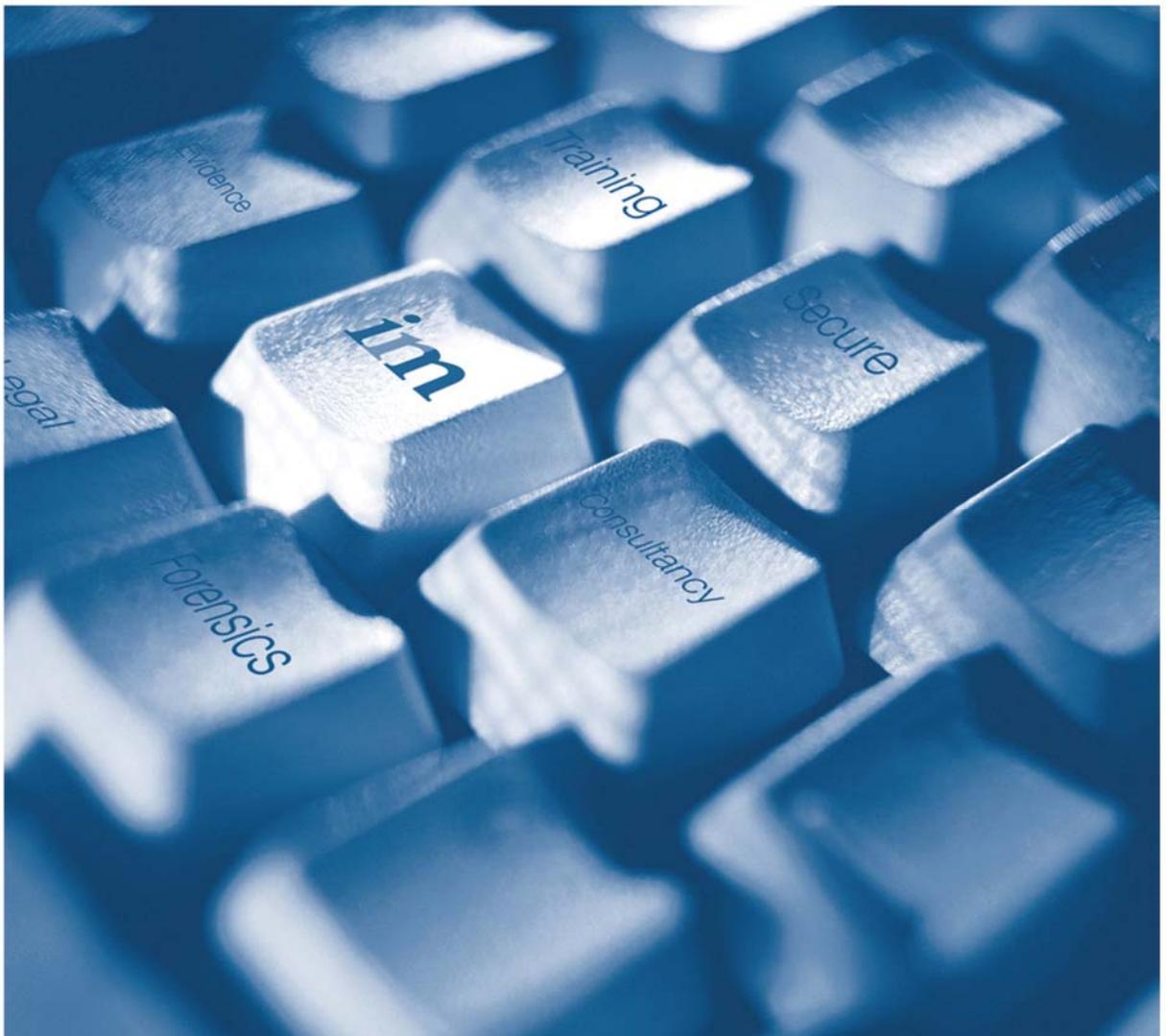




TARGETING VOIP

Kendric Tang



TARGETING VOIP

As more and more companies move towards a full scale replacement of conventional PSTN phones with a VOIP infrastructure, there is an increased incentive for malicious individuals to break into the phone architecture. The main benefit of implementing VOIP over conventional phone systems is cost saving and efficiency. With the primary concern about VOIP implementations being voice quality, latency and interoperability, the security aspects of VOIP deployments are often overlooked.

The traditional separation of the PSTN and data networks in conventional office infrastructures means that vulnerabilities in data networks will have minimum impact on traditional phone systems. However, now with the convergence of voice and data within the same communication environment, security vulnerabilities or weaknesses will be amplified across the two networks (e.g. a virus outbreak within the data environment could potentially affect the VOIP core devices hence bringing down the company's entire communication infrastructure). Therefore, there is a need to ensure the risk and impact introduced into the communication environment as result of this convergence is reduced to a minimum. This paper aims to highlight the potential security issues surrounding a typical Cisco VOIP deployment, how to exploit it, and some common measures to safeguard against them.

1.1 Information Gathering & Traffic Monitoring

One of the first things an attacker will do is to attempt to gather useful information pertaining to the VOIP infrastructure. Assuming that we have access to a connected IP phone, there are a number of areas where useful information can be obtained.

1. Configuration details from IP phones
2. Configuration details from the TFTP service
3. Network broadcast/multicast traffic

1.1.1 Retrieving configuration details from phones

1.1.1.1 IP Phones settings information

The IP phones themselves usually provide a wealth of information that can be useful in identifying useful targets and gaining an understanding of the VOIP infrastructure. By default, if the phone functions are not locked down, it will be straightforward to retrieve phone configuration information using the settings button on the phones to browse network information (e.g. information pertaining to the network location of VOIP core components such as CallManagers, TFTP Servers) and other related phone settings. Moreover, in a typical Cisco phone, the default key combination `**#` will permit a user to unlock specific phone functions to change its assigned settings.

Recommendation:

Consider disabling the Setting Access Setting for the phone from the Cisco CallManager Administration

1.1.1.2 IP Phones web service

The Cisco IP phones by default have a web service enabled. As no authentication is required to access the web pages, it is straightforward to retrieve statistics and configuration information by pointing a web browser directly to the phone's IP address.

Note: In a segregated environment, access to the web service may not be straightforward from a regular PC connected on the data VLAN to access the phone resources.

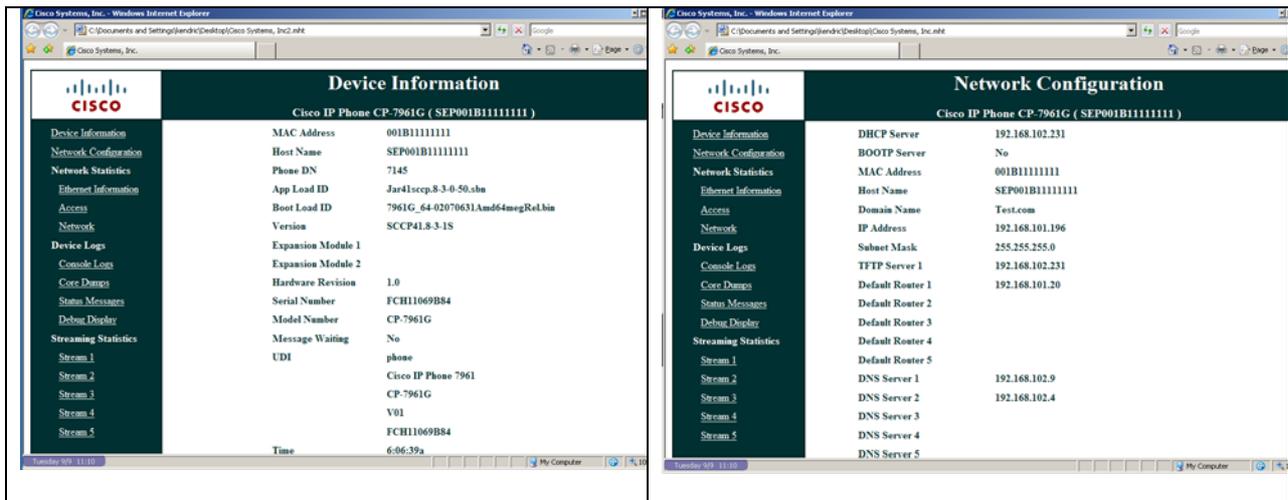


Figure 1: Example of information that can be retrieved from the phones' web service

Recommendation:

Consider disabling the web server functionality for the phone from the Cisco CallManager Administration

1.1.2 Retrieving configuration details from TFTP server

Each registered phone will have a configuration profile stored on the TFTP server which is used to configure the phones with the required setting for functioning on the network during every initialisation. The configuration file is constructed with the device id as part of the filename e.g. *SEPXXXXXXXXXXXX.cnf.xml*. As illustrated in section 1.1, this information is not secret and it is possible to construct the filename by referencing the phone's web service. Below is a simple command to retrieve the device ID from a list of live phones through the web service and then download the respective configuration files of the phones by connecting to the TFTP server. Similarly, the device ID can also be constructed from the phones MAC address.

```
for i in `cat live_phones.txt`; do GET
http://$i/CGI/Java/Serviceability?adapter=device.statistics.device | grep "( " | awk -F '(' '{print $2}' | awk '{print "get \"$1\".cnf.xml"}' | tftp [TFTP server IP address]; done
```

Note: In a segregated environment, access to the TFTP service may not be straightforward from a regular PC connected on the data VLAN to access the TFTP server resources.

1.1.3 Network broadcast/multicast traffic

Broadcast or multicast network traffic can provide useful information about the VOIP infrastructure. Depending on the configuration of the networking environment, it is usually possible to obtain information of the network by applying a network sniffer (e.g. Wireshark) on the network. It is worth examining network traffic from two perspectives:

1. Connecting a PC/laptop in replacement of a phone connection
2. Connecting a PC/laptop to the PC port of the phone

If not correctly configured, broadcast traffic such as ARP, CDP, HSRP, PIMv2, DHCP can provide information on the address range and IP addresses of core devices. Of particular interest are the CDP packets which contained the

VLAN information essential for VLAN attacks (see Section 1.2). Sniffing of CDP packets can be done using any one of the openly available tools such as Wireshark, tshark, Cisco CDP monitor etc.

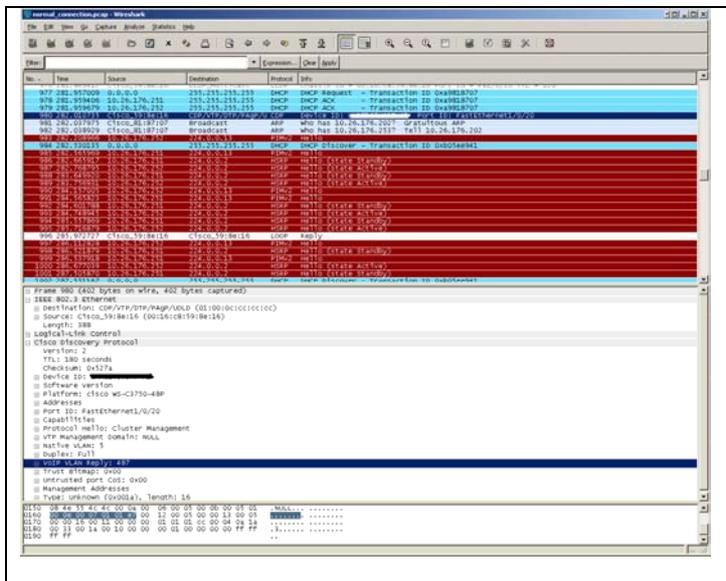


Figure 2: Example of broadcast/multicast traffic from VOIP VLAN on Native VLAN

Recommendation:

Restrict broadcast/multicast traffic from the voice network to the data network

1.2 Network Segregation

Segregation of the voice and data network within a VOIP infrastructure is critical for the security of any VOIP deployment. In an ideal scenario (in a security perspective at least), a physical segregation between the two networks will provide an optimum secure deployment scenario, but unfortunately, such a deployment will mean the cost of new networking equipment and laying new cables for the additional phone port across the entire infrastructure, which is not cost effective and cancels out the benefits of the interoperability and scalability of VOIP.

VOIP solutions are therefore designed to integrate voice traffic into existing data networks. In a typical VOIP infrastructure, the data and voice networks are transmitted through the same cable. Logical separations of the voice and data traffic are usually deployed by means of virtual VLANs where the voice and data networks are separated into different VLAN trunks with unique VLAN IDs. The network switch identifies network packets sent by the phones through the VLAN ID (VVID) and ensures that the traffics are directed to the correct network destination. Network traffic can also be throttled to give priority to voice traffic to fit the 'real-time' requirement of a voice conversation.

Unfortunately, assigning VLANs without network filtering are just considered separation of networks, and should not be mistaken as adequate network segregation. Below describes some the various attack vectors that can be performed in such an environment.

1.2.1 CDP Spoofing and VLAN Hopping

Cisco phones rely on the CDP protocol to obtain network information to communicate on the voice VLAN. It is important to understand that the CDP protocol is not designed as a security protocol and is only used for the purpose of sending network information to devices on the network.

VLAN hopping is a network attack whereby an end-system sends out packets destined for a system on a different VLAN that cannot normally be reached by the end-system. This traffic is tagged with a different VLAN ID to which the end-system belongs. Or, the attacking system may attempt to behave like a switch and negotiate trunking such that the attacker can send and receive traffic between other VLANs.

If CDP is enabled on the switch port and the Voice VLAN feature is enabled, it is possible to determine the Voice VLAN ID (VVID) by examining the CDP packets. This will allow the attacker to create a new Ethernet interface on the PC that tags the 802.1q VLAN header in the Ethernet packet. By successfully sniffing/spoofing the CDP packets and determining the VLAN ID, an attacker will be able to hop onto the voice network and gain access to resources permitted to the VOIP phones.

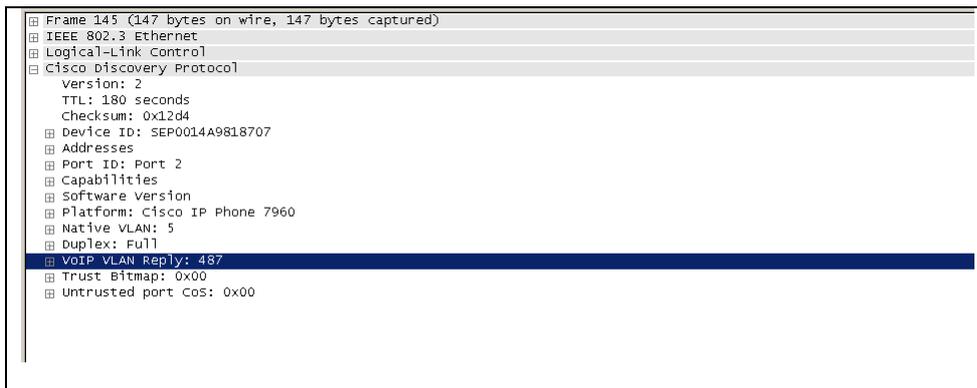


Figure 3: VOIP VLAN ID from CDP packet

To send Ethernet frames with the custom VVID in a Linux environment:

1. Install the 802.1Q VLAN implementation for Linux (<http://www.candelatech.com/~greear/vlan.html>). Or Install using your distribution’s package manager (e.g debian: ‘apt-get install vlan’)
2. Run ‘vconfig add eth0 487’
3. Run ‘dhclient eth0.487’ (assuming the phone IP addresses are configured by DHCP)

Alternatively, a tool called *Voiphopper* [1] was created to automate this whole process (including the ability to decode Avaya’s VLAN ID from the DHCP Option 176 L2QVLAN reply field).

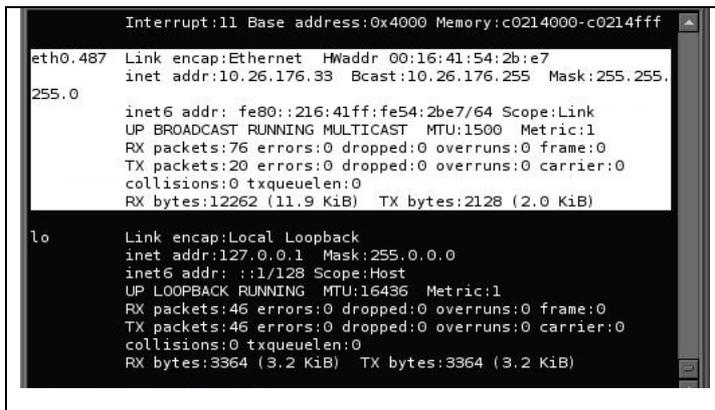


Figure 4: New virtual network interface created for VLAN connection in Linux

To send Ethernet frames with the custom VVID in a Windows environment:

1. Install Intel® PROSet for Windows with Advance Network Services (Assuming you are using an Intel network adaptor).
2. Go to Device Manager -> [Your adaptor] properties -> VLANs -> New -> [Input the VVID of your VOIP VLAN] -> OK
3. A new virtual adaptor will be created and an IP address will be assigned to the new adaptor to communicate on the voice VLAN (Assuming the phone IP address is configured by DHCP).

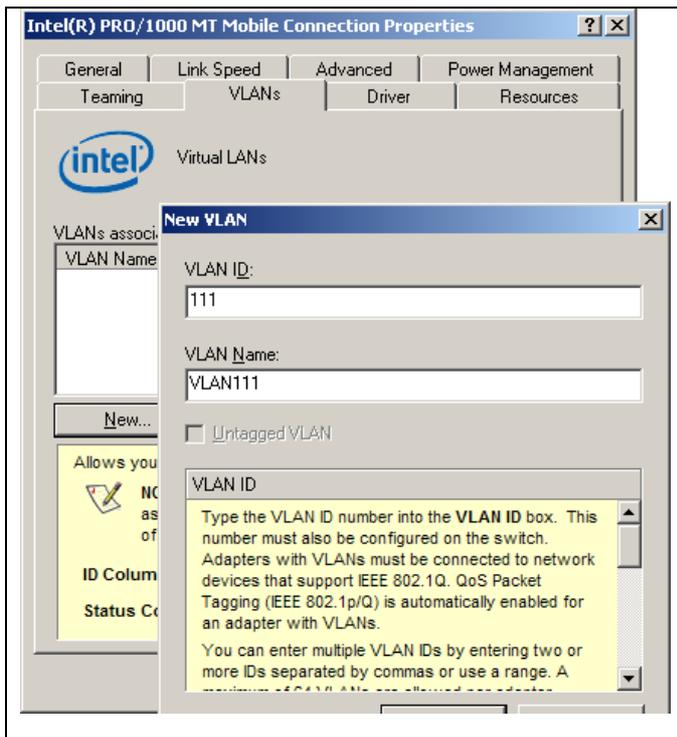


Figure 5: New virtual network interface created for VLAN connection in Windows

Having gained network access to the Voice VLAN would normally have opened up numerous other attack vectors such as ARP poisoning/spoofing attacks which can be used to hijack active voice traffic or execute man-in-the-middle attacks against other VOIP components. If there is insufficient network segregation between the voice VLAN and other parts of the data network (i.e. Finance, HR) it would be straightforward for an attacker to launch further attacks deeper into the network infrastructure.

Recommendation:

1. Ensure network segregation/filtering is correctly implemented. Devices connected to the voice VLAN should only be permitted to required services/ports required for voice communication.
2. If phones support 802.1x authentication, implement port level authentication on network access
3. Consider implementing port level ACLs to restrict outgoing connections

1.3 Targeting Core Components

After successfully hopping onto the voice VLAN, the main targets of interest are the VOIP core components that govern the functioning of the VOIP infrastructure.

In a typical Cisco VOIP environment, a number of critical components are essential for the functioning of the VOIP service. Each of these functions plays an important role in the IP telephony solution and various attack vectors can be associated with each of these identified components. Therefore, on top of the normal enterprise security policies (e.g server hardening, patch management), extra effort should be undertaken to minimise the exposure of these devices to potential threats.

1. TFTP Server – Responsible for the delivery of phone configuration and firmware updates. As the TFTP protocol is a simple form of FTP protocol that uses UDP and provides almost no security, it will be straightforward for an attacker to gain access to phone configurations with just knowledge of configuration filename. Write permission on the TFTP service should be investigated to ensure that configuration files cannot be changed or malicious configuration files cannot be introduced into the system.
2. Call Manager – CallManager is the heart of the VOIP infrastructure. It is a software-based call-processing component of the Cisco IP telephony solution. The software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, Voice-over-IP (VoIP) gateways, and multimedia applications. CallManagers are also responsible for the registering of the phones, extension mapping and tearing down of established connections.
 - Ensure that default/simple usernames and passwords are not used on the management interface
 - All running services should be correctly patched with the latest updates
 - Service hardening procedures should be applied
3. Voice Gateways - VoIP Gateways or Media Gateways are network devices that convert voice, fax, and other incoming calls between the public telephone network and an IP network. Gateways translate the varying coding techniques allowing companies to seamlessly communicate with other parties across other networks (VoIP or a standard phone service). The voice gateway is usually transparent to the client device.
4. Active Directory / LDAP Components – The active directory / LDAP components are usually incorporated into the design as active directory contacts and global address book integration. If not correctly implemented, it will be possible to extract useful information directly from the LDAP service. In addition, if the voice service uses the same Active Directory as the corporate environment, network segregation between the two networks will be much harder to enforce.
5. DHCP / DNS Service – Standard networking components used for IP address assignment and DNS resolution. Again, if the voice service shares the same DNS / DHCP service as the corporate environment, network segregation between the two networks will be much harder to enforce.

Recommendation:

Ensure appropriate patch management and server hardening procedures are followed in each server deployment

1.4 Integrity and Authentication

Integrity and authentication protections are important security measures that need to be considered when designing and securing a VoIP network. The Cisco integrity and authentication module provides the following modes of authentication (refer to Cisco Unified CallManager Security Guide for more information):

- o Image Authentication
- o Device Authentication
- o File Authentication
- o Signalling Authentication

Integrity and authentication protect against the following threats:

- o TFTP file manipulation (integrity)
- o Modification of call-processing signalling between the phone and Cisco CallManager (authentication)
- o Man-in-the-middle attacks (authentication)
- o Device and server identity theft (authentication)

1.4.1 Integrity and Authentication Protection Exploitation

Apart from the standard image authentication, a typical VOIP infrastructure does not have any of the other integrity and authentication mechanisms in place.

Phone authentication is performed through the Cisco SCCP protocol whereby the primary piece of information required for successful authentication is based on the device id of the phone. As was described in Section 1.1, it is relatively straightforward to retrieve the device id through various means via network services therefore making it straightforward to impersonate to the CallManager as a registered phone.

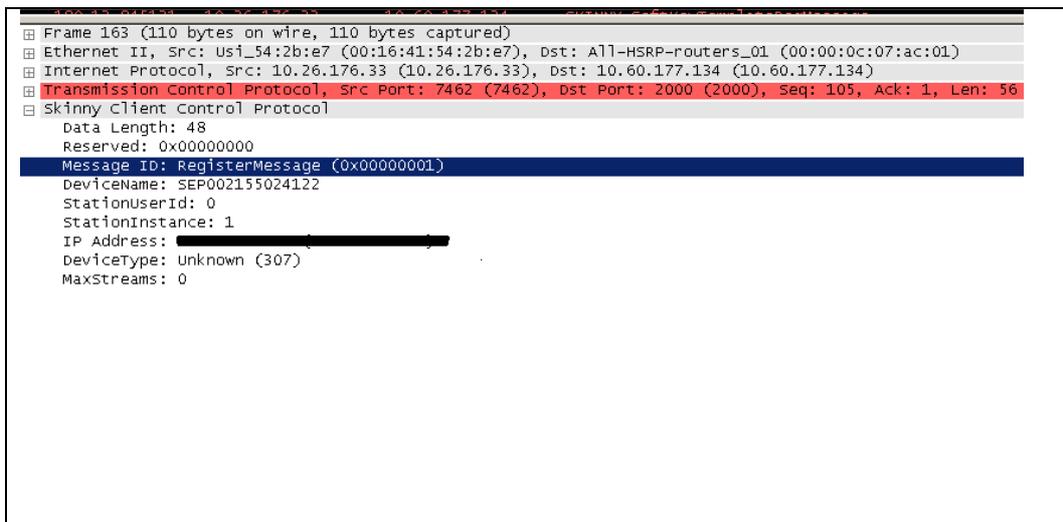


Figure 6: Example of a SKINNY protocol register message

To perform the impersonation attack, phone emulator software such as VT-GO by BlueIP can be used (Note: the trial version will only allow you to use the software for 2 minutes, which is sufficient as a proof of concept). As the phone configurations stored on the TFTP servers are specific to the phone model and is extremely sensitive to incompatible hardware profiles, it is important to customise the emulator to the phone model targeted (which can again be easily retrieved from the phone’s web service).

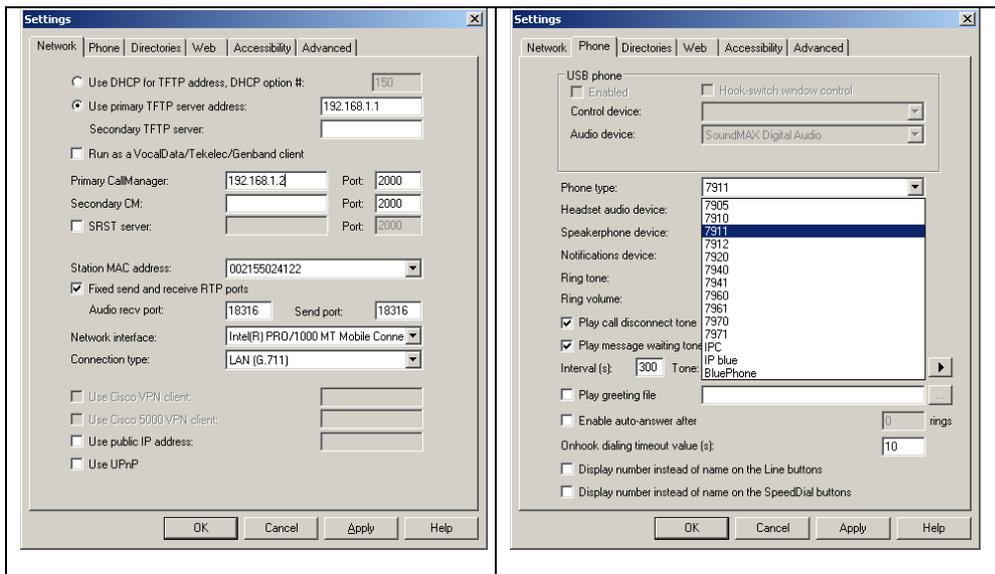


Figure 7: VT-GO configuration settings

One important factor to consider is that the phone software picks up the MAC address of your PC's network adaptors and constructs the device id using that information. To force a specify device id of a known registered phone, one of the ways to achieve this is by spoofing the MAC address of your Ethernet adaptor to that belonging to the targeted phone device. Once the VT-GO program is started and 'Station MAC Address' setting selected, the adaptor's MAC address can be reverted back to the normal to prevent conflicts on network. The TFTP server and CallManager should also be configured to that of the working VOIP environment.

The implication of this is that an attacker can hijack a phone extension and gain access to all available phone resources such as making and receiving phone calls. In addition, an attacker will be able gain access to the mailbox available to the phone extension if no further authentication is required.

Also, if the targeted phone is already connected to the network, the race condition between the spoof device and the real phone will cause a denial of service on the targeted phone.



Figure 8: Phone emulator showing a successful hijacked extension

Recommendation:

Implement the authentication and integrity controls as described in Cisco's *Cisco CallManager Security Guide* [2]

1.5 Media Encryption

Media encryption, which uses SRTP, ensures that only the intended recipient can interpret the media streams between supported devices. Support includes audio streams only. Media encryption includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.

If media encryption is not enabled on the voice payloads, when combined with the ability to hop onto the voice VLAN using a regular PC/laptop device, it will be straightforward using regular network attacks (e.g. ARP spoofing) to sniff and reconstruct RTP traffic with tools such as Wireshark (<http://www.wireshark.org/>) or Vomit (<http://vomit.xtdnet.nl/>).

Recommendation:

Implement media encryption by using the SRTP protocol

Conclusions

With the convergence of voice and data within the same communication environment, vulnerabilities or weaknesses will be amplified across both networks. Therefore, there is a need to ensure the risk and impact introduced into the communication environment as a result of this convergence is reduced to a minimum.

We have identified various ways to gather useful information from a VOIP infrastructure. The lack of network service or phone hardening can all contribute to the leakage of information where core devices in the network can be identified.

Since VOIP solutions are designed to integrate voice traffic into existing data networks, network segregation plays a critical role in ensuring the segmentation of voice and data traffic. Unfortunately, as seen in many VOIP deployments, applying VLAN separation is usually not sufficient in itself in ensuring network segregation. VLAN hopping attacks can be used to circumvent this separation and allow an attacker to gain access to the voice VLAN and resources made available to the phones. Once successfully hopping on the voice VLAN, numerous other vectors of attack will be available to an attacker.

The lack of integrity, authentication and encryption in a VOIP deployment may also result in impersonation attacks, denial of service and the ability to perform network attacks to sniff and reconstruct media traffic with ease.

References

[1] Voiphopper - <http://voiphopper.sourceforge.net/>

[2] Cisco CallManager Security Guide, Release 4.1(3) - http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/4_1_3/secugd.pdf

About the Author

Kendric Tang is a Senior Security Consultant who provides Information System security consulting services, specialising in wireless penetration testing and consultancy, scenario-based penetration testing, application security analysis and general security architecture reviews. Kendric is the head of the IRM's Centre of Excellence (CoE) for wireless technology. As a CoE he is the technical expert within IRM for all wireless-related technology and is also responsible for the research and development associated with any new wireless technology and attack techniques. Kendric is also heavily involved in research and development at IRM through which he has published a number of application related vulnerabilities.

About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at www.irmplc.com for further information.