# The Trivial Cisco IP Phones Compromise

## Security analysis of the implications of deploying Cisco Systems' SIP-based IP Phones model 7960

**Ofir Arkin**
Founder
The Sys-Security Group
ofir@sys-security.com
http://www.sys-security.com


September 2002

**Abstract**

The following paper lists several severe vulnerabilities with Cisco systems' SIP-based IP Phone 7960 and its supporting environment. These vulnerabilities lead to complete control of a user's credentials, the total subversion of a user's settings for the IP Telephony network, and the ability to subvert the entire IP Telephony environment. Malicious access to a user's credentials could enable "Call Hijacking", "Registration Hijacking", "Call Tracking", and other voice related attacks. The vulnerabilities exist with any deployment scenario, but this paper deals specifically with large scale deployments as recommended by Cisco.

# Contents



# Figures

# 1.0 Introduction

The Cisco SIP-based IP Phone 7960 is vulnerable to a significant number of severe security issues which enable a malicious attacker to completely control a user's settings for the IP Telephony network. These security problems include predictable configuration filenames, unauthenticated access to the configuration files of the telephony equipment, and various other issues. Exploiting these vulnerabilities enables a malicious attacker to completely control all operational aspects of the Cisco IP Phone 7960. Complete control over the IP Phone allows an attacker to launch further attacks against the IP Telephony infrastructure, such as "Call Hijacking" or denial of service attacks. In some cases it appears that the design of the Cisco IP Phone 7960 is to blame, rather than simply a flaw in the implementation.

The vulnerabilities exist with any deployment scenario using Cisco SIP-based IP Phones (7960) and their supporting environment. This paper specifically examines the Cisco recommendations for large scale deployments[1]; targeting the weak link in the chain of security – the unauthenticated mechanisms for administrating the IP Phones.

This paper enumerates these problems in the hopes of educating and advising implementers and users of IP Telephony equipment.

[1] SAFE: IP Telephony Security in Depth, http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm.
Security in SIP-based Networks, http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.htm.

## 2.0 The Cisco SIP-based IP Phone 7960

The Cisco SIP-based IP Phone 7960 is a full featured SIP-based IP phone which provides voice communications over an IP network. The IP phone allows one to place and receive phone calls, as well as supporting other features such as network call forwarding, redialing, speed dialing, transferring calls, and placing conference calls[2].

The Cisco SIP-based IP Phone 7960 has two RJ-45 jacks for connecting to external devices, an 'Access port' used to connect a PC or a workstation (also referred as PC-to-phone jack), and a 'Network port' used to connect to an IP network. The 'Access port' and the 'Network port' are part of a 3-port switch built into the Cisco SIP-based IP Phone 7960.

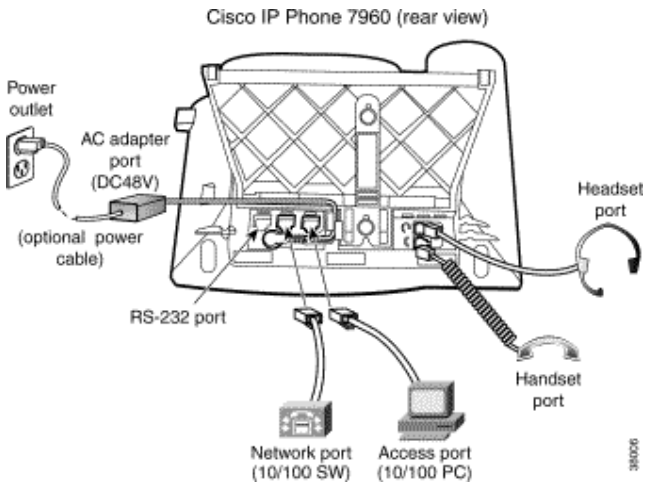


Figure 1: Cisco SIP-based IP Phone 7960 (rear view)[3]

The preferred deployment scenario, recommended by Cisco, is for the IP phone 7960 to be connected to a Cisco Catalyst switch[4]. The "classic" scenario is for the IP Phone's PC-to-phone jack to be connected to a PC, or a workstation, and the 'Network port' connected to a Cisco Catalyst switch.

Cisco recommends configuring two VLANs over the shared network switch port. The first VLAN should be used for voice traffic to and from the IP Phone (in Cisco terms an "auxiliary VLAN"), and the second should be used for data traffic to and from the PC (in Cisco terms a "Native VLAN").

---

[2] The "Cisco SIP IP Phone 7940-7960 User Guide", http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/sip7960/ug/.
[3] The "Cisco SIP IP Phone 7940-7960 User Guide", http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/sip7960/ug/.
[4] Cisco Catalyst modules 4000, 5000, or 6000, because they support the "Power over LAN" feature.

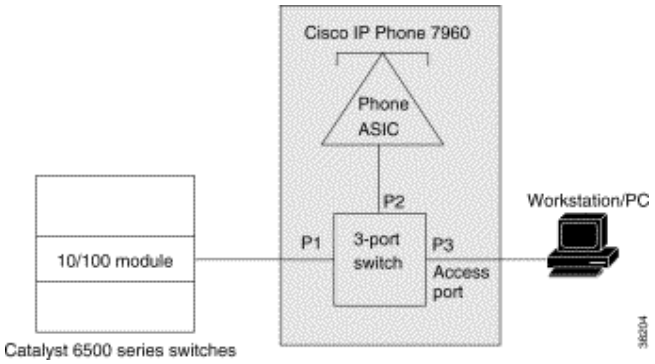


Figure 2: Switch-to-Phone Connections[5]

To implement the two different VLANs, Cisco recommends configuring the Catalyst switch to instruct the IP Phone, via Cisco Discovery Protocol (CDP), to transmit voice traffic over 802.1Q frames using a VLAN ID of 5, and Layer 2 Class of Service (CoS) of 5[6]. The Cisco SIP-based IP Phone 7960 will also set the IP "Precedence bits" (used for quality of service) to the value of 5 (default) for all voice traffic it generates.

The IP Phone's internal 3-port switch is able to perform primitive packet shaping in situations were it is connected to a PC. The 'Access port' can be configured in 'Untrusted' mode to mark 802.1Q or 802.1p frames sent through the port with a default Layer 2 CoS value of 0. The 'Untrusted' mode is the default mode of operation for the 'Access port' when the Cisco SIP-based IP Phone 7960 is connected to a Cisco LAN switch. The IP Phone, when not connected to a Cisco LAN switch, will use 'Trusted Mode' were 802.1Q, or 802.1p, frames will pass through the 'Access port' unchanged. Frame types other than 802.1Q or 802.1p are sent through the IP Phone's switch unchanged.

## 2.1 The Cisco SIP-based IP Phone 7960 Initialization Process

The following sequence of events takes place when a Cisco SIP-based IP Phone 7960 boots[7]:

- The firmware image stored in the Flash memory of the IP Phone is loaded.
- The IP Phone receives from the Cisco switch, via CDP, the VLAN tag to use.
- The IP Phone configures its IP related settings, either by DHCP or from its manually configured settings stored in its Flash memory. These settings include the IP Phone's IP address, the address of the TFTP server (if any), DNS settings, etc.
- The IP Phone confirms that it is running the latest firmware image. This is done by comparing its current firmware version against the firmware images stored on

[5] The "Catalyst 6000 Family Software Configuration Guide", http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/.
[6] The Catalyst switch is also able to instruct the IP Phone to send 802.1p frames carrying a VLAN ID of 0, and Layer 2 CoS of 5, or regular 802.3 frames.
[7] Assuming the Cisco IP Phone 7960 is connected to a Cisco Catalyst switch.

the root directory of the TFTP server. More on the security implications of this below.

- The IP Phone configures its SIP settings. If the IP Phone is using a TFTP server, the settings will be extracted from configuration files stored on it, otherwise local settings from Flash memory will be used.
- If the configuration files the IP Phone retrieved from the TFTP server refer to a different image version than what the IP Phone is using, it will perform a firmware upgrade. The IP Phone will download the required firmware image from the TFTP server, write the image to its Flash memory and then reboot.

## 2.2 Configuring the Cisco SIP-based IP Phone 7960

Configuration changes to the Cisco SIP-based IP Phone 7960 can be made via either a TFTP server on the network, or manually using the IP Phone's buttons and softkeys. As this paper will show, use of a TFTP server to ease configuration of an IP Telephony infrastructure opens a large number of security issues.

Administering the IP Phone can be done in a number of ways:

- Remote administration: editing the appropriate default, and phone-specific, configuration files stored on the TFTP server.
- Local administration: manually configuring the IP Phone using its buttons and softkeys.

Settings which can be changed include the 'Network Settings', the 'SIP Settings', and the 'Date & Time'. Additional access to the IP Phone is provided by the IP Phone's telnet server, which provides a command-line interface (CLI) to debug and troubleshoot the IP Phone. Finally, a physical console port also provides a CLI to the IP Phone.

In terms of security, the key point to be noted about the administration mechanisms of the Cisco SIP-based IP Phone 7960 is that neither mechanism is authenticated. TFTP is an unauthenticated protocol, and the manual configuration can be performed without authenticating to the IP Phone. These core vulnerabilities will be expanded upon throughout the rest of the paper.

## 2.3 The Configuration Files

The configuration files used by the Cisco SIP-based IP Phone 7960 are of two basic types: a generic configuration file shared by all the phones within an environment, and a specific configuration file containing parameters for an individual IP Phone. Cisco recommends that both types of configuration file be stored on a central TFTP server.

### 2.3.1 The Generic Configuration File

The default configuration parameters for all of the Cisco IP Phones within an organization are held in a file called '`SIPDefault.cnf`'. The file should be placed in the root directory of the TFTP server used by the Cisco IP Phones.

This configuration file contains many parameters. One of the more interesting, from a security stand point, is the '`phone_password`' parameter; the password used to remotely login into the Telnet service of the Cisco IP Phones. If this parameter is not set, the default password is '`cisco`'. The implication of this configuration option (contained within the *shared* configuration file) is that the username and password will be the same on all Cisco IP Phones within an organization.

### 2.3.2 Specific Configuration Files

Information specific to individual IP Phones is stored in "specific" configuration files. These files contain the parameters specific to each IP Phone, such as 'line' related information (including authentication credentials specified with the '`linex_authname`' and '`linex_password`' parameters).

The specific configuration files can be stored on the TFTP server's root directory, or in a subdirectory containing all phone-specific configurations files (the directory is specified in a parameter within the global default '`SIPDefault.cnf`' configuration file). Cisco recommends following the naming convention for the filename: '`SIP<MAC ADDRESS OF THE PHONE>.cnf`'. The MAC address of the phone should be entered in upper case, and the file extension 'cnf' in lower case.

# 3.0 The Vulnerability Analysis

Malicious exploitation of the security vulnerabilities enumerated within this paper requires only knowledge of, and access to, the IP address of the TFTP server from which the IP Phones get their configuration files. TFTP is not an authenticated file transfer mechanism, therefore merely having remote network access to the TFTP server is sufficient for an attacker to retrieve any file.

After gaining access to the TFTP server, it is only a matter of time before an attacker is able to retrieve all the credentials used for registering IP Phones on the organization's IP Telephony network. Access to the TFTP Server provides a malicious party with the ability to subvert the IP Telephony based network.

An attacker can choose from a number of attack vectors to compromise the IP Telephony network, using the TFTP server, or physical access to the IP Phone, as needed.

## 3.1 TFTP Server based Attacks

TFTP based attacks have several stages:

- Download the default configuration file from the TFTP server
- Gain knowledge of the MAC addresses used by IP Phones on the network
  - Abuse the network, or
  - Use remote telnet access to the IP Phone
- Download the IP Phones specific configuration files from the TFTP server

Locating the TFTP server is a trivial task, easily accomplished by any of a number of techniques, for instance: scanning for the TFTP server port (UDP 69), or spoofed DHCP requests with option 150, or 66, to elicit DHCP replies containing the requisite information. There are additional methods of discovering the target TFTP server; the specific mechanism used is irrelevant to this discussion.

After locating the TFTP server, the malicious party will want to download the default configuration file '`SIPDefault.cnf`'. This file should be in the root directory of the TFTP server. Among other valuable parameters held in this configuration file (such as the IP address of the SIP Proxy server) this file might contain a very valuable parameter for the malicious party – the '`phone_password`' parameter. This parameter is the password for the telnet service of the Cisco IP Phones. The values contained in this configuration file override any local settings. Since all of the IP Phones in an organization will download this file, the password allowing remote login to the telnet service will be the same for all of the IP Phones.

The next step, for a malicious party, is to gain knowledge of the MAC addresses used by IP Phones on the network. The MAC addresses are the key to the naming convention used for the specific configuration files stored on the TFTP server ('`SIP<MAC ADDRESS OF THE PHONE>.cnf`'). A malicious party able to gain knowledge of the MAC address of

an IP Phone is able to download the IP Phone's specific configuration file from the TFTP server.

**Abuse the Network**

If a malicious party is connected to the same distribution switch(s) as the IP Phones[8], the malicious party can gain knowledge of the MAC addresses of the IP Phones because a frame containing a reply from an answering device will also carry its MAC address. Some possible techniques for retrieving this information include[9]: SIP INVITE request sweep; "ping sweep"; combining ARP attacks with sniffing the wire; mis-configuration issues[10], etc. There are additional methods of discovering MAC Addresses of IP Phones connected to the network; the specific mechanism used is irrelevant to this discussion.

In situations were the attacker is unable to identify the MAC address of the IP Phone (e.g. the IP Phones are not on the same distribution switch(s) as the malicious attacker) the attacker can abuse remote telnet access to the IP Phones.

**Abuse remote telnet access to the IP Phone**

To exploit the telnet server of the IP Phone the malicious party will have to locate the IP address of the Cisco IP Phones, so that the telnet service can be accessed. There are a number of potential techniques which can be used to perform this task, e.g. sweeping the address range with SIP OPTION requests to elicit a response from a SIP-enabled device. However, the specific mechanism used is irrelevant to this discussion.

Any IP Phone located can be logged onto using the password gleaned from the default IP Phone configuration file gained in step one, or by using the default password '`cisco`'. Only access to the TFTP server is required for a malicious attacker to gain remote login access to the telnet service of any IP Phone in an organization.

The telnet service, although it does not allow configuration of the IP Phone's more interesting parameters (only the DNS servers can be changed), does provide vital information for further compromise of the IP Telephony network. A malicious party, having remote access to the IP Phone via telnet, could use the command '`show network`' to receive information about all of the following:

- Phone platform
- DHCP server
- IP address and subnet mask
- Default gateway

---

[8] Even if 'Port Security' is configured with a Cisco Catalyst switch, binding the Cisco IP Phone's MAC address to its port, a malicious attacker can easily bypass the restriction using ARP spoofing techniques.

[9] The parameters a malicious attacker needs to be aware of when trying to get onto the Voice VLAN are the VLAN ID, and the Layer 2 Class of Service (CoS). If the Cisco IP Phone 7960 is connected to a Cisco Catalyst switch, a malicious attacker might try to use the default values for these parameters (the value 5), or simply sniff the information off the wire.

[10] A good example for mis-configuration would be the '`Authentication Password`', the password used by the IP Phone to authenticate any registration challenges by a SIP proxy server during the initialization stage of the Cisco IP Phone 7960. If this value is not configured, and registration is enabled, the IP Phone will use the default logical password which is 'SIP*macaddress*', where *macaddress* is the MAC address of the phone.

- IP address of the TFTP server
- MAC address
- Domain name, and
- Phone name

The information is more than sufficient for total compromise of the IP Telephony infrastructure deployed by an organization. For instance, the MAC address will probably be used to construct the filename used to store the credentials of the Cisco IP Phone 7960's user(s). This file can then be gathered from the TFTP server and the credentials used in further attacks against the IP Telephony infrastructure.

**Download the IP Phone's specific configuration file from the TFTP server**
The MAC address of an IP Phone will probably be used to construct the filename of the specific configuration of the IP Phone. The malicious party merely needs to examine the '`tftp_cfg_dir`' parameter within the generic configuration file to determine where the specific configuration files are stored. Retrieving the file is readily accomplished as TFTP is an unauthenticated protocol.

The most important information stored within the specific configuration file is the credentials used by the Cisco IP Phone's user(s) to authenticate to the IP Telephony network. These parameters are found under the 'line' configuration parameters: '`linex_authname`' and '`linex_password`'.

These credentials, and other information gleaned from the configuration files, can be used in further attacks against the IP Telephony infrastructure of an organization. With these credentials the attacker would be able to perform "Toll Fraud", "Call Hijacking", "Registration Hijacking", impersonations, and various other voice related attacks.

Having valid credentials on the IP Telephony infrastructure is enough for an attacker to subvert the entire IP Telephony deployment of an organization.

### 3.1.1 Preventing Remote Telnet Access to Cisco SIP-based IP Phones 7960

Cisco changed the default telnet service behavior with Cisco SIP-based IP Phone 7960 software version 3.1, Telnet access is now disabled by default. A new optional configuration parameter was added to the default configuration file controlling the behavior of the telnet service: "`telnet_level`". This option can take the values of: 0 (disabled); 1 (enabled), and 2 (privilege).

The author would recommend disabling remote telnet access to the Cisco IP Phone 7960. However, as the following sections illustrate, disabling the telnet service on Cisco IP Phones is not sufficient to prevent a malicious party from extracting the IP Phone's specific configuration files from a TFTP server.

### 3.1.2 Brute Forcing Filenames on the TFTP Server

Other mechanisms of locating and retrieving the specific configuration files exist if telnet access to the IP Phone has been prevented, and the malicious attacker is not on the same distribution switch(s).

The MAC address portion of the filename can be easily brute forced, because the issuing of MAC addresses is controlled by a central authority, who allocates in blocks of consecutive numbers. Knowing the MAC address of a single Cisco IP Phone would enable an attacker to narrow the number of unknown fields that have to be guessed to successfully brute force specific configuration filenames.

### 3.1.3 Re-Enabling the Telnet Service

A malicious party can spoof the TFTP server and inject false configuration files to Cisco IP Phones requesting their configuration information. This attack might be performed utilizing false DHCP replies listing the attacker's TFTP server, rather than the legitimate one. Again there are a number of methods to perform this kind of attack, and the specific mechanism used is irrelevant.

A malicious party can then include the "`telnet_level`" parameter with a value of either 1 or 2 (preferred) within the injected configuration file, and wait for the Cisco SIP-based IP Phone 7960 to reboot. To hasten the reboot, the spoofed TFTP server might include a spoofed new version of the IP Phone's firmware image. The Cisco SIP-based IP Phone 7960 will download the "new" firmware image from the spoofed TFTP server (as part of its boot-up procedure) write the image to the IP Phone's flash memory and then reboot. The "new" firmware image will be downloaded and installed without *any* authentication or authorization (more on these and related issues below).

The telnet service will remain enabled until the next reboot when the DHCP requests will be serviced by the legitimate DHCP server, and the TFTP downloaded configuration files will be correct.

### 3.1.4 Manipulating the Cisco SIP-based IP Phone 7960 Firmware Image

The firmware image for the Cisco SIP-based IP Phone 7960 is downloaded and installed *without authentication*. The firmware image is not signed in any way to verify that it is valid. Any image with a higher version number than the current one is implicitly trusted. Complicating matters, *no authorization* from the user is required before a new firmware image is installed. The combination of the lack of authentication and authorization of the firmware image means that an attacker with write access to the TFTP server is capable of completely controlling all aspects of the IP Phone.

The numerous attacks opened up by this lack of authorization and authentication need not be enumerated here. Suffice to say that manipulating the firmware image provides complete control over all aspects of the Cisco SIP-based IP Phone's operation.

### 3.1.5 Firewalling the TFTP Server

Even if a firewall protects the TFTP server, as recommended by Cisco for large scale deployments, it will not play any part in preventing malicious parties from downloading configuration files from the TFTP server. Valid, though malicious, requests to download configuration files on the TFTP server will pass through the firewall. As has been demonstrated above, this is all a malicious party needs. Additionally, anti-spoofing rules are of little use with the UDP based TFTP protocol.

## 3.2 Physical Access to the Cisco SIP-based IP Phone 7960

Physical access to a Cisco SIP-based IP Phone 7960 allows an attacker to extract critical information (e.g. credentials to authenticate to the IP Telephony network) and, more importantly subvert the IP Phone's operation.

### 3.2.1 Altering the IP Phone's operation

A malicious party with unauthorized physical access to a Cisco SIP-based IP Phone 7960 is able to reconfigure the IP Phone's 'Network Settings', and the 'SIP Settings', using the IP Phone's user interface. Access to the settings is achieved using a key combination: '**#' (star, star hash). Altering these settings would enable the malicious party to perform man-in-the-middle attacks (e.g. pointing the IP Phone to a malicious SIP proxy), denial-of-service attacks (e.g. pointing the IP Phone to a non-existing SIP proxy), and various other attacks. Manually configured parameters take precedence over those from the configuration files on the TFTP server. These changes will remain in effect until the IP Phone reboots and the remote configuration files are reloaded overwriting the settings stored in the IP Phone's flash memory.

Cisco has been aware of the implications of the lack of password authentication with local IP Phone administration for some time[11]. This issue has not yet been resolved, and so far Cisco has shown no signs that they intend to resolve it.

[11] http://online.securityfocus.com/archive/1/273673/2002-05-16/2002-05-22/0

## 4.0 Conclusion

The design of the Cisco SIP-based IP Phone 7960 is fundamentally flawed. The lack of strong physical security and the reliance on unauthenticated TFTP access jeopardizes the entire IP Telephony infrastructure. Applying the recommended best practices for deploying IP Telephony equipment from Cisco does not serve to mitigate the severe security vulnerabilities this paper raises. If unauthorized access is gained to the TFTP server, or the information sent between the TFTP server and a Cisco SIP-based IP Phone 7960 is gleaned, it is an end-of-game scenario. Similar results will be produced with unauthorized physical access to the Cisco SIP-based IP Phone 7960. A malicious party will be able to abuse the information to perform "Toll Fraud" and "Call Hijacking", as well as subvert the entire IP Telephony environment.

Clearly deploying Cisco SIP-based IP Phones 7960 within an IP Telephony infrastructure dramatically decreases the overall security of the infrastructure. The severe design flaws with the Cisco SIP-based IP Phones 7960 prohibit any sort of secure deployment. Cisco's reliance on the unauthenticated TFTP protocol means that every large scale installation is at risk.

The fundamental design flaws highlighted within this paper have greater implications beyond simply Cisco's recommended IP Telephony network designs. The flaws are shared among other Cisco network designs which rely on a TFTP server for distributing either firmware images and/or configuration files.

## 5.0 Acknowledgment

I would like to acknowledge the assistance lent to me by Josh Anderson during the development of this paper.