White Paper

Password Amplifier

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200167 -001 Feb 2006

Overview

The Password Amplifier is a utility that allows you to increase the security of a RADIUS shared secret. You can start with the type of shared secret that you are used to using – for example, something you find easy to remember – and pass it through the Password Amplifier to create a new shared secret that is much more resistant to attack.

The Password Amplifier was created to help administrators create strong shared secrets for use with RADIUS servers. But its usefulness is not limited to RADIUS servers; you can use the Password Amplifier to add to the security of any password that you might use for any purpose.

You Mean My Secret Is Not Good Enough?

Your password or shared secret may or may not be good enough.

A password is typically used to sign a message to prove that it came from you, or to sign a message provided to you to prove your identity. Typically, a cryptographic "hash" function is used to sign messages. The hash function is also known as a "one-way function"; it mixes your password and with the message in such a way that your password cannot be determined from the signature that is produced. Thus, the only way to crack your password from the signature is by brute force – the attacker performs the hash function with the message and many potential passwords until one of the passwords produces the same signature.

This type of brute force attack against passwords is usually called a "dictionary attack". The attacker starts with a dictionary of possible passwords, and tries them all in an attempt to recover your password.

The resistance of a password to a dictionary attack is measured by its entropy. Entropy refers to the amount of randomness or unpredictability of the password. For example, "swordfish" and "Phyllis" are weak; "potrzebie!" and "Mr. Mxyzptlk" are better; and something like "Ontogeny&recapitulates$phylogeny" would be pretty hard to crack.

Entropy is measured in bits, and the number of attempts required on average to recover a password is 2 ^ E, where E is the number of bits of entropy.

A typical dictionary attack might proceed by trying all words in an actual dictionary. The Oxford English Dictionary contains fewer than a million words, and an attacker could try all of them in seconds. So a password that is an ordinary or even an unusual word is automatically suspect.

Another form of the dictionary attack uses probabilities rather than an actual dictionary. Thus, the sequence "tr" is more likely to be followed by an "a" than a "z". Such an attack can proceed by trying more likely sequences of letters before less likely ones. It has been estimated that the entropy of English is about 2.5 bits per character, so an 8-character English-looking password can be recovered in 2 ^ 20 (one million) tries.

Amplifying Your Password Or Shared Secret

The Password Amplifier uses a simple mechanism to generate a high-entropy password from a low-entropy one. It takes your original "precursor" password and applies a series of over one million hash operations to it to produce an amplified password, which is a sequence of 16 seemingly unrelated characters.

When you use the amplified password, an attacker now has a much harder job. For each trial password in the dictionary, the attacker must perform the same sequence of over one million hashes prior to trying that password against the message you signed. Thus, cracking your password has become a million times harder.

Another way of looking at this is that password amplification adds 20 bits of effective entropy to your password; in other words, a password with 30 bits of entropy that is then amplified is as resistant to attack as an unamplified password with 50 bits of entropy.

But don't think of the Password Amplifier as an excuse to use weaker passwords! Most people already use weak passwords, and if you shorten your password even further prior to amplifying it, you won't have gained that much in security. You should always use as strong a password as possible. If you are using ordinary text as your password, we recommend at least 12 characters – 16 characters if possible – prior to amplification.

Managing Multiple Passwords Using The Salt

You may need to use a password for access for multiple purposes. For example, you may use a password to log in to Windows at work, to manage your bank account, to read an online newspaper, and so on.

It's tempting to use the same password for all of them, so that you have just a single password to remember. *But that's a really bad idea!* Remember, each of these sites knows your password, and you are relying on the security practices of each of them to protect it. If any site is compromised, your password is compromised for all the sites with which you use it. Worse yet would be to reveal your password to a site that is unscrupulous to begin with.

You should especially take care not to use high value credentials, such as your company or bank credentials, on any site other than the one that it is intended for.

The Password Amplifier can help you manage multiple passwords for use in different contexts. In addition to the precursor password, you can enter a "salt" phrase, which will be incorporated into the amplification process.

Think of the salt as a master password. You can have one high-entropy salt phrase, and separate precursor passwords for each different use. The total entropy of the amplified password will include the entropy of the salt, the entropy of the precursor password, and the 20 bits of effective entropy provided by the Password Amplifier. So if you have a good salt, you can use weak precursor passwords. You can even set each precursor password to the name of the site or service it is used with.

For example, your salt might be "This is pretty !$%# hard to crack". With that single salt, you could use precursors such as "bank", "nytimes" or "stocks". Now you have only one long password to remember, and multiple easy ones.

Protecting Your RADIUS Infrastructure

The Password Amplifier is an ideal way to create stronger shared secrets for use with RADIUS. But first, we'll describe how shared secrets are used in RADIUS and examine the security threats related to them.

The Shared Secret

A shared secret is configured between a RADIUS client and RADIUS server to protect communication between them. The same shared secret is configured on both devices. Note that the RADIUS client may itself be a RADIUS server when "proxy" RADIUS is used.

The shared secret is used for the following purposes:

1. To authenticate communication between client and server.
   Messages between client and server are signed using the shared secret, so that each one can verify that the message it received is from the expected sender and has not been tampered with.
   [Note that the Message-Authenticator attribute, which performs this function, is always used with EAP authentication but is optional otherwise.]
2. To encrypt session keys returned to the AP or NAS.
   With wireless access in particular, the RADIUS server returns keys to the AP to allow it to create a confidential channel of communication with the user's PC, encrypted using WEP, TKIP or AES.
3. To encrypt PAP passwords.
   This application of the shared secret is happily falling into disuse, as PAP is understood to be a weak authentication mechanism unless used within an EAP tunneled protocol (where the shared secret is not involved).

The Dictionary Attack Threat

One concern that people have expressed is that, when weak shared secrets are used, if an attacker can eavesdrop on a single RADIUS exchange, the attacker could mount a dictionary attack to recover the shared secret. The attacker could then use that knowledge to eavesdrop on additional RADIUS exchanges in which session keys are transmitted and decrypt those keys. The attacker might even mount an ARP poisoning attack to attract packets intended both for the RADIUS server and for the AP to its own device, and act as a man-in-the-middle able to view and decrypt all RADIUS packets.

A lurid scenario indeed! However, it is not as scary as it may at first seem.

An attacker that is able to perform such exploits is a threat to security with or without RADIUS. If the attacker already has access to the wired network, why should he bother to try to crack the RADIUS shared secret when all the user session traffic will have been decrypted by access points before being introduced onto the wired network, where the attacker can view it directly?

However, there may be cases in which there is a real danger. For example, if RADIUS traffic is proxied between RADIUS servers, there may be a network further down the proxy chain where such an attack against the shared secret is possible. This would allow an attacker that does not have access to the immediate network onto which user traffic is bridged to decrypt data on the wireless network by recovering session keys on the proxy network.

As architectures increase in complexity, one's ability to thoroughly analyze the security of those architectures decreases. The wisest approach is to analyze as thoroughly as possible, but protect against threats you don't think possible as well as threats you recognize. It's easy enough – especially with the Password Amplifier – to protect your RADIUS infrastructure from dictionary attack in the face of attacker exploits that nobody might have predicted.

The Widespread Dissemination Threat

When the same shared secret is in use on multiple devices, the very dissemination of that shared secret is itself a threat – if any one device is compromised, all devices are compromised. It is also likely that multiple devices are configured by multiple people, and when secrets are shared among people as well as devices, they tend to take on the character of common knowledge rather than secrets.

The Password Amplifier's optional "salt" feature is particularly useful in organizations with a large RADIUS infrastructure, and can simplify the task of setting different shared secrets for different RADIUS client/server pairs.

When the salt is used, it is cryptographically combined with the original secret you enter to produce the amplified secret. The effective entropy of the amplified secret will be the sum of the entropy of the original secret, the entropy of the salt, and the 20 bits of entropy added by amplification.

The suggested use of the salt is as follows: Define a single, high-entropy salt phrase to use with all shared secrets. You can then use different precursor secrets for different RADIUS client/server pairs. Since the salt automatically adds its own entropy to the amplified secret, you can use lower entropy precursor secrets that are more easily remembered. For example, you could use the IP or MAC address of the RADIUS client as the precursor secret; the salt sets the lower bound for the final entropy.

By using the salt, you have only one high-entropy secret to remember; other secrets can be lower-entropy. But be sure to guard the salt carefully; if the salt is revealed, attacks against amplified secrets with low-entropy precursors become much easier.

Guidelines For RADIUS Security

Here are some guidelines for securing your RADIUS infrastructure:

1. If possible, use RADIUS clients that send a Message-Authenticator attribute for Access-Requests and configure your RADIUS server to only accept authentication requests that include a Message-Authenticator (when EAP is used, RADIUS mandates the inclusion of a Message-Authenticator).
2. Use tunneled EAP protocols, which are not susceptible to dictionary attack (e.g. EAP-TTLS, EAP-PEAP).
3. Within the tunneled EAP protocol, use password protocols that provide mutual authentication (e.g. MSCHAP-V2).
4. Avoid PAP; if you must use it, do so only within a tunneled EAP protocol.
5. Make sure hostile parties can't view RADIUS traffic. Where possible, keep RADIUS traffic on a secured VLAN.
6. As much as possible, set unique shared secrets for each RADIUS client/server pair, or

at least restrict the use of a single shared secret to a small number of devices. The more widespread the use of a shared secret, the more likely it is to be revealed.

7. Use the Password Amplifier to create strong shared secrets for your RADIUS servers.
8. Use a salt phrase with the Password Amplifier to easily create separate shared secrets for different RADIUS client/server pairs.
9. If your RADIUS servers have a proxy relationship with external RADIUS servers (for example, you are an ISP or have a managed service relationship with an ISP), make sure the other party also uses the Password Amplifier in order to establish strong shared secrets between the two RADIUS domains.

Using the Password Amplifier

The Password Amplifier takes an ordinary password or shared secret and converts it into an amplified shared secret that is over 1,000,000 times harder to attack.

You can start with a shared secret that you find easy to remember, amplify it, then copy-and-paste the result into the configuration utility of both the RADIUS client and RADIUS server that will share that secret.

You don't have to remember the amplified shared secret. You can always recreate it from the original.

The amplified shared secret is 16 characters long. For compatibility with the widest variety of applications, it is entirely composed of alphanumeric characters and is guaranteed to have at least one alpha character and at least one numeric character.

Creating an Amplified Shared Secret

Here are the steps:

1. Enter your original shared secret in the "Precursor secret" field.
2. If you'd like to use a "salt" (see below), check the "Enter salt" field and enter a phrase for use as salt.
3. Click [Amplify].
4. After a few seconds, the amplified secret will be displayed.
5. Click [Copy to clipboard].
6. Run the configuration application for your RADIUS server, and paste the amplified secret into its "shared secret" field.
7. Run the configuration application for your AP or other RADIUS client, and paste the amplified secret into its "shared secret" field.
8. Click [Erase clipboard] to ensure that strangers walking up to your PC can't copy the amplified secret into Notepad.
9. Close the Password Amplifier.