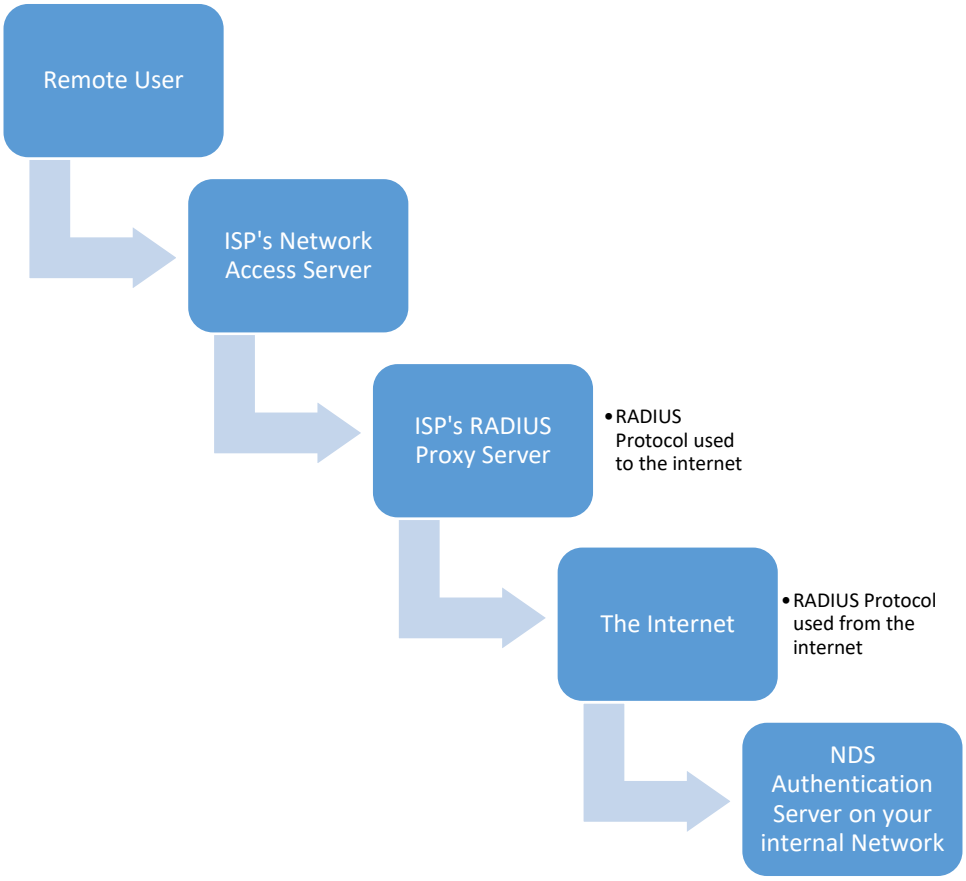
RADIUS

Jason Delaney, Taylor Bauer, Sebastian Mieller

Saint Leo University

Radius stands for Remote Authentication Dial-In User Service. It is software that lets remote access servers connect with a central server. It is specifically used for authenticating users and giving permission to access the system or service they were prompted to log in to. Radius is commonly used by major corporations because it allows the company to maintain user profiles in a central database that all remote servers can share. It also enables companies to set up a policy that can be applied at a single administered network point; this provides better security. Radius is an AAA protocol which stands for Authentication, Authorization, and accounting. Authentication refers to checking the credentials you have entered into the password prompt. Authorization deals with the access you have to the system or service. Lastly, accounting logs the time you entered and the time you logged out. This makes it easier for the companies to track usage for billing and for keeping network statistics.

How it works is a remote user sends their credentials to access a network access server. A network access server is merely acting as a gateway and makes it easier to control access to networks. The network access server then sends the access request to the remote user database authentication server. This is known as the central database where companies usually have their quarries of people's credentials. The RADIUS server will respond in one of three ways to the NAS. Send an access reject; the user is denied all access to the requested network. Send an access challenge, requesting additional information from the user. Lastly, it could send an access to accept granting the user all access to the resources the network has to offer.



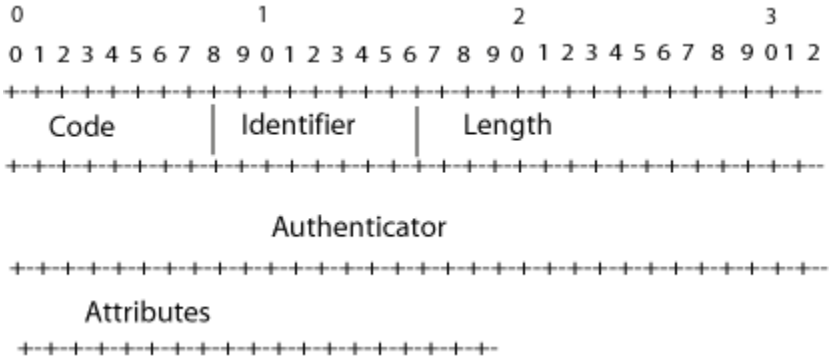
As shown in the diagram a user is trying to access the RADIUS server. Before the user is allowed to come in contact with the server they have to go through multiple steps of security. In the diagram the first step of security is the Internet Service Provider's NAS. NAS is Network Access Server. This is used to connect the user to the internet. The NAS then passes the information collected and send it to the RADIUS server. The next step in this set up is to go through the RADIUS Proxy Server. This is where the triple A's would come into play. The server will authenticate, authorize, and account for users. The first step to authenticating a user is to ask for username and passwords. After they are authenticated they will then be authorized to have access to the server and its data. The accounting part will start tracking the packages.

The server will either accept or reject the user. The NAS then provides the user access to the authorized user.

History

RADIUS was originally created by the Livingston Enterprise. It was made to be used on the client-server model. They needed to create a client for users to interact with so they developed NAS. This is used to pass requests to the server. Since the main purpose of creating this was for security, they needed a way to keep everything protected going through the servers. They decided to encrypt their data with a private key.

Packets



The code part of the packet is 1byte. This identifies the type of packet that is being passed through the server. There are certain code numbers that are used to identify key types of packets. Code 1 is used to request access to the server. Code 2 is sent if Access is accepted and 3 is sent if it is denied. 4 is used as an accounting request and 5 is when the accounting response is getting sent. The identifier is used to match the request with the response. This is to make sure that the millions of packets being sent through the server are not lost. The length is a total of 2 bytes and shows how long the total packet is. The minimum requirement for a packet is 20 and the maximum is 4096. The Authenticator is 16 bytes long and is used by the client to verify

that the package is legit and not a fake. It is also used by the server to hide the password and add another layer of security. Attributes contain the information that packet has in the format of TLV. TLV stands for type, length and value.

Vulnerabilities

There are many issues and vulnerabilities that come with using the RADIUS protocol. Its vulnerability doesn't just come from the protocol itself but also could be caused by the clients poor implementation of the protocol. Keep in mind that this is a very brief list and not all the ways to get around the security of RADIUS.

One vulnerability is a method called, response authenticator based shared secret attack. The response authenticator is basically a MD5 based keyed hash. The goal is to attack the shared secret otherwise known as your set password, private key, or long string of random characters and numbers. The attackers goal is to witness a valid access-request packet as well as the access-accept or access-reject packet that would follow. Using that information, the user would then launch an off-line exhaustive attack on the shared secret.

Another method used for attack is, user-password attribute based shared secret attack. RADIUS uses stream cipher for the protection of the User-Password. Attackers can gain information on the shared secret by simply observing the network traffic and then making attempts to authenticate the password. The attackers goal is to capture the resulting access-request packet and XOR's. From there they can use that valuable information to run codes to try and guess the password.

In addition, the request authenticator attacks illustrate a different vulnerability that penetrates the RADIUS server. These attacks are solely based on the construction of the request

authenticator field and its strength. Due to the request authenticators lack of uniqueness and predictability the RADIUS becomes less secure. More specifically, the protocols do not prioritize the need for the authenticator generation to construct an advanced request authenticator. Moreover, the limited amount of security can be attributed to the use of the pseudo random number generator (PRNG). The algorithm generates random numbers that compromises the RADIUS protocol. Due to its numerical boundaries it limits the potential combinations it could produce. To emphasis if the protocol was not limited to numerical values it could create a more exclusive request authenticator.

Correspondingly, another issue that arises with the RADIUS protocol is the incompetence with the network engineer. The radius server's security could be strengthened through the matiness of a server administrator as opposed to a network engineer. This problem originates from the lack of communication between the network engineer and server administrators. As a result, it generates pockets in which the security server is exploited to outside threats.

To conclude, there were many flaws with the RADIUS protocol. The flaws ranged from the internal structure to even the lack of communication by the external personal. Some of the internal flaws included a response authenticator based shared secret attack, which attacks your set password, private key, or long string of random characters and numbers. A user-password attribute based shared secret attack, which is when information is gained through observing network traffic. The lack of uniqueness that the request authenticators has makes it easier for the passwords to be generated because of the absence of other characters and symbols. Finally, just the incompetence and lack of communication by the people that are supposed to maintain and monitor the server.

Alternatives

RADIUS is not the only technology out there that used for remote authentication. TACACS+ and Diameter are also used in the industry. Diameter derives its name from RADIUS, being half of a circle and diameter being the full length of a circle. Thusly, Diameter is an improvement over RADIUS in ways such as error handling, message delivery reliability and so on. Diameter uses newer protocols and does not rely on UDP, which RADIUS did. What packets are lost are retransmitted at each hop. The TCP and SCTP protocols used are able to adapt to congestion. A "heartbeat" message is sent on the Application layer to work around failed systems in a timely fashion. This allows Diameter to continue doing its job. It has a 32 bit identifier versus the old 8 bit identifier. This is significant because considerably more unique sessions and users can be allowed to use the service. Security using IPSEC or TLS is used at each hop. IPSEC uses cryptographic security and is useful for packet filtering, end to end security, among other things. TLS is a protocol that is responsible for authentication and key exchanges between users and servers. A secret key is exchanged automatically in Diameter. Diameter can also issue requests for re-authentication or even re-authorization of a specific user. Also, hardware that fails usually has a failover so that the system can remain in place while a replacement is occurring. This updated security allows Diameter to operate in the modern world.

Another technology used is TACACS+. TACACS+ uses only TCP. TACACS+ encrypts the entire packet while keeping the header unencrypted. This is to tell the receiver whether the packet itself is encrypted or not. RADIUS only encrypts the password in a single packet, making a man-in-the-middle attack very easy. TACACS+ separates authentication and authorization, which RADIUS does not. Because of this, a system can use different styles of authorization and authentication if they so choose. Additionally, the access server can ask for clarification of

authorization if the server deems it necessary. For example if a user wants to access a file called "Only CEO can read this.txt" the server will ask for authorization before allowing the user to access this specific file. This can decouple the server from needing extra authentication mechanisms. RADIUS cannot allow users to dictate what commands are allowed on the server or not. However, TACACS+ does and it has two rules. One rule is the assign certain levels of privilege to a command. If one does not have those privileges according to the TACACS+ server, they cannot use that command. Another rule to state explicitly which users or groups of users have access to which commands or not. TACACS+ servers should be deployed as close as possible to the user database. This will increase performance while also helping to reduce points of failure and unneeded complexity.

There are specific services for specific A's. One such service is called Kerberos. Kerberos is for the Authentication A. This service was developed in the mid 1990's by a professor at MIT, which still hosts the Kerberos website. They are so old that they still have a statement on Y2K, which describes how Y2K would not endanger any of their services. The service is still being updated today with the last update being the 25th of September of 2017. Its current version is V5. V5 assumes that the initial transmissions from clients and servers can be easily tampered with or listened into. For that reason, the service uses a cryptographic key. This was the standard authentication package on Windows 2000. Essentially, it would allow a service to impersonate the client while accessing whatever was needed for client. A lot of the time, it would merely access local files. One had to connect to a domain controller in order to authenticate the client. Using the Kerberos protocol each party, client and server, can make sure that the other is who they claim to be. Kerberos makes sure no one can mess with the client's ticket with several different encryptions. They use long-term keys, client/server session key, and

KDC/user session keys. A long-term key is a key that only the server and client know about. The client/server session key is the key that is used for encrypt the messages sent and received by both the server and client. The KDC/user session key is the key that the KDC (Key Distribution Center) and the user share in order to send the session key. Kerberos also makes use of symmetric and asymmetric encryptions.

In short, RADIUS is an older technology that for its time functioned quite well. However, in this modern age of massive cyber-attacks and new protocols to secure traffic, it shows its age quite well.

Server and Accounting Log Files

When implementing a RADIUS server, there is the option to set up log files. These files will keep track of when something is started up or shut down. It will also keep track of user acceptance or rejections. This can be used when it comes to system security to see if someone is consistently trying to hack the network and getting declined. The system logs the date and time followed by a description of the event that has occurred.

Accounting log files record accounting events that happen on the server. This includes a start message, which is the beginning of a connection, an end message, which is the end to a connection that was in progress, and interim messages that's indicates if the connection started is still on going. The good thing about these files are that they are recorded in a format that is meant to be exported into a spreadsheet or database. The first six fields of every accounting log are recorded by RADIUS in a simple way. This is to help the user be able to sort through the log quickly and make it easier to find data needed. These fields are date, time, RAS-Client, Record-Type, Full-Name, Auth-Type. The date and time fields list the date that the event occurred and at

what time it occurred. RAS-Client is the name or IP address of which RADIUS server is sending the log. Record-Type is the type of packet that was sent. These are the basic and standard RADIUS packet types. Full-Name is the name of the user that was a part of this event. Auth-Type indicates the type of authentication that was performed.

Radius Proxy

A Network Policy Server (NPS) can be used as a RADIUS proxy server. This can be used to route RADIUS messages between clients and servers while performing authentication, Authorization and Accounting. When NPS is used as a RADIUS proxy, it is used as the central switch and routing point that access and accounting packets use. Since the information is going through the NPS, it keeps and accounting log of all the packets that go through it. There are users that go through an access server first in order the get to the NPS. Before the connection can be made to the NPS the RADIUS protocol has to be applied. If access is granted they are allowed through the NPS and the connection is made to the RADIUS server. This means that the RADIUS server send an Access-accept message to the NPS server meaning that the connection is authenticated and authorized. This just adds an extra step of security before a user can access the radius server.

Conclusion

RADIUS is one of the main types of authentication devices used by many companies. RADIUS works by sending either reject or accept keys to users after they authorize that the user is who they say that they are. It gets that done by being one of the main components of an AAA protocol. This AAA protocol stands for Authorize, Authentication, and Accounting. In most cases an NAS server is usually used when a RADIUS server is in play. With every action taken

on the server there are logs that are taken so the system administrator has a log to see who has done what on the system. This is a major help in the security industry when trying to track intrusions into the system and where there can be vulnerabilities in the system. Since the computer industry is a big business, there are also alternatives to RADIUS with each having their own strengths and weaknesses. RADIUS is useful when it comes to keeping a network secure and has played a very important role in the development of cyber security.

Work Cited

http://searchsecurity.techtarget.com/definition/RADIUS

https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

https://technet.microsoft.com/en-us/library/cc726017(v=ws.10).aspx

http://www.untruth.org/~josh/security/radius/radius-auth.html

Szilagyi, Daniel, et al. "RADIUS: A REMOTE AUTHENTICATION DIAL-IN USER SERVICE."*RIVIER ACADEMIC JOURNAL*, vol. 5

http://lms.uni-mb.si/~meolic/ptk-seminarske/radius.pdf

Development, RSA Information Design and. "RADIUS Server Log Files." *RSA Link*, 13 June 2017, community.rsa.com/docs/DOC-77304.

http://books.gigatux.nl/mirror/wireless/0321202171/ch13lev1sec4.html

http://www.techduke.com/2007/09/13/radius-vulnerabilities/