RADIUS: A REMOTE AUTHENTICATION DIAL-IN USER SERVICE

Daniel Szilagyi*, Arti Sood and Tejinder Singh[§]**
M.S. in Computer Science Program, Rivier College

Abstract

This paper provides an overview of RADIUS deployment in the network. It also introduces the various protocols, such as EAP, that is used to implement this service, and PAP, CHAP, MSCHAP, EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-FAST, EAP-FAST that provide authentication mechanisms. These protocols are not discussed in detail but only to present the idea of workflow as to how the RADIUS works in conjunction with them. The role of RADIUS is outlined in point-to-point and VPN connection. Also the 802.1x framework and RADIUS are described briefly. The various AAA protocols are discussed briefly along with DIAMETER, an enhanced version of the RADIUS protocol. This paper is intended for readers with Computer Science or Information Technology background.

1. Overview

With growing numbers of remote users like telecommuters using wireless laptops, PDA(s) trying to access the network, Remote Authentication Dial-In User Service (RADIUS) is widely used. RADIUS, a distributed service, provides centralized management of user access control and security. RADIUS manages and secures the Wireless Local Area Network (WLAN), remote Virtual Private Network (VPN), and wired access. RADIUS is available as a standalone service like Internet Authentication Service (IAS), Access Control Server (ACS) etc. It may also be embedded in the network devices such as routers, switches etc. Users are authenticated by the RADIUS server against a central database which stores profile data such as passwords, type of access, etc. The user is granted access to the resources in the network accordingly.

2. Details

Originally created by Livingston Enterprise which was later acquired by Lucent [1], and as defined by IETF's RFC 2865 (RADIUS authentication and authorization) and RFC 2866 (RADIUS accounting), RADIUS is based on the client-server model and message exchanges takes place over User Datagram Protocol (UDP). The Network Access Server (NAS) acts as a RADIUS client which passes on the user request to the RADIUS server. The other RADIUS clients may be wireless access points, routers, and switches. The RADIUS server performs authentication, authorization, and accounting (AAA) for users after it receives requests from the client. The communication between the client and the server is encrypted using a private key (shared secret) which is never sent over the network. Both the client and server are configured with this secret before communication can take place, and it fails if the secret does not match at both ends.

The RADIUS server supports various methods for authentication and it can be integrated with a variety of databases such as Structured Query Language (SQL) or Lightweight Directory Access Protocol (LDAP). In this case, the RADIUS server matches the authentication/authorization request with information in these databases. RADIUS itself has its own local database where users may be configured if it is not deemed necessary to use an external database. The users configured in the local database are called native users.

The RADIUS server may also act as proxy server where the RADIUS server forwards the requests from a RADIUS client to another remote RADIUS server and receives the reply from the remote server and forwards it back to the client. This feature is commonly used to support roaming profiles and is extensively used by Internet

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

Service Providers (ISPs). The ability to act as proxy server permits two ISPs to allow each other's user to dial in to either network for service.

A RADIUS server may just service authentication and authorization requests or services only accounting requests. A RADIUS server can also operate with other backend authenticators such as RSA SecurID. The RADIUS standard initially used User Datagram Protocol (UDP) ports 1645 and 1646 for RADIUS authentication and accounting packets. The RADIUS standards group later changed the port assignments to 1812 and 1813, but many organizations still use the old 1645/1646 port numbers for RADIUS [2].

RADIUS allows a variety of authentication mechanisms. It is an extensible protocol as the list of the attributes can be extended with new attributes without affecting the existing implementation. Vendors can specify their own specific attributes if necessary. RADIUS has Extensible Authentication Protocol (EAP) support which allows more authentication protocols to be supported by it. Radius's usage with EAP enabled RADIUS to be widely deployed in WLAN as compared to the past where it was mostly used to provide remote access. The EAP messages can be encapsulated in RADIUS packets and intermediate devices such as wireless access points to which the wireless client attempts to connect do not need to implement EAP. The wireless access point in this instance just provides pass through to RADIUS packets without understanding EAP. Only the RADIUS server that ultimately authenticates the wireless client needs to implement EAP. RADIUS has IPv6 support available.

Figure 1 below summaries how RADIUS can be implemented in a network to provide the centralized management of the distributed services.

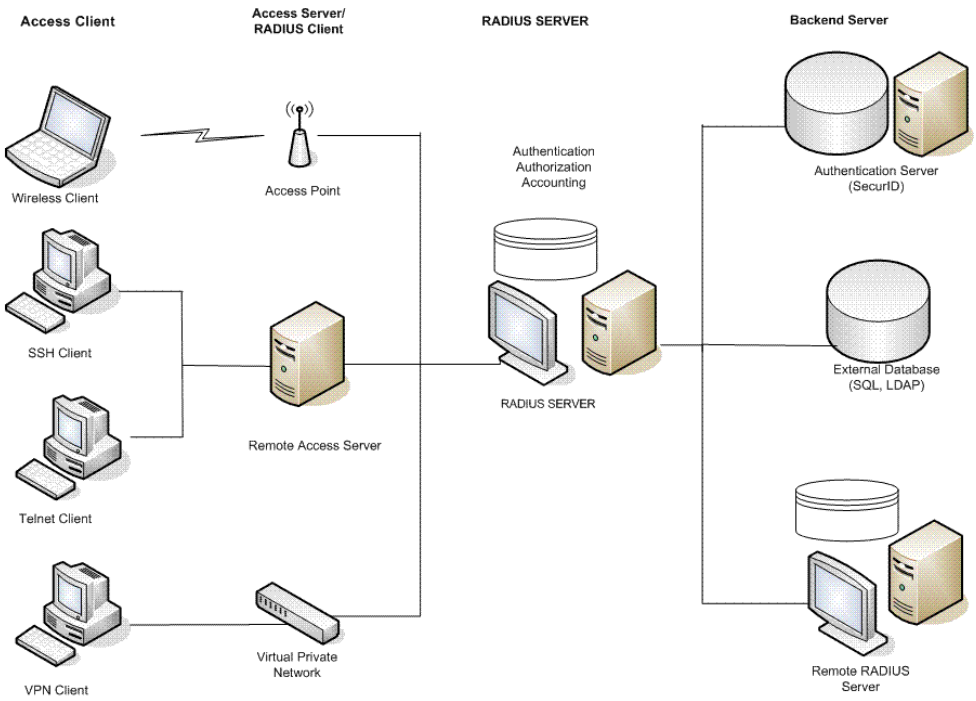

Figure 1: Deployment of RADIUS in the enterprise

3. Implementations

FreeRADIUS is free open source code created by a team who call themselves the FreeRADIUS project. The project was started in 1999 by Alan DeKok and Miquel Smoorenburg with a GNU General Public License. The software package includes a RADIUS server, a licensed client library, a Pluggable Authentication Module library, and an Apache module. It is a very complicated piece of software that requires a lot of configuration. There are

plenty of "how to" documents and forums available for review but much is incomplete. Currently, there are over 50,000 deployments and100 million users. It is supported on UNIX operating systems, but also available on many other platforms. OpenSSL is used for its cryptographic functions implementing Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. Previous versions have already had several security attacks such as Buffer Overflow, Denial of Service and SQL injections. The team even offers a survey to let them know what improvements or updates are needed. The Department of Defense regulations prohibit the use of open source code [3][4][5]. Figure 2 below demonstrates the deployment of FreeRADIUS with Active Directory, where a client connected to a switch uses 802.1x/PEAP authentication methods for gaining access. The client is authenticated by the RADIUS server against Active Directory using the NT LAN Manager (NTLM) authentication protocol.

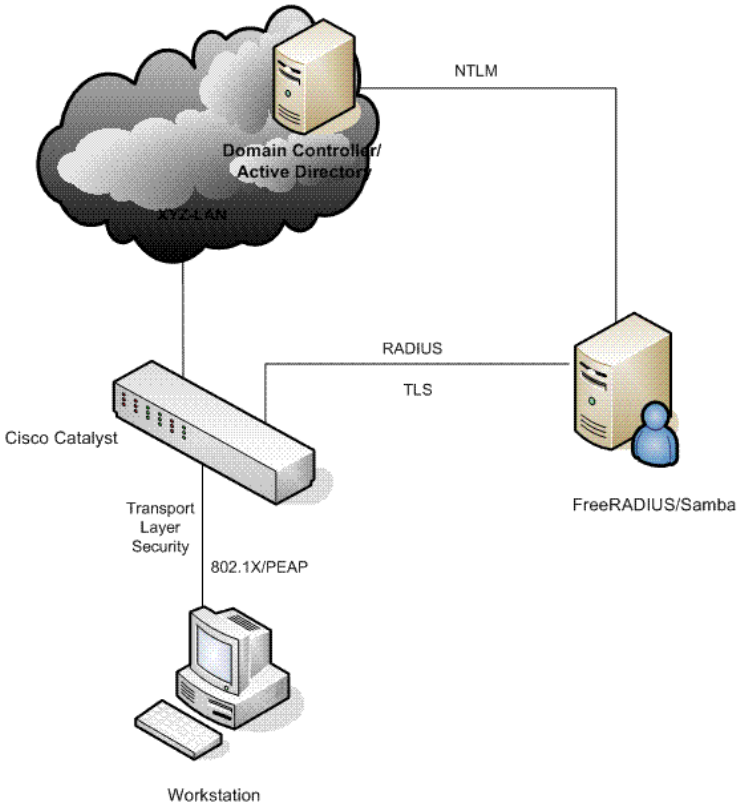

Figure 2: FreeRADIUS Deployment

Cisco Secure (Access Control Server) is another option available to control access to the network. The server authenticates, authorizes and provides audit trails. It is available in three different types of packages ACS 4.2(soon 5.0), ACS View and ACS Express, depending on the size of the network. It provides remote access, wireless, and network administration controls. It supports many protocols including Extensible Authentication Protocol (EAP) and non-EAP protocols which provide authentication requirements. It is set up/configured for centralized control [6-8].

Internet Authentication Service (IAS), the Windows RADIUS server, supports multiple domain setups. It works seamlessly with Routing and Remote Access (RRAS) used for small businesses. It offers centralized Authentication Authorization Accounting (AAA) and stores its information in Active Directory. Active Directory allows administrators to create and set up policies, authenticate thousands of computers and users. It can forward authentication and accounting messages to other RADIUS servers. It supports many protocols such as PPP, PAP, CHAP, MS-CHAP, MS-CHAP v2. These protocols and many others are defined later in the paper. It has been

replaced in Windows Server 2008 by Network Policy Server (NPS), which can also handle VPN and 802.1x Wireless [9-10].

OpenRADIUS (OR) modules are reused for better management and simpler scripts. OR is another freeware implementation like freeRADIUS. It has a unique user interface that can talk to other RADIUS servers and multiple databases in many computer languages. It has a flexible behavior which imposes restriction on user, but also controls the amount of information it gives the user. It includes a powerful extensive dictionary, explaining protocols and functions [11].

The **SBR-RADIUS package** is offered for Windows, Solaris and appliance versions. It was developed by Funk Software but now is part of Juniper Networks. Since then, support for standalone Steel Belted RADIUS (SBR) has been dropped and it is now integrated into a network access control solution called UAC (Unified Access Control) which is placed anywhere in the network to control access to protected resources. It provides the same AAA functionality as the other implementations mentioned above and has an HTML/XML admin interface.

4. Backend Databases and Authentication Servers

RADIUS can be used in conjunction with different backends such as mySQL, PostgreSQL, Oracle, OpenLDAP, Active Directory and eDirectory. Active Directory, openLDAP and eDirectory are directory services used in the enterprise that store network data such as users, computers, and other resources in the network. Oracle, mySQL and PostgreSQL are databases that store network data and on which Structured Query Language (SQL) queries can be executed to obtain information.

RADIUS servers can operate with other authentication servers such as RSA SecurID server, TACACS+ server, IAS server, ACS server or UNIX password files.

5. Authentication Authorization Accounting

Authentication determines the identity of the user and whether the user has appropriate permissions to access the resource to which it is requesting access. This is accomplished by matching the credentials such as username and password, digital certificates, short duration validity passwords called One Time Passwords (OTP), generated by (OTP) tokens to user's profile.

Authorization involves determining whether adequate information was provided to connect and grant services to the user when the user is connected. This step involves user/session specific configuration. Examples of services may be the type of address the user is assigned or the duration for which the connection to the network is allowed.

Accounting involves tracking usage during the lifetime of connection. Typically, the information regarding the identity of the user, the services provided to the user and duration of service is tracked. This assists in management, billing, and planning.

RADIUS is one of the most popular protocols to provide centralized management to perform distributed services of AAA. Other remote authentication protocols include TACACS (Terminal Access Controller Access Control System) and TACACS+.

TACACS uses TCP for transport and runs on port 49. It is commonly used in UNIX environment by NAS to communicate with the authentication server to perform authentication.

TACACS+ is a protocol that provides access control to NAS devices, routers, and other devices by using more than one centralized server. Like TACACS, this protocol also uses TCP for the transport and runs on port 49. This protocol has capabilities like RADIUS, but it allows authentication, authorization, and accounting separately. For example, Kerberos may be used for authentication but TACACS+ is used for authorization and accounting.

DIAMETER is an enhanced version of RADIUS which is not backward-compatible. It uses the reliable transport protocol TCP instead of UDP. It has larger space for attribute-value pairs, better roaming support, and error notification. It is defined by RFC 3588 [12].

6. RADIUS Packet, Attributes, and Authentication Protocols

6.1 PACKET

The operation of the RADIUS protocol involves the exchange of six types of packets between client and server. The RADIUS packet is shown in Figure 3, and has the fields as described below.

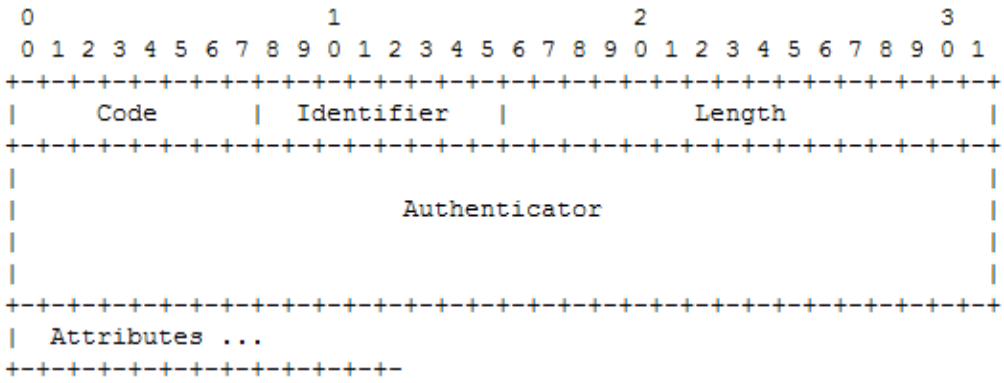

Figure 3: RADIUS packet

Code is 1 byte or 1 octet long, and identifies the type of the packet. The code value 1 is used to identify the Access-Request type of packet, 2 for Access-Accept, 3 for Access-Reject, 11 for Access-Challenge, 4 for Accounting-Request and 5 for Accounting-Response. Code 12 and 13 are for future use.

Identifier is 1 byte long and is used to match the requests to their responses.

Length is two bytes long and specifies the length of the packet including the Code, Identifier, Authenticator and Attributes fields. The minimum length is 20 and maximum is 4096.

Authenticator is 16 bytes long and is used by a RADIUS client to verify the validity of a RADIUS server's response and used by a RADIUS server for password hiding.

Attributes contain authentication, authorization or configuration information in TLV (Type, Length, and Value) format.

6.2 MESSAGES

The operation of the RADIUS protocol involves six types of packets as described in the following sections.

Access-Request is sent by a client to a RADIUS server and it contains the information to determine whether the user is allowed access to specific NAS and requested services. The Code field is set to 1 and the packet must contain User-Name attribute, NAS-IP-Address or NAS-Identifier attribute, User-Password or CHAP-Password or State, NAS-Port or NAS-Port-Type. If User-Password is included, it is encrypted using RSA Message Digest Algorithm MD5. The Authenticator field is called the Request Authenticator in the Access-Request packet and is used for security functions.

Access-Accept are sent by a RADIUS server to a client along with the necessary information to begin the delivery of a requested service. The Code field is set to 2. The Identifier field is a copy of Identifier field of Access-Request to which this is a response. The Authenticator field is called the Response Authenticator for all packets sent by the server and it is calculated by the server using the MD5 algorithm.

Access-Reject is sent by a RADIUS server to a client if the value of the attribute is not acceptable. The Code field is set to 3. The Identifier field is a copy of the Access-Request for which the reject is generated.

Access-Challenge is sent by a RADIUS server to a user through NAS as a challenge that requires response. The challenge is a request to a client for more information. The Code field is set to 11 and relayed to the user by NAS. The user responds with the required information which is conveyed to the server in another Access-Request message.

Accounting-Request is sent by an NAS/client to a RADIUS server which is also performing the accounting. The server adds an accounting record to the log and acknowledges the request while NAS activates the user's session. The code field is set to 4 for this packet. Any attribute that can be used in Access-Request or Access-Accept can be included.

Accounting-Response is sent by a RADIUS server with the code field set to 5. The Attributes are not required for this packet. The Response Authenticator is calculated in a similar way as in Access-Accept or other packets.

Status-Server (experimental) with code field 12 is for future use.

Status-Client (experimental) with code field 13 is for future use.

6.3 ATTRIBUTES

Attributes carry information between client and server. For the accounting attributes, it may be statistical information about the user, e.g. account type, connection type etc. There are two types of attributes:

Standard type attributes are fixed and specified by the Request For Comment (RFC).

Vendor Specific attributes are flexible and are defined by the vendor (Cisco, 3Com etc). The attributes are in TLV (Type Length Value) format. The type and value are 1 byte long whereas the value may be 0 or more bytes (see Fig. 4).

Type field is an assigned number by Internet Engineering Task force (IETF).

Length indicates length of this attribute including type, length, and value.

Value field may be of type text, string, address, integer, or time.

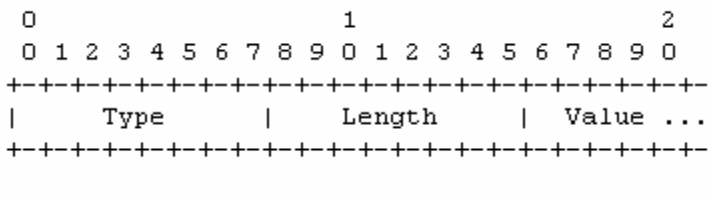

Figure 4: RADIUS Attribute Format

Some standard attributes are as follows:

User-Name specifies the name of the user to be authenticated. The type is 1 and the length is greater than or equal to 3. The value is of string type.

User-Password specifies the password of the user to be authenticated. This is used only in Access-Request packet. The type is 2, and it is encrypted.

CHAP-Password is used only in Access-Request packets, indicates the response value provided by Point-to-Point Protocol (PPP) such as Challenge-Handshake Authentication Protocol (CHAP). Type 3 is used.

NAS-IP-Address is assigned Type 4. It is of length 6, contains the IP address of the NAS that is requesting user authentication. Either NAS-IP-Address or another attribute called NAS-Identifier must be included in Access-Request. It's value is IP address in four octets format.

NAS-Port is assigned 5. It is of length 6, contains the physical port of the NAS that is authenticating the user. It can be used only in Access-request.

Service-Type is assigned 6. It can be included in Access-Request or Access-Accept packets. The length is 6 and the value is 4 octets, 1 for login, 2 for framed, 7 for NAS prompt, 8 for Authenticate only, and so on.

Vendor-Specific is assigned type 26, and is to allow vendors to specify their own attributes to be used in the packets.

EAP-Message is assigned 79, and is for encapsulating the EAP information to be exchanged between a client and a RADIUS server. This is the attribute that allows the EAP protocol be used with RADIUS.

Message-Authenticator's role is to ensure message integrity by encrypting the EAP messages with a RADIUS shared key. Its Type is 80 according to IETF [13].

6.4 AUTHENTICATION PROTOCOLS

RADIUS uses various types of authentication protocols. The few listed below are used with Point-to-Point protocol. These protocols are also used with EAP in an 802.1x framework commonly used in the WLAN.

6.4.1 PAP

PAP (Password Authentication Protocol) is used when hosts and routers connect to the PPP network through a dial up or other dedicated lines. The peer establishes its identity with 2-way handshake. Link is established followed by repeated sending of the id and password to the authenticator until it is acknowledged or until the connection is terminated. It is not a strong authentication method as the password is sent over in clear text [14].

6.4.2 CHAP

CHAP (Challenge-Handshake Authentication Protocol) is another widely supported protocol used in a PPP link in which -- in contrast to PAP where the password itself is sent-- the password's representation is sent during the authentication process. The authentication process involves a 3-way handshake. After link establishment, the authenticator sends a challenge to the peer, the peer responds by sending over a value calculated using a hash algorithm to compute a MD5 hash result based on the password and the challenge. The authenticator, at this stage uses the peer's password with the same hash function and computes the hash result and compares it to the value sent by peer. If it matches authentication is considered successful. The hash algorithm provides one-way encryption which is not easy to crack [15].

6.4.3 MSCHAP (v1/v2)

MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) is Microsoft's version of the CHAP. Both version 1 and version 2 are available, but Version 1 is deprecated. It used MD4 and the DES encryption algorithm and is used in Microsoft's networks.

7. Extensible Authentication Protocol (EAP)

EAP is an Internet standard, described in RFC 3748 that provides a framework for network access clients and authentication servers. EAP supports multiple authentication mechanism called EAP methods. EAP only defines how the messages are to be exchanged between client, authenticator, and the authentication server. EAP does not require the IP protocol to communicate as it uses the link layer.

It was originally developed for use with PPP, but now it is used with the Institute of Electrical and Electronics Engineers (IEEE) 802.1x for wired and wireless access. In the framework, the client may be a remote user trying to access a network and the authenticator may be wireless access point or an 802.1x wired switch. For the backend authentication server, RADIUS server may be used.

In order to allow exchange of EAP messages two additional attributes have been defined in RADIUS specification as per RFC 3579.

The commonly supported EAP protocols are as follows:

EAP-MD5 (Message–Digest 5), as specified in RFC 1194, username and password are used as the authentication credentials. This is a simple protocol. A RADIUS server authenticates a connection request by verifying the MD5 hash of the user's password. The server sends the client a random challenge to which the client responds by hashing the challenge and its password with MD5. It does not provide server authentication. Therefore it is open to attacks. This makes it more suited to wired networks.

EAP-TLS (Transport Layer Security), as specified in RFC 2716, provides strong security by requiring both client and server to be validated and authenticated using PKI certificates. The EAP message interaction between client and server is protected against eavesdropping using an encrypted network connection called a TLS tunnel. The disadvantage with this protocol is the usage of certificates at both ends which makes it tedious to maintain as the certificates have to be installed and maintained in both places.

EAP-TTLS (Tunneled TLS) is based on the Internet draft proposed by Funk and Certicom. It is an extension of TLS that provides the benefits of strong encryption without requiring mutual certificates on both client and server. It only requires the authentication server to be validated to the client with certificates and the client can use a username and password for authenticating to the server. A TLS tunnel can be used to protect EAP messages.

PEAP (Protected EAP protocol) is a draft similar to EAP-TTLS in terms of mutual authentication functionality and is proposed by RSA Security, Cisco, and Microsoft as an alternative to EAP-TTLS. The EAP weakness is handled by protecting the user's credentials, securing EAP negotiation, standardizing key exchanges, supporting fragmentation and reassembly, and supporting fast reconnects.

Cisco LEAP (Lightweight EAP Protocol) was developed to address security issues of wireless networks. LEAP is a form of EAP that requires mutual authentication between client and authenticator. If the authentication is successful, a network connection opens. LEAP is based on user name and password instead of certificates. This is proprietary to Cisco and has not been adopted by other networking vendors.

EAP Flexible Authentication via Secured Tunnel (EAP-FAST) is a protocol invented by Cisco and was submitted to the IETF. EAP-operates just like PEAP and has two phases. The first phase is setting up a secure encrypted tunnel and phase two involves a MS-CHAPv2 session that verifies the client to the authentication server. The encrypted tunnel established in Phase one provides a safe environment for the MS-CHAPv2 session and protects it against dictionary attacks. The difference between PEAP and EAP-FAST is that EAP-FAST uses a PAC (Protected Access Credentials) shared secret to set up the tunnel whereas PEAP uses the server side digital certificate to set up a TLS tunnel. A unique user specific PAC file is generated from a single EAP-FAST Master Key on the authentication server for each and every user. The PAC may be automatically provisioned by the ACS server and this step is also identified as Phase 0 [16].

The use of authentication protocols listed above resolve the security issues like dictionary and man-in-the-Middle attacks described below.

Dictionary Attack: During the password authentication session the attacker attempts to crack the password using the brute force method. 802.1X solves this type of attack by using the TLS tunnel between the client and authenticator thus protecting the username and password exchange.

Man-in-the-Middle Attack: The attacker intercepts the packets between the client and the authenticator, then after obtaining necessary information insert their host between the two, he becomes the "man in the middle". The use of Public Key Infrastructure (PKI) certificates and stronger authentication methods provides protection against such attacks [17].

8. RADIUS Operation (Dial-In/VPN/802.1x)

8.1 Dial-In User using RADIUS Client and Server

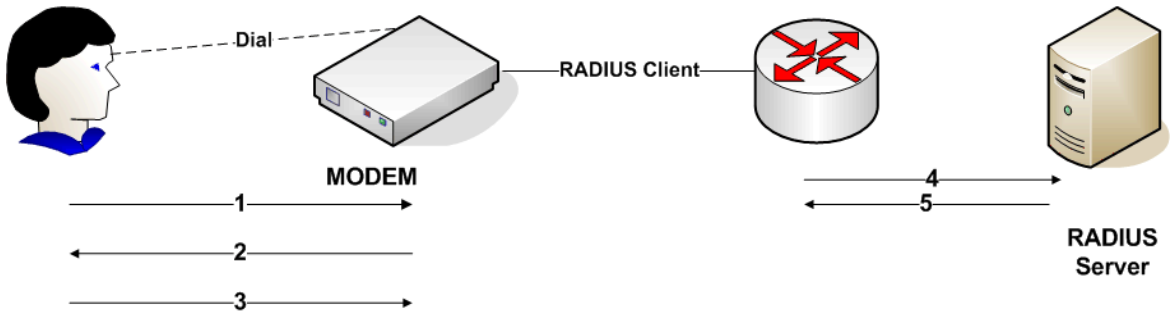

Figure 5: Dial-in User Authentication

In the above diagram (see Fig. 5), the simplest interaction is shown between dial-in user, NAS, RADIUS client and server. The user initiates the PPP authentication to the NAS. In this scenario NAS prompts for username and password if the authentication protocols such as PAP or CHAP are used. The user replies back with the information. The RADIUS client sends username and encrypted password to the RADIUS server which responds back with either accept, reject or challenge. Finally the RADIUS client acts on the services bundled with accept or reject. The RADIUS server can support a variety of methods to authenticate a user. Typically Access-Request is sent from NAS to the RADIUS server and RADIUS responds with either Access-Accept or Access-Reject. As described in previous sections Access-Request contains attributes such as the username, encrypted password, NAS-IP-Address and UDP port. On receiving the request the RADIUS server searches for the username in the local database. If the user is not found sends back an Access-Reject; message otherwise an Access-Accept message is sent with attribute-value pairs such as service type, protocol type, IP address assigned to user, access list to apply or a static route to install in the NAS routing table [18].

8.2 RADIUS Server to Authenticate a Cisco VPN Client

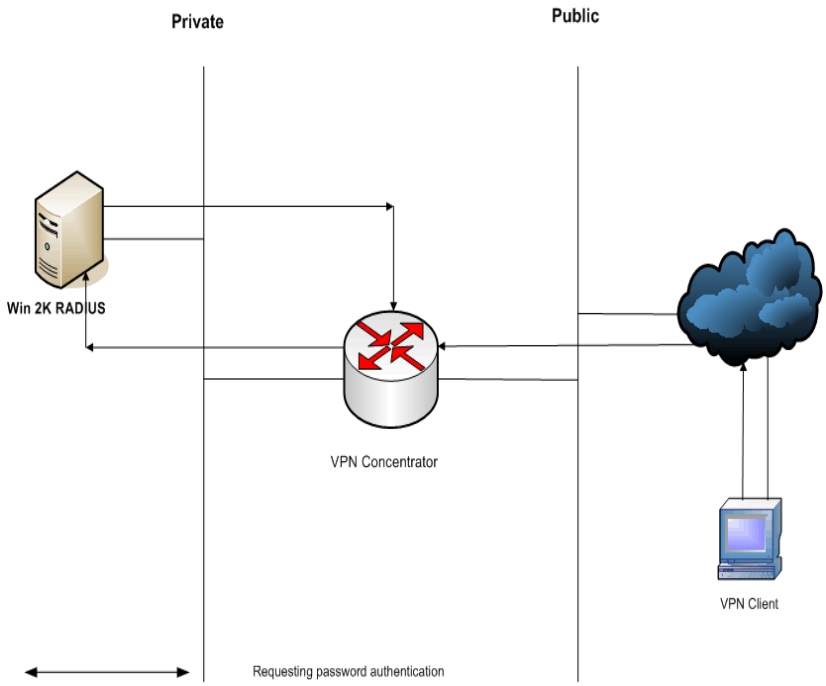

Figure 6: VPN User Authentication

The diagram above (see Fig. 6) demonstrates another simple RADIUS operation: an IAS server running on Windows 2000 server authenticates a VPN client user. Here the VPN concentrator receives a request from the VPN Client in the public network which includes an encrypted username and password. Before the VPN concentrator sends the information to RADIUS server in the private network, it hashes it, using the HMAC/MD5 algorithm. Once the user is successfully authenticated by the RADIUS server an encrypted VPN tunnel is set up for the client to use. In the interaction above the PAP is used as authentication method and VPN tunnel using Internet Protocol Security (IPSec) is set up between VPN client and concentrator. The RADIUS message exchange is similar to the scenario described previously [19].

8.3 Wireless Authentication Using RADIUS Server

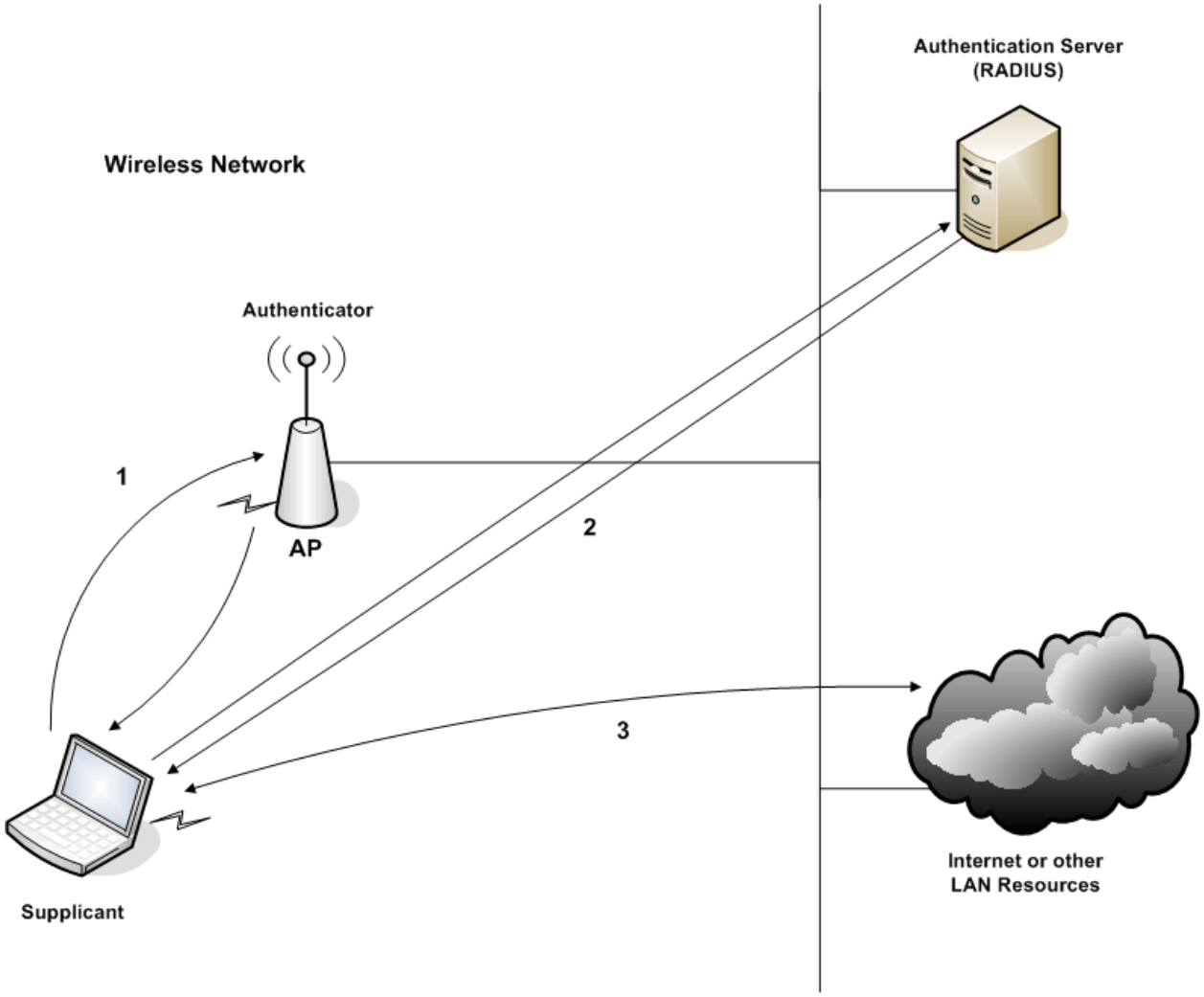

Figure 7: 802.1x WLAN Authentication

The 802.1x provides port-based wired authentication or authentication for wireless 802.11 networks that involves communication between supplicants (the clients), authenticator (a wired Ethernet 802.1x switch or wireless access point) and authentication server (RADIUS) using EAP messages. In the 802.11, wireless networks access point act as a guard to protect network. The client or user does not get past the authenticator until the supplicant's identity is authorized. With 802.1x wireless, the supplicant provides credentials, such as user name / password or digital certificate using encryption like Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) to the

authenticator, and the authenticator forwards the credentials to the authentication server for verification. One of the EAP methods such as EAP-TLS, EAP-TTLS, PEAP may be used for authentication by the RADIUS server. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network. Figure 7 shows the laptop connecting to network through a wireless access point once it has been authenticated by the RADIUS server [20].

9. Glossary

Active Directory – also referred to as AD, is a hierarchical collection of the network data such as users, computers, printers etc. that can be used by systems running Windows operating system.

eDirectory – formerly called Netware Directory Services (NDS) is hierarchical collection of the network data such as users, computers, printers etc by Novell.

LDAP – Lightweight Directory Access Protocol is a protocol based on the client server model used by applications to access directory service. It runs over TCP. For example Domain Name System (DNS) is a name service that provides mapping names of machines and IP addresses. The LDAP clients can access this service.

IPSec – Internet Protocol Security is set of protocols used to secure IP communication by encrypting and authenticating the packets. It is widely used for deploying VPN.

ISP – Internet Service Provides, a company or business that provides access to the internet. The users connect to ISP's servers to access internet through the devices in their homes such as dial-up (using telephone lines), cable modem and Digital Subscriber Line (DSL).

NTLM (NT LAN Manager) – NTLM is the authentication protocol used on the networks of machines running Windows operating system. There are two versions available NTLM and NTLMv2.

OpenSSL – open source software that implements protocols such as SSL and TLS.

PKI – Public Key Infrastructure is a mechanism that allows exchange of data securely over public internet. It enables secure communication through the use of public and private digital certificates.

Samba – is free software based on client-server model that re-implements Service Message Block (SMB)/Common Internet File System (CIFS), used to provide file and print services between UNIX based and Windows based systems.

SSL – Secure Socket Layer is a cryptographic protocol developed by Netscape to exchange data securely between client and server. Its common use is indicated by the URLs of the websites e.g. https.

TLS – Transport Layer Security is crypto protocols successor to SSL that provides privacy and data integrity during the exchange.

VPN – Virtual Private Network is use of the public network to create a private network to connect the remote sites or users. A secure communication channel called tunnel is established over the internet between the parties over which encrypted data is exchanged.

WEP – Wired Equivalent Privacy is a privacy protocol for 802.11 wireless networks to protect against eavesdropping. 40 bit, 64 bit or 128 bit keys are used to encrypt the data.

WPA and WPA2 – WiFi Protected Access is a new specification to ensure secure communication in 802.11 wireless networks to address weaknesses found in WEP.

802.1x – is a standard by IEEE is a specification for passing EAP over wireless and wired local area network.

802.11 – are set of standards by IEEE that specifies the communication in Wireless Local Area Network (WLAN) in 2.4, 3.6 and 5 GHz radio frequency bands.

10. References

[1] RADIUS from Answers.com. Retrieved May 2, 2009, from http://www.answers.com/topic/radius-1/

[2] RADIUS Overview. Retrieved May 2, 2009, from https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/Concepts2.html

[3] The FreeRADIUS Project. Retrieved April 30, 2009, from http://freeradius.org/
[4] BSD License Definition. Retrieved April 30, 2009, from http://www.linfo.org/bsdlicense.html
[5] RADIUS Protocol: Implementation and Weakness. Retrieved April 30, 2009, from http://www.security.nnov.ru/news1563.html
[6] Cisco Secure Access Control Server for Windows. Retrieved May 1, 2009, from http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html
[7] BSDRadius. Retrieved May 1, 2009, from http://en.wikipedia.org/wiki/BSDRadius
[8] Powerful RADIUS Server Performance. Retrieved May 2, 2009, from http://www.interlinknetworks.com/performance.htm
[9] Internet Authentication Service. Retrieved May 2, 2009, from http://technet.microsoft.com/en-us/network/bb643123.aspx
[10] Internet Authentication Service. Retrieved May 2, 2009, from http://en.wikipedia.org/wiki/Internet_Authentication_Service
[11] OpenRADIUS. Retrieved May 2, 2009, from http://www.xs4all.nl/~evbergen/openradius/
[12] Diameter. Retrieved May 5, 2009, from http://en.wikipedia.org/wiki/Diameter_(protocol)
[13] Remote Authentication Dial-In User Service (RADIUS). Retrieved May 3, 2009, from http://tools.ietf.org/html/rfc2865
[14] PPP Authentication Protocols. Retrieved May 3, 2009, from http://www.networksorcery.com/enp/rfc/rfc1334.txt
[15] Challenge Handshake Authentication Protocol (CHAP). Retrieved May 3, 2009, from http://technet.microsoft.com/en-us/library/cc775567.aspx
[16] EAP Authentication protocols for WLANs Retrieved May 4, 2009, from http://www.ciscopress.com/articles/article.asp?p=369223&seqNum=5
[17] White Paper: 802.1X Authentication & Extensible Authentication Protocol (EAP). Retrieved May 5, 2009, from www.scribd.com/doc/7434181/8021X-AUTHENTICATION-EXTENSIBLE-AUTHENTICATION-PROTOCOL-EAP
[18] How Does RADIUS work? Retrieved May 5, 2009, from http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml
[19] Windows 2000 RADIUS Server authentication using VPN Client. Retrieved May 5, 2009, from http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008009467f.shtml
[20] Wireless authentication using RADIUS server. Retrieved May 5, 2009, from http://en.wikipedia.org/wiki/802.1x

---

* **DANIEL SZILAGYI** is an Information Technology Manager working for the Department of Defense at Hanscom Air Force Base in the Plans and Programs department. Daniel has over eleven years working for the DoD and the United States Air Force. He has received two Associates in Information Management and Criminal Justice from the Community College of the Air Force. Daniel has also completed his Undergraduate degree in Information Technology and is currently pursuing his Masters degree in Computer Information Systems from Rivier College as well. Daniel enjoys restoring his 1952 Chevrolet Pickup and remodeling his old house in his spare time.

** **ARTI SOOD** received her Bachelor's degree in Science and Education from Punjab University, India. After obtaining P.G. Diploma in Computer Science, she worked as a database-based application developer. She moved to the U.S. in 1996 and worked with Gambit Communications, Inc. on network simulation tools and with Juniper Networks, Inc. on wireless networking technologies. Since March 2008, she is employed by F5 Networks, Inc. as Sr. Test Engineer, working on file virtualization and data storage technologies. Arti is pursuing M.S. in Computer Science at Rivier College.

§ **TEJINDER SINGH** is a Software Engineer at Harte Hanks Data Technologies. He received his Master's Degree in Computer Information Systems from Rivier College in 2009. He grew up in India where his mother was a preschool teacher and father served in the Indian Air Force. He has a younger brother who is an Electronic Engineer. After completing his undergraduate degree in Mechanical Engineering, Tej worked for an ancillary unit of Maruti, a car company in India. He came to the United States in 1999 as a Software Engineer for the company he is currently employed with. Tej is married to Raj who is a high-school teacher at a local public school. He has two sons, who are 13 and 11 years old. He loves all sporting and outdoor events, particularly soccer and tennis, and enjoys cooking and listening to music.