Wireless Voice Security Recommendations

Overview

This document describes the security options on the Cisco 7920 Wireless IP Phone as well as recommendations for implementing a secure deployment.

A number of protocols are available to secure your data network. However, at this time the security solutions available on the Cisco 7920 Wireless IP Phone are wired equivalent privacy (WEP) and LEAP (part of the 802.1X architecture).

Recommendations

Before you design the architecture for a wireless voice network, Cisco recommends that the security of the wireless data network be deployed as per the Cisco SAFE architecture, which is documented at this URL:

http://www.cisco.com/en/US/netsol/ns954/index.html

For a wireless voice deployment, Cisco recommends the following security solutions:

- Strong passwords and unique logins for wireless voice
- Separation of data and voice VLANs
- Separation between wireless voice usernames and passwords and wired equivalents

Cisco recommends that all wireless voice deployments eventually use LEAP. While it is common for new deployments to use static WEP in order to solve any installation problems before adding LEAP, static WEP should be used only during the installation period.

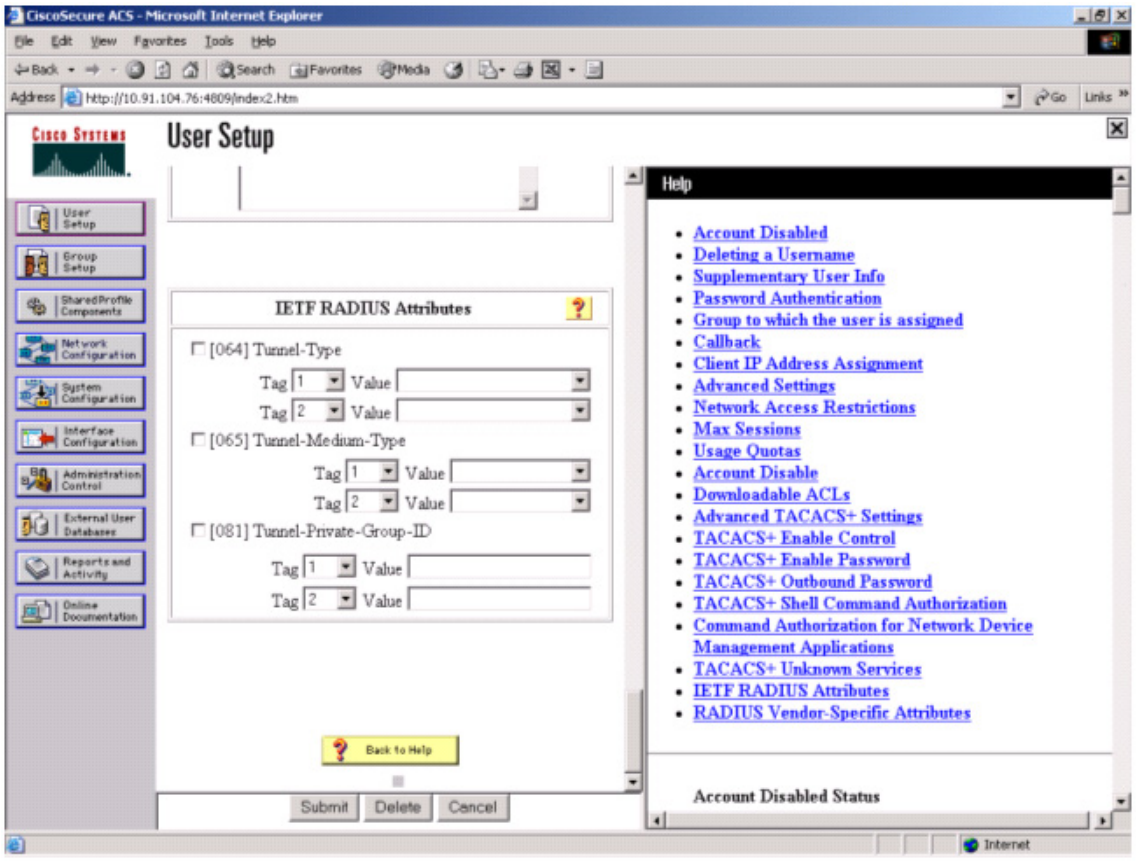
When a deployment begins to use LEAP, Cisco recommends using strong passwords, which contain a minimum of 10 characters comprising uppercase and lowercase letters as well as special characters such as *&%$#@?!. Strong passwords are generally not easy to enter into the phone and therefore are usually stored locally on the phone. These passwords are hidden and cannot be seen.

Caution The phone authenticates automatically, regardless of who is using it. Therefore, you must make sure that the password for the phone is NOT the same password that is used on the data VLAN. This practice also enables administrators to track voice clients separately from data clients.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

In some deployments, the Cisco Secure Access Control Server (ACS) can be used to force users who authenticate with a specific username and password to a specified VLAN, regardless of the VLAN to which they are associated. This feature is called *dynamic VLAN allocation*. It can be set using the ACS Dynamic VLAN Allocation Setup page on the Cisco Secure ACS server (see Figure 1).

Figure 1 ACS Dynamic VLAN Allocation Setup Page



For tracking purposes, you should have a separate username and password for wired and wireless logins. This practice enables administrators to apply different security policies to each group, such as setting expiration periods on passwords. Because it is difficult to change passwords on the phone and impossible to see when a password has expired, Cisco recommends that you do not allow the wireless phone passwords to expire.

With the addition of VLANs to the access points, the wireless network can be logically segmented, much like the wired network. Therefore, it is important to have at least two VLANs on the access point, one for wireless data and one for wireless voice. After you create these VLANs, you can implement access control lists (ACLs) on network switches to segment the voice VLAN from the rest of the network, giving it permission to access only the voice-related servers. Because the Cisco Secure ACS directs users to a specific VLAN, if a user tries to use a voice password on the data VLAN, the ACS redirects the user to the voice VLAN.

In the near future, Cisco will release firmware on the Cisco 7920 Wireless IP Phone with message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). Although these protocols are already available on most Cisco data networks, they are critical for adding incremental security to the voice VLAN. Cisco recommends that these protocols be implemented as soon as they are available.