Network Admission Control System

B. Thanudas[*], Jeby M. Abraham[*], Ashwini B.[#], Vini Vijayan[#]

[*] *Vikram Sarabhai Space Centre*
Thiruvananthapuram, India

[#]*Department of Computer Science, Cochin University of Science and Technology*
Cochin, India

***Abstract*— Network Admission Control (NAC) is a computer networking concept that uses a set of protocols to secure the network nodes prior to their accessing the network. NAC provides an enforcement mechanism that helps to ensure that computers are properly configured and comply with the organisation's security policy. In this paper we have provided a simple cost effective NAC system using open source software satisfying the needs of the organization.**

***Keywords*— Network Admission Control, Wire1x, EAP, TNC-Architecture, IEEE 802.1x Authentication.**

I. Introduction

NAC, restricts access to the network based on identity or security posture. When a network device is configured for NAC, it can force user or machine authentication prior to granting access to the network. NAC was designed to make the decision whether a particular user and the associated endpoint should be allowed on the network or not, and potentially what to do with them if they were not in compliance. [1], [2]

II. Analysis and Design

The architecture and technologies used for the proposed system are described here:

A. Architecture

The Trusted Network Connect Work Group is working to define and promote an open solution architecture that enables network operators to enforce policies regarding the security state of endpoints in order to determine whether to grant access to a requested network infrastructure. The Trusted Network Connect (TNC) architecture will leverage and integrate the network access control mechanisms such as 802.1X.[25]

The primary roles in the TNC architecture are the Access Requestor (AR), the Policy Enforcement Point (PEP), the Policy Decision Point (PDP), The AR requests access to a protected network. The PDP compares the AR's credentials (e.g. user certificates, password, etc.) and information about its security posture against certain network access policies, and then decides whether network access should be granted to the AR. If a PEP is present, the PDP then communicates its decision to the PEP, which actually grants or denies access (i.e. enforces access control). [6]- [15]

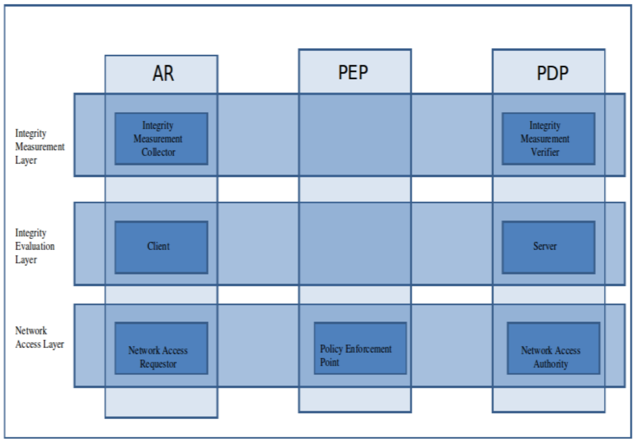
AR
PEP
PDP
Integrity Measurement Layer
Integrity Measurement Collector
Integrity Measurement Verifier
Integrity Evaluation Layer
Client
Server
Network Access Layer
Network Access Requestor
Policy Enforcement Point
Network Access Authority

Fig. 1 Architecture for the proposed system

B. Network Access Technology -IEEE 802.1x

The 802.1X standard provides a framework for port based access control (PBAC) that is increasingly becoming accepted for LANs and WLANs.[16],[27]. IEEE 802.1X provides port authorisation on a per-user or per-host basis (the authenticator will not forward frames until the RADIUS server signals that the supplicant is authorised), support for multiple authentication methods (using EAP), separation of the authenticator from the back-end authentication server, allowing user management and policy decision making to be centralised. A Supplicant in 802.1X maps quite readily to an AR in TNC architecture. Here, the Supplicant that wishes port access at an Authenticator (e.g. 802.11 Access Point, Switch) will be authenticated by the Authentication Server (AS) based on the access policies defined in the AS. Integrity measurement and reporting can enhance an 802.1X deployment by providing the AS with additional data regarding the integrity status of the Supplicant. [26]

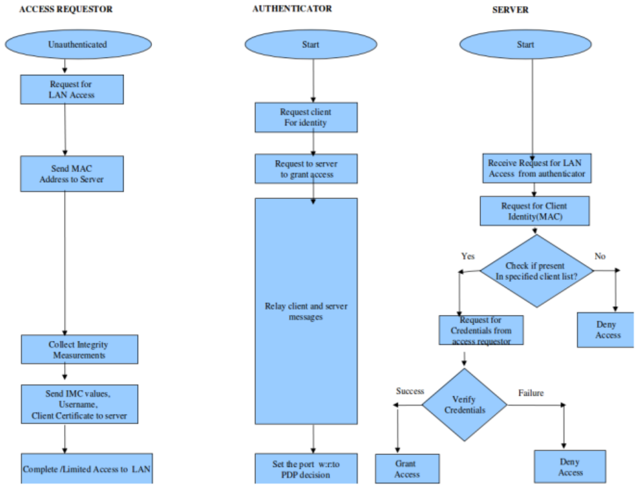
ACCESS REQUESTOR
AUTHENTICATOR
SERVER
Unauthenticated
Request for LAN Access
Send MAC Address to Server
Collect Integrity Measurements
Send IMC values, Username, Client Certificate to server
Complete /Limited Access to LAN
Start
Request client For identity
Request to server to grant access
Relay client and server messages
Set the port w.r.to PDP decision
Start
Receive Request for LAN Access from authenticator
Request for Client Identity(MAC)
Yes
No
Check if present In specified client list?
Request for Credentials from access requestor
Deny Access
Success
Failure
Verify Credentials
Grant Access
Deny Access

Fig. 2 Flow diagram for Authentication

C. Message Transport Technology-EAP-TLS

EAP is a protocol that supports multiple authentication mechanisms such as EAP-MD5, EAP-TLS, EAP-TTLS, EAP-LEAP and EAP-PEAP. From comparison our preference is EAP-TLS because of its strong security feature. It based on Public Key Infrastructure (PKI) and X.509 certificates to handle the authentication. The supplicant has it own certificate that can be verified by the server. As far as the mutual authentication, the server will also present its certificate to the supplicant to be validated.[3],[18]-[21]

Code	Identifier	Length
Req/Res: Type	Data	

Fig. 3 EAP-Packet format

D. PDP Technology-RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol created by Lucent Remote Access. RADIUS is an Internet draft standard protocol. User profiles are stored in a central location, known as the RADIUS server. RADIUS clients (such as an Access Point) communicate with the RADIUS server to authenticate users. The primary functions of RADIUS are authentication, authorization, and accounting. [18]

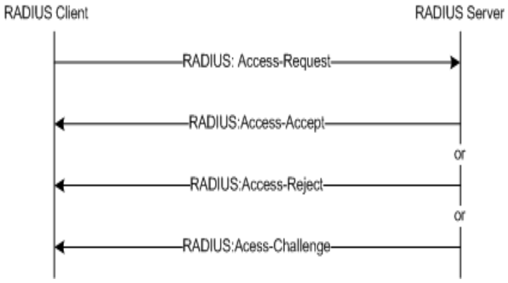

Fig. 4 RADIUS Authentication and Authorization Flow

III. Implementation

A. *Network Access Layer*

The server machine (Authenticating Server) loaded with the operating system Red Hat Enterprise Linux version 5 to configure the RADIUS server for the authentication. The client machine (Access Requestor) loaded with Windows 7 and Cisco Catalyst 2960 (Authenticator) switch.

OpenSSL is used for TLS-based authentication methods i.e. generating the certificates for authentication process. It is an open-source library that crypts and decrypts messages required by the TLS authentication methods. The 802.1x authentication using EAP-TLS requires the generation of three different certificates for the authentication process: Root certificate for CA, Server certificate, Client certificate.

Network Driver Interface Specification (NDIS) is used for the purpose of defining a standard API for "Network Interface Cards" (NIC) to communicate with network systems. Wire1x 2.0 is used as the supplicant for IEEE 802.1x authentication. The user provides their login credentials via the supplicant and the switch provides the login information to the server. [4], [5], [23], [24]

WIRE1x is an open-source implementation of IEEE 802.1x client (supplicant) developed by the Wireless Internet Research & Engineering (WIRE) Laboratory, National Tsing Hua University.

FreeRADIUS is the open source RADIUS server used for the implementation. It supports all common authentication protocols. It is the basis for many commercial RADIUS appliances that support Network Access Control and WiMAX. The server is fast, feature-rich, modular, and scalable.

Switch controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (PEP) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

B. *Integrity Measurement Layer and Integrity Evaluation Layer*

On top of the Network Access Requestor, still on the client system and part of the Access Requestor are Integrity Measurement Collectors (IMCs).The IMV is a component that verifies a particular aspect of the AR's integrity, based on measurements received from IMCs and/or other data. These are software components that are responsible for evaluating the security posture of the end system. For the policy enforcement in our NAC system the selected policies are: to check the username and password of the client and to check the status of antivirus software installed in the client. The IMC and IMV modules are developed as custom modules and integrated to the Wire1x supplicant and FreeRADIUS server respectively.

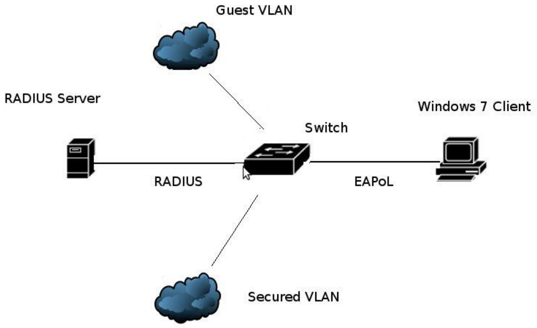

Fig. 5 NAC system implementation

IV. Results

A typical configuration for a system under 802.1X control established. In this scenario, the client wishes to use services offered by server behind the switch. The PC is connected to a port on the switch that has 802.1X port authentication control enabled. The PC must therefore act in a supplicant role. Message exchanges take place between supplicant and authenticator, and the authenticator passes the supplicant's credentials to the authentication server for verification. The authentication server then informs the authenticator whether or not the authentication attempt succeeded, at which point the client is either granted or denied access to the LAN behind the switch.

V. Future Enhancements

For experimental purpose, in our NAC system the selected policies are to check the username and password of the client and to check the status of antivirus software installed in the client. More complex policies can be included. Also, remediation features i.e. to bring the AR up to date in all integrity-related information, as defined by the current policy for authorization can be integrated.

Acknowledgements

We are indebted to Vikram Sarabhai Space Centre for providing us with the infrastructure for this project. We are grateful to Dr. Poulose Jacob and Mr. G. Santosh Kumar, Department of Computer Science, Cochin University of Science and Technology (CUSAT) for their unfailing encouragement of this project. Finally, we are indebted to the anonymous reviewers for helpful suggestions that improved the quality of this paper.

References

[1] Denise Helfrich, Lou Ronnau, Jason Frazier, Paul Forbes , " Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design", Copyright 2007, Cisco Press

[2] Jazib Frahim, Omar Santos , David White,"Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting", Copyright 2007, Cisco Press

[3] Stephen A Thomas, "SSL & TLS Essentials: Securing the Web Book", Copyright 2000, Wiley Computer Publishing

[4] Edward N. Dekker, Joseph M. Newcomer, " Developing Windows NT Device Drivers: A Programmer's Handbook", Copyright 1999, OSR Press

[5] Art Baker, Jerry Lozano, " The Windows 2000 Device Driver Book: A Guide for Programmers" , 2nd Edition, Copyright 2001,
Prentice Hall

[6] Trusted Computing Group, TCG 1.1b Specification Architecture Overview, Revision 0.14, March 2004.

[7] Trusted Computing Group, IWG Reference Architecture for Interoperability (Part 1), Specification Version 1.0, June 2005.

[8] Trusted Computing Group, TCG Credential Profile, Specification Version 1.0, January 2006.

[9] Trusted Computing Group, TPM Specifications v1.2, October 2003.

[10] Trusted Computing Group, TNC IF-TNCCS Specification v1.0, May 2006.

[11] Trusted Computing Group, TNC IF-T Specification v1.0, May 2006.

[12] Trusted Computing Group, TNC IF-PEP Specification v1.0, May 2006.

[13] Trusted Computing Group, TNC IF-IMC Specification v1.1, May 2006.

[14] Trusted Computing Group, TNC IF-IMV Specification v1.1, May 2006.

[15] Trusted Computing Group, TCG Glossary, June 2004.

[16] IEEE802, Port-Based Network Access Control, IEEE Std 802.1X-2001, June 2001, Institute for Electrical and Electronics Engineers (IEEE).

[17] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, PPP Extensible Authentication Protocol (EAP), RFC3784, Standards Track, June 2004, IETF.

[18] C. Rigney, S. Willens, A. Rubens, W. Simpson , Remote Authentication Dial In User Service (RADIUS), RFC2865, Standards Track, June 2000.

[19] "EAP-MD5" RFC3748: Extensible Authentication Protocol (EAP) (June 2004)

[20] "EAP-TLS" RFC2716: PPP EAP TLS Authentication Protocol (October 1999)

[21] "EAP-TTLS" RFC5281: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) (August 2008)

[22] "WinPcap" http://www.winpcap.org

[23] "NDIS" http://www.ndis.com/

[24] "NDISArchitecture"http://www.microsoft.com/technet/prodtechnol//windows2000serv/reskit/ cnet/cnad _arc_vepi.mspx?mfr=true

[25] http://www.trustedcomputinggroup.org/developers/trusted_network_connect/

[26] http://tldp.org/HOWTO/html_single/8021X-HOWTO/