions are however renewed to ensure continuous operation of an ongoing service. The time it takes to renew the 802.1x session can be determined by closely examining the end to end communication. This can be defined by the Equation

$$TR = TSX - TRQ \quad (2)$$

Where:
TSX = Success time and
TRQ = Time of Request Identity

Lower reconnection time indicates faster renewal of EAP sessions and gives better performance for delay sensitive traffic such as VoIP or in cases when RADIUS authentication is enabled for wireless networks and the user roams from one access point to another.

3.3. Overhead

802.1x by its design certainly adds some additional overhead on the network traffic at the time of starting or renewal of EAP sessions. The overhead can be calculated by examining the length of packets (measured in bytes) transmitted during successful or failed authentications and at the time of reconnections. Lower overhead means better network performance of an authentication system

Table 3. Configuration for Test Lab equipment.

Hardware Platform for Authentication System	
Processor	Intel Corei5 2450M
Memory	4GB RAM
Storage	500GB HDD
Network	100/1000Mbps NIC
Input/output	Standard Keyboard, mouse and display
Virtualization	Virtual machine with bridge network adapter in Oracle VM 4.2.6 r82870
Operating System	
Server1	Microsoft Windows Server 2008R2 X64 SP1
Server2	Centos 6.4x64
Authentication System	
Server1	Microsoft Network Policy Server
Server2	Free Radius
Authenticator	
Manageable Switch	CISCO Catalyst 3560 24port with CISCO IOS12.2
Supplicant	
Client Computer	Windows 81. Professional X64

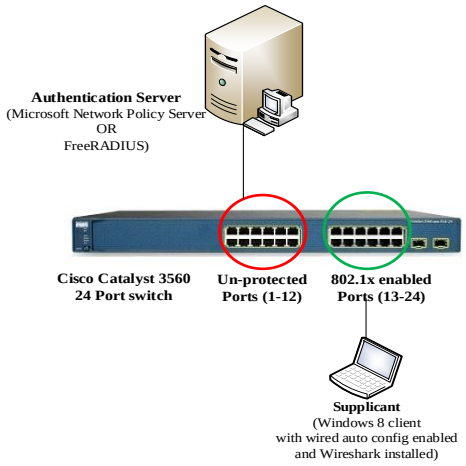

Figure 5. Test lab diagram for 802.1x wired authentication with NPS and FreeRADIUS.

3.4. Tests

In order to correctly measure the performance of the two authentication systems, it was necessary to deeply analyze the network traffic. Figure 5 represents Test Lab Diagram for 802.1x Wired Authentication with NPS and FreeRADIUS. The Windows Event viewer and log of FreeRADIUS both failed to provide the level of insight required. Windows Event Viewer although displayed the 802.1x events with greater time accuracy (timestamps in milliseconds), however it did not display a step by step authentication process for the 802.1x communication. FreeRADIUS logs on the other hand provided the logs with timestamps in seconds only that can certainly not fulfil the requirement of this research.

Wireshark, previously known as Ethereal was therefore a tool of choice because it not only provided the required insight of 802.1x traffic but also helped in analyzing the traffic. Wireshark was installed on the same computer supplicant was running on. Wireshark is an open source, free tool, known for its benefits in educational community, learning IT ethics [18], teaching networking and its use as packet sniffer [9, 12]. It supports a variety of media access methods and network protocols including 802.1x, support for deep analysis of captured traffic, advanced filtering and exporting the traces to a variety of data sets. Wireshark claims to be the world's most popular network protocol analyzer.

Live traffic was captured on the supplicant system with Wireshark version 1.12.4 installed and connected to the controlled port of the authenticator, Cisco Catalyst 3560 switch. The Ethernet interface of the supplicant system was captured for 801.x traffic for the following scenarios:

- 10 successful authentication attempts of supplicant to Microsoft NPS (re-plugging network cable each time).
- 10 successful authentication attempts of supplicant to FreeRADIUS (re-plugging network cable each time).
- 10 failed authentication attempts of supplicant to Microsoft NPS (re-plugging network cable each time).
- 10 failed authentication attempts of supplicant to FreeRADIUS (re-plugging network cable each time).
- 8 attempts of reconnection from supplicant to Microsoft NPS (with periodic re-authentication set to 10 seconds at the authenticator).
- 8 attempts of reconnection from supplicant to FreeRADIUS (with periodic re-authentication set to 10 seconds at the authenticator).

4. Results and Discussion

The following graphs shows the comparison of the two authentication systems as per key performance indicators.

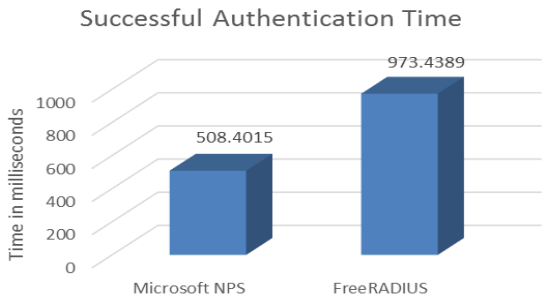

Figure 6. Successful authentication time with NPS and FreeRADIUS.

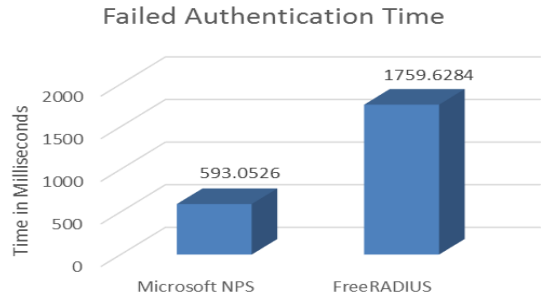

Figure 7. Failed authentication time with NPS and FreeRADIUS.

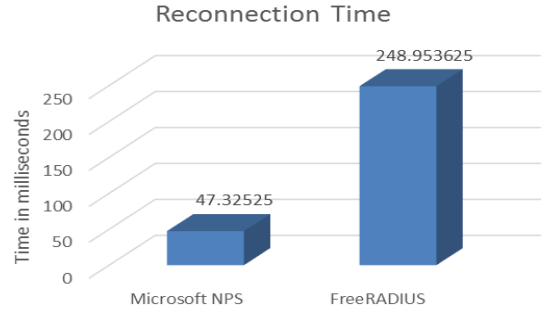

Figure 8. Reconnection time with NPS and FreeRADIUS.

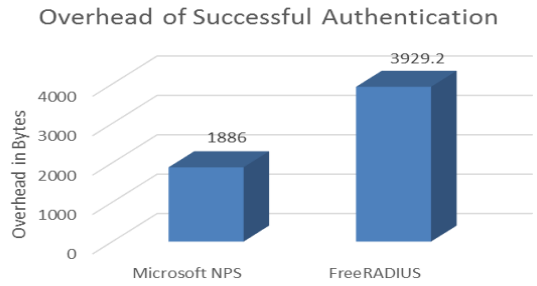

Figure 9. Overhead with successful authentications.

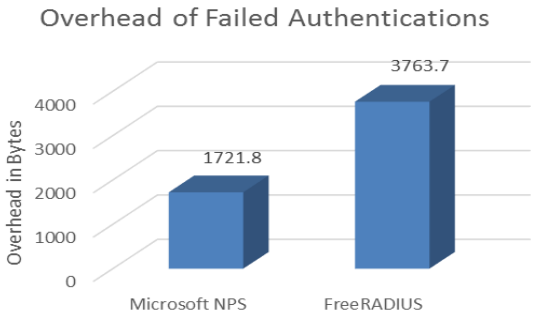

Figure 10. Overhead with failed authentications.

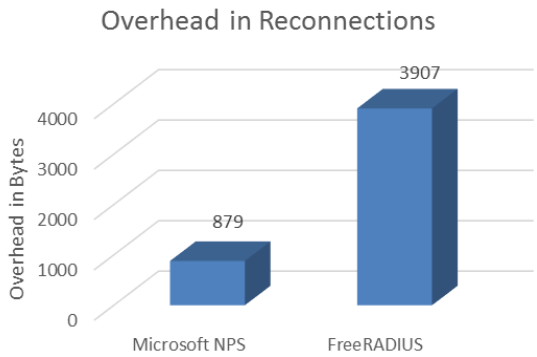

Figure 11. Overhead with reconnections.

The results presented in these graphs i.e., Figures 6, 7, 8, 9, 10, and 11 establish the following facts:

- Microsoft NPS has better performance for successfully authenticated sessions.
- This shows that Microsoft NPS has better performance for the sessions where authentication failed.
- Reconnections were fast in case of Microsoft NPS.
- FreeRADIUS exhibited greater packet overhead as compared to Microsoft NPS. The difference in overhead was due to larger packet exchange by FreeRADIUS after "Client Hello" packet.
- Overhead in failed authentications were observed lower in Microsoft NPS.
- Overhead in reconnections were large in FreeRADIUS as it initiated a new EAP session altogether, resulting in an overhead nearly equal to that of a complete authentication phase. Microsoft NPS contrary to this started the session from "Request Identity" phase, resulting in a considerably lower overhead in reconnections.

5. Conclusions

Network Admission/Access Control is extremely important for all corporate networks where a variety of connecting devices require different level of authorization on the network resources. Be it the servers, client computers, network peripherals or guest stations 802.1x authentication provides a solid layer of physical port security at MAC layer.

Experiments revealed that implementing port security adds performance as well as administrative overhead on the existing network. It is therefore important for the network managers to carefully examine the possible degradation of network performance of their chosen authentication system. It is encouraging to see that 802.1x security by design does not impose a constant packet overhead in end to end communication, but only while establishing or renewing the authenticated sessions.

In the given scenario, Microsoft NPS outperformed FreeRADIUS for the complete performance matrix such as successful authentication, failed authentications, session reconnections and protocol overheads for Windows 8.1 supplicant.

The research revealed that FreeRADIUS by default allows the support for a variety of authentication methods including the ones using clear text passwords. This is okay if the implementer thinks of a broader compatibility but at the same time allows the network intruders may manipulate the user passwords. Additionally, FreeRADIUS was trying to initiate full authentication sessions when only reconnections were required. This ended up in increased overhead of the authentication system.

It was noted that Microsoft NPS was generating smaller fields for application data when certificate services were not in use, whereas, FreeRADIUS kept on trying negotiating full cipher-suite even when the client was not using any certification authority and the default authentication method was PEAP. In addition to the RADIUS service, Microsoft NPS was capable of checking the health state of the connecting client and any non-compliant clients can be blocked or applied for automatic remediation of network health procedures.

Whether it is an open source or proprietary authentication system, faster or slower, 802.1x protected network ports on corporate networks are better than unprotected network ports on wired Ethernets.

6. Recommendations

- Keeping in view the authentication time of 802.1x (even in worst case it was under 1 second) it is highly recommended to have port based authentication in all corporate networks despite of the additional administrative overhead.

- As 802.1x overhead is not persistent, i.e., additional packets are only exchanged at the time of session establishment and renewal, 802.1x authentication does not degrade the network performance. Therefore, a suitable reconnection time could be set at the authenticator to ensure integrity of sessions depending upon the size of the network
- Weak authentication methods should not be used (especially the ones with cleartext passwords). PEAP provides the strongest encryption along with MS-CHAPv2 in the "certificate on the server only" environments.
- The network should be segmented into multiple sub-networks or VLANs according to the logical grouping of the computers. The Tunnel-Pvt-Group-ID can be used to allocate the authenticating client to an appropriate network segment.
- It is recommended to have few ports un-protected in your network in physically secured premises due to the following reasons:
- To provide the access to the network devices in worst case situation, when all RADIUS servers are down or inaccessible and the administrator wants to change the network configuration to allow the client devices to connect to the network.
- Connect legacy network devices that do not support 802.1x, such as legacy network printers/ copiers, scanners, projectors/ displays etc.
- To allow 8021x non-compliant supplicants for PXE (Preboot eXecution Environmet) to automatically deploy the operating systems to the computers
- The un-protected ports must still be using some other basic security such as restricting the ports to a guest VLAN or binding the port to the MAC address of the specified device.
- Once 802.1x authentication is enabled for a network, all the devices attempting to connect to the designated ports must be authenticated by the RADIUS Server. In absence of a RADIUS server, no connection can be made. It is therefore highly desirable to have some fault tolerance mechanism for the server, that can easily be achieved by implementing multiple RADIUS servers on the network that will not only provide fault tolerance but also help balancing the load of incoming 802.1x connections.

7. Directions and Future Work

- Conduct the experiments with increased number of supplicants and authenticators.
- Use actual Hardware Abstraction Layer instead of virtualization for the authentication systems.
- Test variety of supplicants to test performance of the two RADIUS servers.
- Evaluate more EAP types, especially EAP-TLS, where a certificate infrastructure is required to operate with RADIUS and is considered to be the most secure implementation of IEEE 802.1x authentication.
- Work with more complex scenarios such as automatic assignment of IP addresses and dynamic VLAN tagging.
- Integrate the wired authentication to provide a backbone of 802.11 wireless infrastructure.
- Explore vulnerabilities of 802.1x.
- Measure performance of both authentication systems on wireless networks and roaming clients.

References

[1] Aboba B., Blunk L., Vollbrecht J., Carlson J., and Levkowetz H., "Extensible Authentication Protocol (EAP)," Technical Report RFC 3748, Network Working Group, 2004.

[2] Aboba B., Simon D., and Hurst R. "The EAP-TLS Authentication Protocol-RFC 5216," Technical Report, Network Working Group, 2008.

[3] Alabady S., "Design and Implementation of a Network Security Model using Static VLAN and AAA Server," *in Proceedings of 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, Damascus, pp. 1-6, 2008.

[4] Apurva M., Pyo W., Nikolich P., and Gilb J., "LAN/MAN Standards Committee, IEEE Standard for Local and Metropolitan Area Networks, IEEE Computer Society," Technical Report, 2014.

[5] Bhakti M., Abdullah A., and Jung L., "EAP-based Authentication with EAP Method Selection Mechanism," *in Proceedings of International Conference on Intelligent and Advanced Systems*, Kuala Lumpur, pp. 393-396, 2007.

[6] Chiornita A., Gheorghe L., and Rosner D., "A Practical Analysis of EAP Authentication Methods," *in Proceedings of 9th RoEduNet IEEE International Conference*, Sibiu, pp. 31-35, 2010.

[7] Congdon P., Aboba B., Smith A., Zorn G., and Roese J., "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," Technical Report IETF, 2003.

[8] DeKok E. and Weber G., "RADIUS Design Guidelines," Technical Report, Internet Engineering Task Force, 2011.

[9] Gandhi C., Suri G., Golyan R., Saxena P., and Saxena B., "Packet Sniffer-A Comparative Study," *International Journal of Computer Networks and Communications Security*, vol. 2, no. 5, pp. 179-187, 2014.

[10] Gyland Ø., Myren T., Sydskjør R., and Bøe G., *Implementation of IEEE 802.1X in Wired*

Networks-Best Practice Document, UNINETT Led Working Group On Security, 2013.

[11] Hu H., Wu D., and Tang T., "Network Security Admission Solution Based on IEEE802.1X," *in Proceedings of International Conference on Computing, Measurement, Control and Sensor Network*, Taiyuan, pp. 336-339, 2012.

[12] Khan A., Qureshi K., and Khan S.,"An Intelligent Approach of Sniffer Detection," *The International Arab Journal of Information Technology*, vol. 9, no. 1, pp. 9-15, 2012.

[13] Kiravuo T., Sarela M., and Manner J., "A Survey of Ethernet LAN Security," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1477-1491, 2013.

[14] Microsoft Corporation, Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol (CHAP), [online] available: https://msdn.microsoft.com/en-us/library/cc224618.aspx, Last Visited, 2015.

[15] Nunoo H., Kofi E., and Osei K., "A Review of Opensource Network Access Control (NAC) Tools for Enterprise Educational Networks," *International Journal of Computer Applications*, vol. 106, no. 6, pp. 28-33, 2014.

[16] Qian Q., Li C., and Zhang X., "On Authentication System Based on 802.1X Protocol," *in Proceedings of International Conference on Internet Technology and Applications*, Wuhan, pp. 1-4, 2010.

[17] Wang S. and Liang M., "A Network Access Control Approach for QoS Support based on the AAA Architecture," *in Proceedings of International Symposium on Intelligence Information Processing and Trusted Computing*, Huanggang, pp. 507-511, 2010.

[18] Woods D. and Howard E., "An Active Learning Activity for an IT Ethics Course," *Information Systems Education Journal*, vol. 12, no. 1, pp. 73-77, 2014.

[19] www.juniper.net, "802.1X: Port-Based Authentication," [Online]. Available: www.juniper.net/us/en/local/pdf/whitepapers/2000216-en.pdf. Last Visited, 2014.

Farrukh Chughtai has been working in in IT industry at different international organizations such as Save the Children and UNDP for several years. He did his MS computer science in BUITEMS, Pakistan.

Riaz UlAmin earned PhD Degree in Computer Science from University of Glasgow, UK. He has extensive experience of Industry and Academia. Currently, He is working as Associate Professor and Chair of Dept. of Computer Science at BUITEMS, Quetta Pakistan.

Abdul Sattar Malik holds PhD Degree from China. Currently, He is working as Assistant Professor and Head of Dept. of Electrical Engineering at BZU Multan Pakistan.

Nausheen Saeed holds MS degree from BUITEMS, Quetta and proceeding her PhD in Sweden. She is serving as Assistant Professor in the SBK Women University Quetta, Pakistan