Table of Contents

Cisco IOS Password Encryption Facts

Introduction

A non−Cisco source has released a program to decrypt user passwords (and other passwords) in Cisco configuration files. The program will not decrypt passwords set with the **enable secret** command. The unexpected concern that this program has caused among Cisco customers has led us to suspect that many customers are relying on Cisco password encryption for more security than it was designed to provide. This document explains the security model behind Cisco password encryption, and the security limitations of that encryption.

Note: Cisco recommends that all Cisco IOS devices implement the authentication, authorization, and accounting (AAA) security model. AAA can use local, RADIUS, and TACACS+ databases.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

User Passwords

User passwords and most other passwords (*not* **enable secret**s) in Cisco IOS configuration files are encrypted using a scheme that is very weak by modern cryptographic standards.

Although Cisco does not distribute a decryption program, at least two different decryption programs for Cisco IOS passwords are available to the public on the Internet; the first public release of such a program of which Cisco is aware was in early 1995. We would expect any amateur cryptographer to be able to create a new

program with little effort.

The scheme used by Cisco IOS for user passwords was never intended to resist a determined, intelligent attack. The encryption scheme was designed to avoid password theft via simple snooping or sniffing. It was never intended to protect against someone conducting a password−cracking effort on the configuration file.

Because of the weak encryption algorithm, it has always been Cisco's position that customers should treat any configuration file containing passwords as sensitive information, the same way they would treat a cleartext list of passwords.

enable secret and enable password

The **enable password** command should no longer be used. Use the **enable secret** command for better security. The only instance in which the **enable password** command might be tested is when the device is running in a boot mode that does not support the **enable secret** command.

Enable secrets are hashed using the MD5 algorithm. As far as anyone at Cisco knows, it is impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks).

Note: This applies only to passwords set with **enable secret**, and *not* to passwords set with **enable password**. Indeed, the strength of the encryption used is the only significant difference between the two commands.

Which Cisco IOS Image Supports enable secret?

Look at your boot image using the **show version** command from your normal operating mode (Full Cisco IOS image) to see whether the boot image supports the **enable secret** command. If it does, remove **enable password**. If the boot image does not support **enable secret**, note the following caveats:

- Setting an enable password might be unnecessary if you have physical security so that no one can reload the device to the boot image.
- If someone has physical access to the device, he can easily subvert the device security without needing to access the boot image.
- If you set the **enable password** to the same as the **enable secret**, you have made the **enable secret** as prone to attack as the **enable password**.
- If you set **enable password** to a different value because the boot image doesn't support **enable secret**, your router administrators must remember a new password that is used infrequently on ROMs that don't support the **enable secret** command. By having a separate enable password, administrators may not remember the password when they are forcing downtime for a software upgrade, which is the only reason to log in to boot mode.

Other Passwords

Almost all passwords and other authentication strings in Cisco IOS configuration files are encrypted using the weak, reversible scheme used for user passwords.

To determine which scheme has been used to encrypt a specific password, check the digit preceding the encrypted string in the configuration file. If that digit is a 7, the password has been encrypted using the weak algorithm. If the digit is a 5, the password has been hashed using the stronger MD5 algorithm.

For example, in the configuration command:

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

The enable secret has been hashed with MD5, whereas in the command:

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

The password has been encrypted using the weak reversible algorithm.

Configuration Files

When you send configuration information in e−mail, you should sanitize the configuration from type 7 passwords. You can use the **show tech−support** command, which sanitizes the information by default. Sample **show tech−support** command output is shown below.

```
...
 hostname routerA
 !
 aaa new-model
 aaa authentication login default local
 aaa authentication ppp default if-needed local
 enable secret 5 <removed>
 !
 username jdoe password 7 <removed>
 username headquarters password 7 <removed>
 username hacker password 7 <removed>
 ...
```

When saving your configuration files on a Trivial File Transfer Protocol (TFTP) server, change the privileges on that file when it is not in use or put it behind a firewall.

Can The Algorithm Be Changed?

Cisco has no immediate plans to support a stronger encryption algorithm for Cisco IOS user passwords. If Cisco should decide to introduce such a feature in the future, that feature will definitely impose an additional administrative burden on users who choose to take advantage of it.

It is not, in the general case, possible to switch user passwords over to the MD5−based algorithm used for enable secrets, because MD5 is a one−way hash, and the password can't be recovered from the encrypted data at all. In order to support certain authentication protocols (notably CHAP), the system needs access to the clear text of user passwords, and therefore must store them using a reversible algorithm.

Key management issues would make it a nontrivial task to switch over to a stronger reversible algorithm, such as DES. Although it would be easy to modify Cisco IOS to use DES to encrypt passwords, there would be no security advantage in doing so if all Cisco IOS systems used the same DES key. If different keys were used by different systems, an administrative burden would be introduced for all Cisco IOS network administrators, and portability of configuration files between systems would be damaged. Customer demand for stronger reversible password encryption has been small.

Related Information

- **Password Recovery Procedures**
- **Improving Security on Cisco Routers**
- **Technical Support − Cisco Systems**