

IEEE 802.1x, RADIUS AND DYNAMIC VLAN ASSIGNMENT

Hüseyin ÇOTUK

TOBB University of Economics
and Technology
Information Technologies
hcotuk@etu.edu.tr

Ahmet ÖMERCİOĞLU

TOBB University of Economics
and Technology
Information Technologies
omercioğlu@etu.edu.tr

Nurettin ERGİNÖZ

TOBB University of Economics
and Technology
Master Student
nerginoz@etu.edu.tr

ABSTRACT

Remote Authentication Dial-In User Service (RADIUS) is a widely deployed protocol enabling centralized authentication, authorization, and accounting for network access. Originally developed for dial-up remote access, RADIUS is now supported by Virtual Private Network (VPN) servers, wireless access points, authenticating Ethernet switches, Digital Subscriber Line (DSL) access, and other network access types. This report provides an overview of RADIUS and the Extensible Authentication Protocol (EAP) and discusses how to minimize or resolve various security issues of the RADIUS protocol using implementation and deployment best practices.

Keywords: radius, IEEE 802.1x, EAP, authenticator, NAS, authorization, authentication, PEAP, accounting

1. INTRODUCTION

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world.

Remote Authentication Dial-In User Service (RADIUS) is a widely deployed protocol enabling centralized authentication, authorization, and accounting for network access. Originally developed for dial-up remote access, RADIUS is now supported by Virtual Private Network (VPN) servers, wireless access points, authenticating Ethernet switches, Digital Subscriber Line (DSL) access, and other network access types. This report provides an overview of RADIUS and the Extensible Authentication Protocol (EAP) and discusses how to minimize or resolve various security issues of the RADIUS protocol using implementation and deployment best practices.

2. PROBLEM DEFINITION

It's very important to understand that in security, one simply cannot say "what's the best system?" There are two extremes: absolute security and absolute access.

The closest we can get to an absolutely secure machine is one unplugged from the network, power supply, locked in a safe, and thrown at the bottom of the ocean. Unfortunately, it isn't terribly useful in this state. A machine with absolute access is extremely convenient to use: it's simply there, and will do whatever you tell it, without questions, authorization, passwords, or any other mechanism. Unfortunately, this isn't terribly practical, either: the Internet is a bad neighborhood now, and it isn't long before some bonehead will tell the computer to do something like self-destruct, after which, it isn't terribly useful to you. Every organization needs to decide for itself where between the two extremes of total security and total access they need to be. A policy needs to articulate this, and then define *how* that will be enforced with practices and such. Everything that is done in the name of security, then, must enforce that policy uniformly.

"Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

3. IEEE 802.1x NETWORK AUTHENTICATION

Security and flexibility are often seen as mutually exclusive requirements in a network, yet both are equally important. Security is crucial on any network. Flexibility, in particular the ability to roam, is increasingly fundamental. Therefore, Ethernet networks need a device authentication method that is highly secure but not tied to a port's physical location. In addition, the appropriate network access for users needs to be determined from their authentication credentials. 802.1x user authentication solves these multiple requirements. What is more, it is relatively uncomplicated and has very little impact on network performance. It is also a protocol that is medium-independent – equally effective on wireless and wired connections. 802.1x user authentication is rapidly

To configure network devices with 802.1x and radius support, following settings must be done.

```

authorize (
#
# The preprocess module takes care of sanitizing some bizarre
# attributes in the request, and turning them into attributes
# which are more standard.
#
# It takes care of processing the 'raddb/hints' and the
# 'raddb/huntgroups' files.
#
# It also adds the %(Client-IP-Address) attribute to the request.
preprocess
#
# If you want to have a log of authentication requests,
# uncomment the following line, and the 'detail auth_log'
# section, above.
auth_log
#
# attr_filter
#
# The chap module will set 'Auth-Type := CHAP' if we are
# handling a CHAP request and Auth-Type has not already been set.
chap
#
# If the users are logging in with an MS-CHAP-Challenge
# attribute for authentication, the mschap module will find
# the MS-CHAP-Challenge attribute, and add 'Auth-Type := MS-CHAP'
# to the request, which will cause the server to then use
# the mschap module for authentication.
mschap
#
# If you have a Cisco SIP server authenticating against
# FreeRADIUS, uncomment the following line, and the 'digest'
# line in the 'authenticate' section.
digest
#
# Look for IPASS style 'realm/', and if not found, look for
# 'realm', and decide whether or not to proxy, based on
# that.
IPASS
#
# If you are using multiple kinds of realms, you probably
# want to set "ignore null = yes" for all of them.
# Otherwise, when the first style of realm doesn't match,

```

```

Kenar Switch - SecureCRT
File Edit View Options Transfer Script Tools Window Help

Manager A1-1> create vlan=radius vid=26
Info (1089003): Operation successful.
Manager A1-1> add ip int=vlan26 ip=192.168.1.22 mask=255.255.255.0
Info (1005275): interface successfully added.
Manager A1-1> add radius server=192.168.1.22 secret="radius" port=1812 acc
tport=1813
Error (3051012): Parameter "acctport" not recognised.
Manager A1-1> add radius server=192.168.1.22 secret="radius" port=1812
Error (3051015): Parameter PORT. invalid decimal integer "1812?".
Manager A1-1> add radius server=192.168.1.22 secret="radius" port=1812
Options : ACCPort Local
Manager A1-1> add radius server=192.168.1.22 secret="radius" port=1812 acc
tport=1813
Info (1051003): Operation successful.
Manager A1-1>
RADIUS raw PKT Tx: Server: 192.168.1.22
04330029 4C5E898A 060C11FD 5085C909 4A38B2CC 28060000 00072C09 41636374 204F6E04 060A0A01
RADIUS DECODE PKT Tx: Server: 192.168.1.22
Code .....Accounting-Request
Identifier .....0x33
Length .....41
Authenticator .....0x4C5E898A 060C11FD 5085C909 4A38B2CC
Attribute type .....Acct-Status-Type
Attribute length .....6
Attribute value .....0x00000007
Attribute type .....Acct-Session-ID
Attribute length .....9
Attribute value .....0x41636374 204F6E
Attribute type .....NAS-IP-Address
Attribute length .....6
Attribute value .....

Manager A1-1>
RADIUS raw PKT Tx: Server:
04330029 4C5E898A 060C11FD 5085C909 4A38B2CC 28060000 00072C09 41636374 204F6E04 060A0A01
Ready Telnet 49, 15 50 Rows, 132 Cols VT100 NUM

```

```

authenticate (
#
# PAP authentication, when a back-end database listed
# in the 'authorize' section supplies a password. The
# password can be clear-text, or encrypted.
Auth-type PAP (
pap
)
#
# Most people want CHAP authentication.
# A back-end database listed in the 'authorize' section
# MUST supply a CLEAR TEXT password. Encrypted passwords
# won't work.
Auth-type CHAP (
chap
)
#
# MSCHAP authentication.
Auth-type MS-CHAP (
mschap
)
#
# If you have a Cisco SIP server authenticating against
# FreeRADIUS, uncomment the following line, and the 'digest'
# line in the 'authorize' section.
digest
#
# Pluggable Authentication Modules.
pam
#
# See 'man getpwent' for information on how the 'unix'
# module checks the users password. Note that packets
# containing CHAP-Password attributes CANNOT be authenticated
# against /etc/passwd: See the FAQ for details.
unix
#
# Uncomment it if you want to use ldap for authentication
# Note that this means "check plain-text password against
# the ldap database", which means that PAP won't work,
# as it does not supply a plain-text password.
Auth-type LDAP (
ldap
)

```

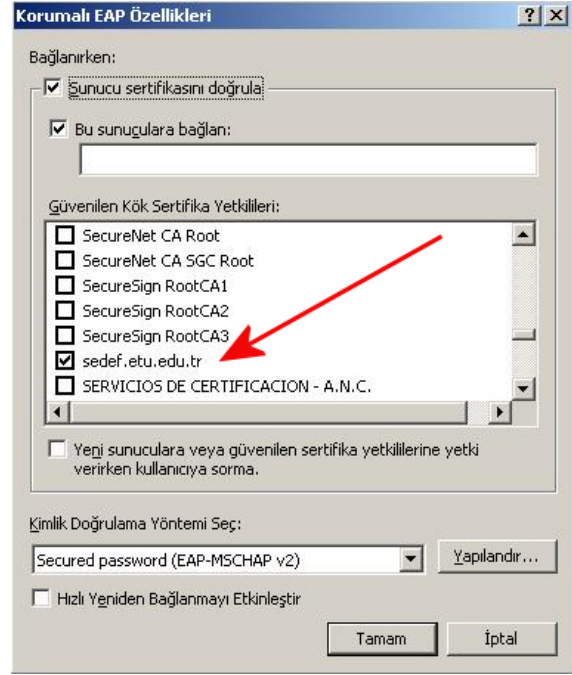
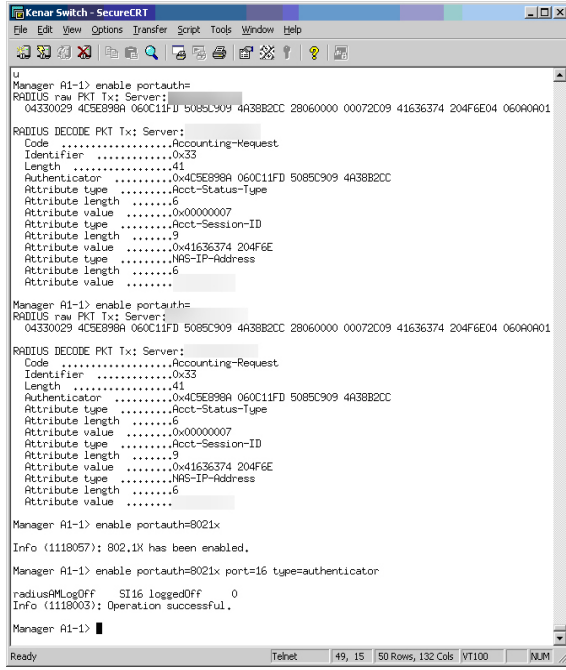
```

Kenar Switch - SecureCRT
File Edit View Options Transfer Script Tools Window Help

Manager A1-1> enable portauth=
RADIUS raw PKT Tx: Server:192.168.1.22
04330029 4C5E898A 060C11FD 5085C909 4A38B2CC 28060000 00072C09 41636374 204F6E04 060A0A01
RADIUS DECODE PKT Tx: Server:192.168.1.22
Code .....Accounting-Request
Identifier .....0x33
Length .....41
Authenticator .....0x4C5E898A 060C11FD 5085C909 4A38B2CC
Attribute type .....Acct-Status-Type
Attribute length .....6
Attribute value .....0x00000007
Attribute type .....Acct-Session-ID
Attribute length .....9
Attribute value .....0x41636374 204F6E
Attribute type .....NAS-IP-Address
Attribute length .....6
Attribute value .....10.10.1.11

Manager A1-1> enable portauth=8021x
Info (1118057): 802.1X has been enabled.
Manager A1-1> enable portauth=8021x port=16 type=authenticator
radius#LogLevel SI16 loggedOff 0
Info (1118003): Operation successful.
Manager A1-1>
Ready Telnet 49, 15 50 Rows, 132 Cols VT100 NUM

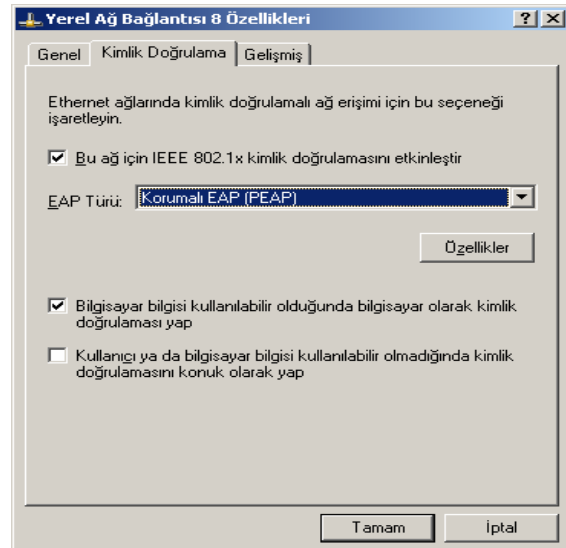
```



Wireless access points are configured as follows:



Client side settings are done as follows:



5. RESULTS

The implemented system supports advanced authentication, authorization and accounting features. When a user wants to connect to a network, switch takes its request and relays this request to the radius server. Radius server asks for an identity for the user. If the user successfully introduces himself to the system, he can get access to the network. While he is getting access to the network, in the server side radius specifies the user's access rights and logs the accounting information about the user. When user logs out from the network, a logout request is sent to server and server can estimate the duration of the session. Furthermore, according to user profile radius server sets user's IP address and VLAN settings. So, user can always get the same IP address and VLAN settings regardless of the connection location. It provides mobility for the system users. Wherever he connects to the network, access rights do not change. With the help of using the same user database, users can login into the system with a unique username and a password. Either it is the easiest way for users to remember and keep these information or it is quite useful for the system administrators. In order to change user information or add a user to the system can be executed by only one step. Older systems generally cannot deal with a large number of users with distinct authentication information. This requires more storage than many embedded systems possess. This system requires less system resources.

In the further stages of the project, TACACS+ protocols shall be considered. TACACS+ encrypts all of the packets and it uses TCP protocol. Radius

encrypts only the important attributes of the packet like password and it uses UDP protocol.

But nowadays, it is not standardized for all authentication requirements. TACACS+ is developed by Cisco and other vendors do not support this protocol yet. Cisco is still working on the TACACS+ to supply RFC requirements.

After the TACACS+ is supported by all vendors and required specifications are achieved, this protocol can be adapted to current project.

REFERENCES

- [1] [RFC 2865](#) Remote Authentication Dial In User Service (RADIUS)
- [2] [RFC 2866](#) RADIUS Accounting
- [3] [RFC 2618](#) RADIUS Authentication Client MIB
- [4] [RFC 2619](#) RADIUS Authentication Server MIB
- [5] [RFC 2620](#) RADIUS Accounting Client MIB
- [6] [RFC 2621](#) RADIUS Accounting Server MIB
- [7] [RFC 3579](#) RADIUS Support for EAP
- [8] [RFC 3580](#) IEEE 802.1X RADIUS Usage Guidelines
- [9] [RFC 4014](#) RADIUS Attributes Suboption for the DHCP Relay Agent Information Option
- [10] [RFC 2548](#) Microsoft Vendor-specific RADIUS Attributes
- [11] [RFC 2809](#) Implementation of L2TP Compulsory Tunneling via RADIUS
- [12] [RFC 2867](#) RADIUS Accounting Modifications for Tunnel Protocol Support
- [13] [RFC 2868](#) RADIUS Attributes for Tunnel Protocol Support
- [14] [RFC 2869](#) RADIUS Extensions
- [15] [RFC 2882](#) Network Access Servers Requirements
- [16] [RFC 3576](#) Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- [17] [RFC 4590](#) RADIUS Extension for Digest Authentication
- [18] Paranoid Penguin - Securing WLANs with WPA and FreeRADIUS, Part I
- [19] Paranoid Penguin - Securing Your WLAN with WPA and FreeRADIUS, Part II
- [20] Paranoid Penguin - Securing Your WLAN with WPA and FreeRADIUS, Part III
- [21] <http://www.ietf.org/IESG/Implementations/Radius-implementation.txt>
- [22] <http://www.stat.ufl.edu/system/man/portmaster/RADIUS/guide/2server.html>
- [23] <http://www.portmasters.com/tech/docs/radius/introducing.html>
- [24] http://www.csee.umbc.edu/help/oracle8/network.815/a67766/03_radiu.htm
- [25] <http://www.portmasters.com/tech/technotes/500/510008.html>
- [26] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftaprad.htm
- [27] <http://www.belgeler.org/howto/p8021x-howto-intro.html>