Counterfeit with CISCO IP COMMUNICATOR

Author: Suman Sah – Sumanssah@gmail.com
Date – 23/May/2016

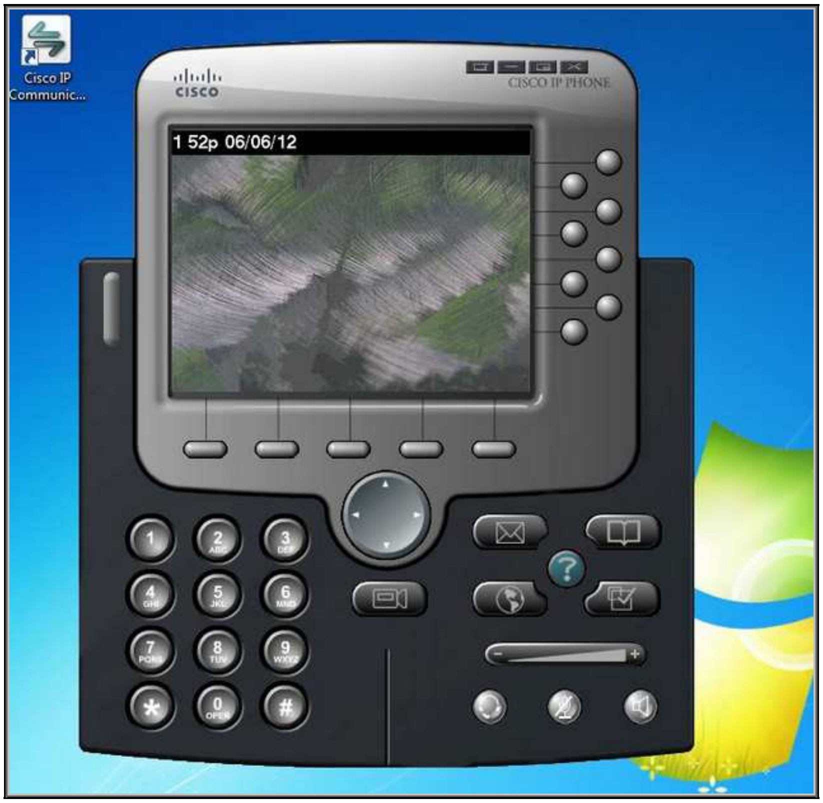
Introduction:

Cisco IP Communicator is a Windows PC-based softphone application provided by Cisco that lets you use your personal computer to make premium voice and video calls. Mostly used by moving users of organization to make voice & video calls.

With a USB headset or USB speakerphone and Cisco IP Communicator, you can easily access your corporate phone number and voicemail. All you need is an Internet connection and remote access to your corporate network, whether you are working from home, supporting a contact center, or traveling on business.

By exploiting this bug/vulnerability, we are able to make calls/receive calls from User number (Number allotted to user by organizations to make & receive calls)

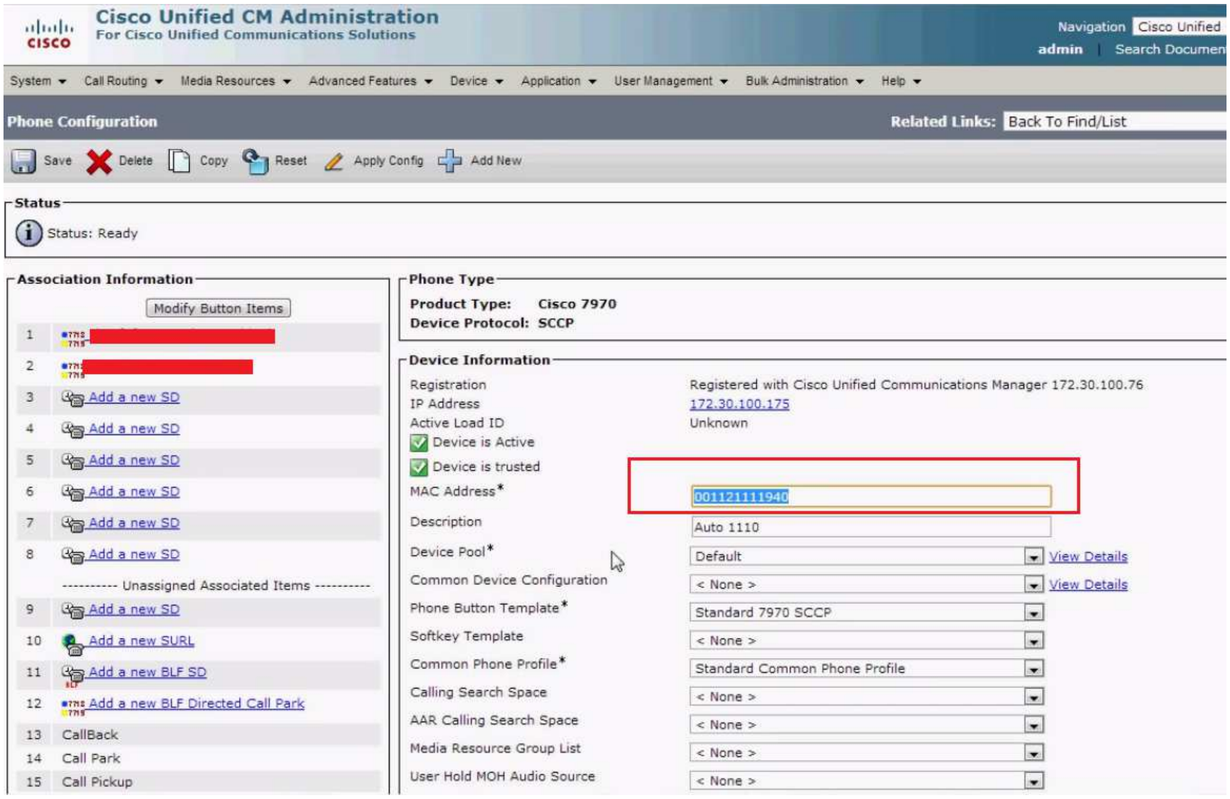
Screenshot for Cisco IP Communicator (Software phone) application is shown below:



Authentication mechanism with CISCO IP COMMUNICATOR:

Most of the organizations/corporate uses MAC base authentication to login to CISCO IP COMMUNICATOR. In normal (Hardware) CISCO Phone’s authentication is done with “User ID & Password”. However, in case of CISCO IP COMMUNICATOR (software phone) authentication is done with MAC address, i.e. MAC Address of user system is bind to a its user ID.

In general User ID is assigned to an IP address but in the organizations we generally don’t a lot static IP for user. So to overcome this MAC based authentication is used for authentication. Please check below mentioned screenshot of “Cisco Unified CM Administration” to add a device (Software / Hardware phone)



Status

Status: Ready

Association Information

1 [redacted]
2 [redacted]
3 Add a new SD
4 Add a new SD
5 Add a new SD
6 Add a new SD
7 Add a new SD
8 Add a new SD
---------- Unassigned Associated Items ----------
9 Add a new SD
10 Add a new SURL
11 Add a new BLF SD
12 Add a new BLF Directed Call Park
13 CallBack
14 Call Park
15 Call Pickup

Phone Type

Product Type: Cisco 7970
Device Protocol: SCCP

Device Information

Registration	Registered with Cisco Unified Communications Manager 172.30.100.76
IP Address	172.30.100.175
Active Load ID	Unknown
☑ Device is Active	
☑ Device is trusted	
MAC Address*	001121111940
Description	Auto 1110
Device Pool*	Default View Details
Common Device Configuration	< None > View Details
Phone Button Template*	Standard 7970 SCCP
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >

Exploiting the BUG of CISCO IP COMMUNICATOR

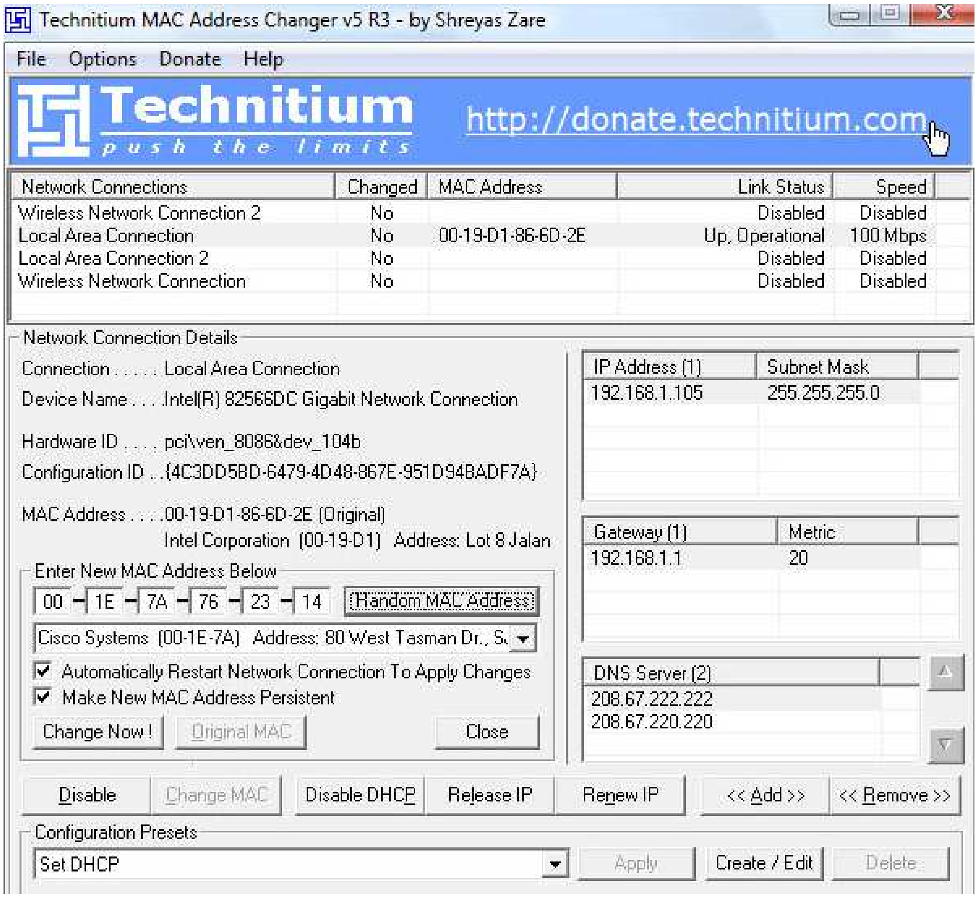
Prerequisite:

1. Check for user how Cisco IP communication installed on his system, by any method have ☺.
2. Get IP address of the user system locally or remotely by performing a network scan.
3. Get MAC address of user system locally or remotely (Using tools Nmap, advance IP scanner, Angry IP scanner etc.).

Exploiting the BUG:

1. For **IP based authentication**, simply change the IP address of the system to the IP address assigned to the user using Cisco IP Communicator.

2. For **MAC Based authentication**, install a MAC changer application e.g *technetium (TMAC), MAC Address Changer etc.*
   - Change your system MAC to the user system MAC Address by cloning MAC address. Attaching a screenshot for TMAC application for reference.


Technitium MAC Address Changer v5 R3 - by Shreyas Zare
File
Options
Donate
Help
Technitium
push the limits
http://donate.technitium.com

Network Connections	Changed	MAC Address	Link Status	Speed
Wireless Network Connection 2	No		Disabled	Disabled
Local Area Connection	No	00-19-D1-86-6D-2E	Up, Operational	100 Mbps
Local Area Connection 2	No		Disabled	Disabled
Wireless Network Connection	No		Disabled	Disabled

Network Connection Details

Connection . . . . . Local Area Connection
Device Name . . . Intel(R) 82566DC Gigabit Network Connection
Hardware ID . . . . pci\ven_8086&dev_104b
Configuration ID . . {4C3DD5BD-6479-4D48-867E-951D94BADF7A}
MAC Address . . . . 00-19-D1-86-6D-2E (Original)
Intel Corporation (00-19-D1) Address: Lot 8 Jalan

IP Address (1)	Subnet Mask
192.168.1.105	255.255.255.0

Gateway (1)	Metric
192.168.1.1	20

DNS Server (2)
208.67.222.222
208.67.220.220

Enter New MAC Address Below
00 - 1E - 7A - 76 - 23 - 14
Cisco Systems (00-1E-7A) Address: 80 West Tasman Dr., S.
☑ Automatically Restart Network Connection To Apply Changes
☑ Make New MAC Address Persistent

Now you are able to login with User (Victim) ID and make and receive calls from his number (Number allotted to the user by organization). I tried and exploited this bug and able to call from my HR number ☺ .