UNIVERSITY OF ALBERTA

Capstone Project (MINT-709)
Implementation of Unified Communication and analysis of the Toll Fraud Problem

Presented by
Anuvansh Sharma

Supervisor
Dr. Mike MacGregor

Table of Contents

Introduction to the Traditional telephony system

The phonograph, invented by Thomas Edison in 1877, was a method of capturing the audio signal to give audio information, and speech technology has advanced significantly since then. Telephone networks quickly grew in the 1980s to handle practically all long-distance traffic. As voice and data merge in the current environment, many aspects of traditional telephony are changing. However, many others remain the same, such as the Public Switched Telephone Network (PSTN), which is still useful today. Long before the internet existed, the Public Switched Telephone Network created the foundation for long-distance communication. Before using connected digital circuit-switched phone systems, the PSTN used an analog global network of telephone equipment.

Understanding the Analog Telephony System

In analog telephony, the human voice is captured by the telephone's transmitter and converted into an electrical signal that changes continually in response to variations in sound. Analog sounds, like the human voice, are the original form of sound. As we speak different words, the sound wave is altered by changes in pitch and tone. The analog sound waves are captured by a microphone and an analogue circuit, and they are then sent electrically across copper wiring. The analog sound waves can be converted into electrical signals and sent across the PSTN to the other end of the phone line. The electrical signal is transformed back into analog sound waves and transmitted through the receiver speaker when it reaches its destination. Two wires are normally used to transport a basic plain old telephone service (POTS) line from the phone company to a residence or place of business. There is full-duplex voice communication over these two wires. The central office is the final PSTN hop before reaching the customer's location (CO). Your circuit is combined with those of other customers by the central office, which then switches them to other COs on the PSTN as needed. A local loop is a circuit you use to connect to the central office. [1] Figure 1.1 shows the PSTN network.

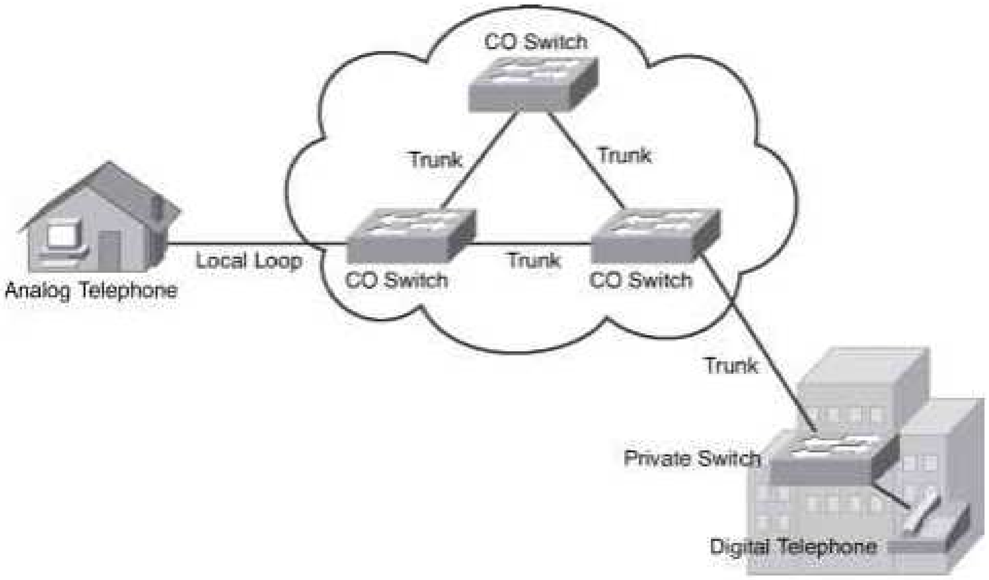


Figure 1.1 PSTN Components

Challenges with Analog Telephony

For many years, businesses have been sustained by analog systems. They are dependable, have good speech quality, and have the regular functions you might find in a typical home phone, such as hold, mute, redial, and speed dial. They are built on ordinary copper lines and POTS (plain old telephone service) phones. Additionally, they could be able to move calls between extensions. Their qualities, however, stop there. They are generally cheap because of their simplicity and constrained room for growth. However, analog systems can be expensive to maintain, set up, and upgrade due to their usage of less flexible technology. Another limitation is the distance. Since analog signals are only electrical on the line, they degrade when sent over long distances. Analog transmission distances can be increased with the aid of electrical repeaters (shown in figure 1.2).

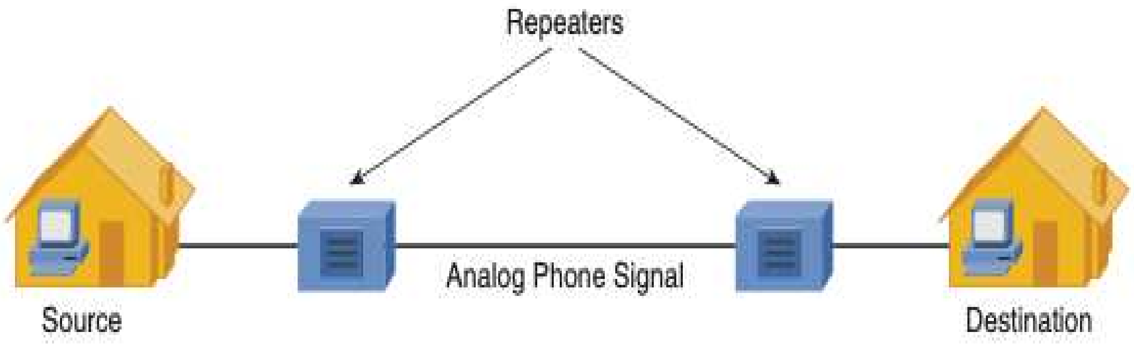


Figure 1.2 Repeaters for Analog Signal

While this may help to extend analog distances a little more, they eventually stop being useful. This is so that repeaters don't mistakenly think that electrical pulses on the line called noise are a component of the signal that needs to be repeated. A sizable amount of electrical noise now accompanies our original analog voice signal once the signal is repeated numerous times. The opposite side finally picks up the electrical noise, and audible static is heard on the receiving phone handset. [2]

Introduction to Digital Signal

Analog telephone signals are first converted to a discrete, quantized time format in a digital system. Time-division multiplexing (TDM), a technique in which each digitized telephone transmission is given a specific slot within a predetermined time period, is then used to multiplex the signals. Digital signals become noise-immune due to the analog nature of noise responses, which allows intermediate devices to readily distinguish between the data signal and noise, allowing them to transcend the limitations of analogue signals in telephony. [3]

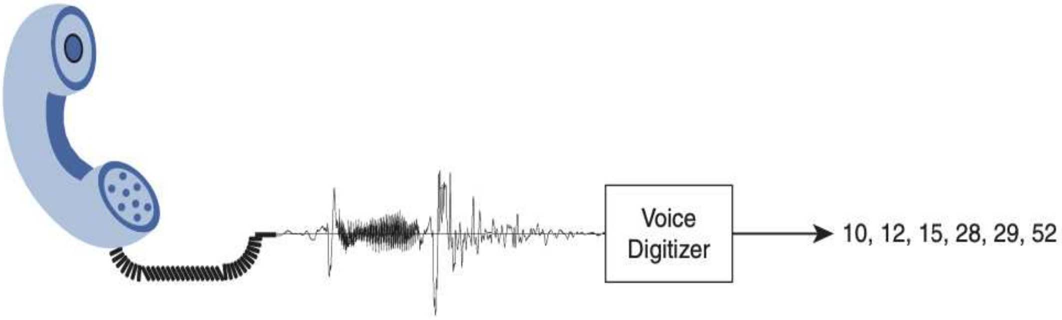


Figure 1.3 Analog to digital conversion

New Frontier: Voice over IP (VoIP)

VoIP, to put it simply, is the process of putting 1s and 0s into a data packet with headers containing IP addressing information. Instead of having a separate phone and data system, we can take that VoIP packet and send it through the existing data network. The main advantage appears to be the reduction of cable prices alone. However, if we look more closely at the effects of running voice over data networks, we start to find several hitherto unrealized advantages.

Benefits of VoIP include the following [4]:

1. Communication costs are reduced because VoIP lets you relay conversations through WAN connections rather than using pricey tie lines or toll fees to connect offices.
2. Cutting the cost of cabling in half is a common practice for VoIP deployments, which operate a single Ethernet connection in place of separate voice and data connections.
3. A typical PBX system's moves, adds, and changes (MAC) are estimated to cost between $55 and $295 per device. This cost is essentially gone with VoIP phone systems. Additionally, IP phones are increasingly plug-and-play, enabling migrations with little to no voice network reconfiguration. Additionally, users can bring IP phones home with them while keeping their work extension when used in conjunction with a VPN configuration.
4. SoftPhones are the best illustration of what is possible when voice and data networks are combined. Users can use their laptop or desktop as a phone. SoftPhones are becoming more and more connected with other programmes, including video telephony, instant messaging, and email contact lists.

Understanding Private Branch Exchange (PBX) systems

Numerous companies support hundreds or even thousands of phones throughout the organization. The expense of buying a direct PSTN connection for each of these phones would be expensive for the business. Instead, most businesses decide to handle their internal phones using a PBX system. Internal users can call each other within the office utilizing these systems without using PSTN resources. We can simply call them mini telephone exchanges

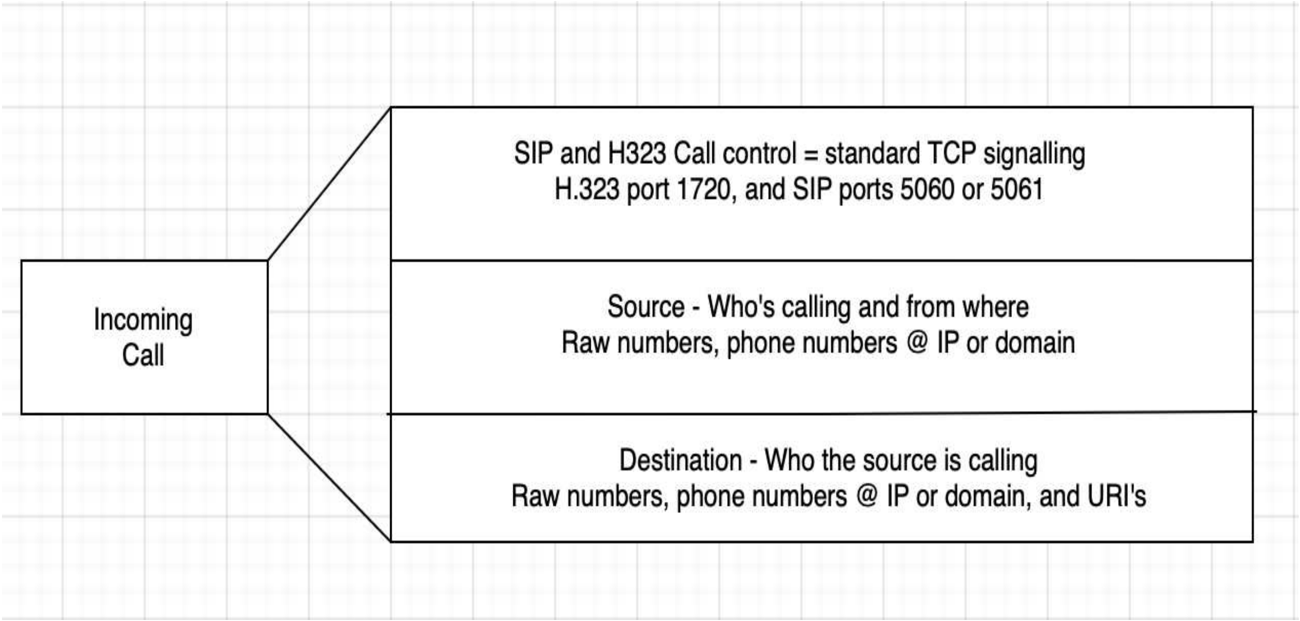
Types of PBX:

There are three types of PBX system that you may come across, each has it own functionality.

1. **Traditional Analog PBX:** These systems, which have been around for a while, use Plain Old Telephone Service (POTS) lines to connect to the Public Switch Telephone Network (PSTN). By being physically connected to phones and fax machines via copper cable, the PBX controls calls between them. Calls can be moved between phones via the PBX, and incoming calls are routed through the PBX and out to the phones. The analog PBX is linked to POTS lines, which exist before the Internet. These systems are limited in terms of flexibility, scalability and are incompatible with several functions of contemporary phone systems, including voicemail-to-email. [5]
2. **IP PBX or VoIP PBX:** By connecting phone lines over the internet and potentially enabling remote access for employees, IP (internet protocol) PBX systems allowed organizations more flexibility. They also offered extra capabilities like messaging and video conference sessions. Systems with IP PBXs use a process known as SIP trunking (session initiation protocol). SIP is an application layer that enables you to connect phone systems over the Internet and run a phone service over your office network. Although IP PBX is a little more adaptable than classic PBX, it still requires a sizable upfront investment and specialists to operate your IP phones.

3. **Hosted PBX:** A hosted PBX (or virtual PBX) solution moves your phone system "in the cloud". In other terms, a hosted PBX is a VoIP-based PBX that a service provider manages and that enables companies to connect to via the public Internet. As a result, the client no longer has to pay for PBX maintenance, struggle to update PBX software, or deal with service failures because these problems are taken care of by the service provider you enter into a contract with.

The Call Components


Incoming Call
SIP and H323 Call control = standard TCP signalling
H.323 port 1720, and SIP ports 5060 or 5061
Source - Who's calling and from where
Raw numbers, phone numbers @ IP or domain
Destination - Who the source is calling
Raw numbers, phone numbers @ IP or domain, and URI's

Call Control: In call control signalling, the caller starts the conversation and ends it by hanging up. Two-way voice is the medium that has been set up, and RTP (Real-time Transfer Protocol) is used to stream the data. The calls are established up using the H.323 and SIP protocols, which are both widely used.

Examples of SIP requests [6]:

1. **INVITE:** Opens a dialog that will initiate the call. INVITE include a unique identifier for the call, the destination address, source's address, and information about the type of session that both the entities wishes to establish.
2. **200OK:** Corresponds to any request's success. The information returned with the response depends on the method used in the request like INVITE, REGISTER.
3. **Bye:** At the end of the call, BYE message is used the terminate the session gracefully. The other party that receives the BYE, confirms the receipt by sending 200 OK response. This terminates the BYE transaction.
4. **Cancel:** is used to cancel a previous request sent by a client. Specifically, it asks the server to cease processing the request and to generate an error response to that request. CANCEL has no effect on a request to which a UAS has already given a final response (200 OK, ACK).

Examples of H.323 requests [7]:

1. **Q.931 SETUP**: Initiate the call once the TCP connection has been established between two entities.
2. **Q.931 CONNECT**: Once the call has been answered by the remote side it shares the IP and port on which they want RTP to be connected using CONNECT message.
3. **Q.931 BYE**: This is used to terminate the call gracefully.

SOURCE: It defines who is the originator of the call. Every protocol has a different set of messages that help the Voice application understand the source of the call. Below are the headers used:

a. SIP uses FROM header. The From header as the name says specifies who the call is coming from. Syntax of the from:
   From: “{name/number}”<sip: (user)@(domain)>
b. H.323 carries calling information in its Information Elements (IE). The IEs carry information related to the message type, such as calling and called number, bearer capability and so on.

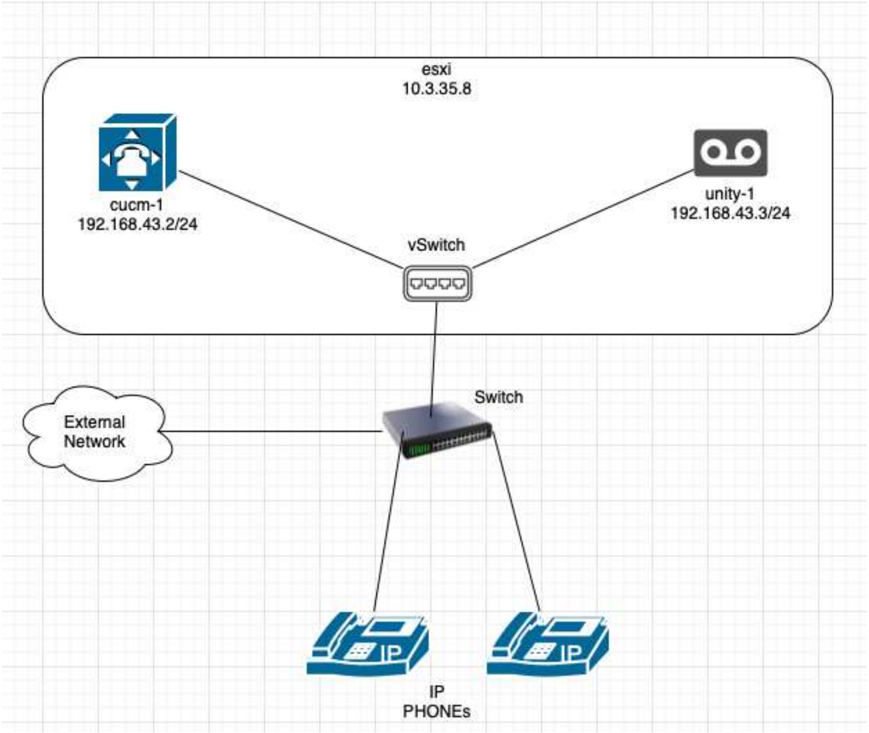
DESTINATION: It defines to whom the call is intended for. H.323 carries this information in its IE however SIP uses TO header to denote the destination of the message which has similar format as FROM header. Below is the syntax of SIP TO header:

To: “{name/number}”<sip: (user)@(domain)>

Attackers who commit toll fraud often conceal their point of origin IP address by "spoofing," or they alter their domain suffix by using a fake domain.

Lab Setup

To recreate the most typical and straightforward arrangement in the businesses, we used Cisco Unified Communications Manager and Cisco Unity Connection in the lab setup for this project. The network topology we employed in the lab is shown below:



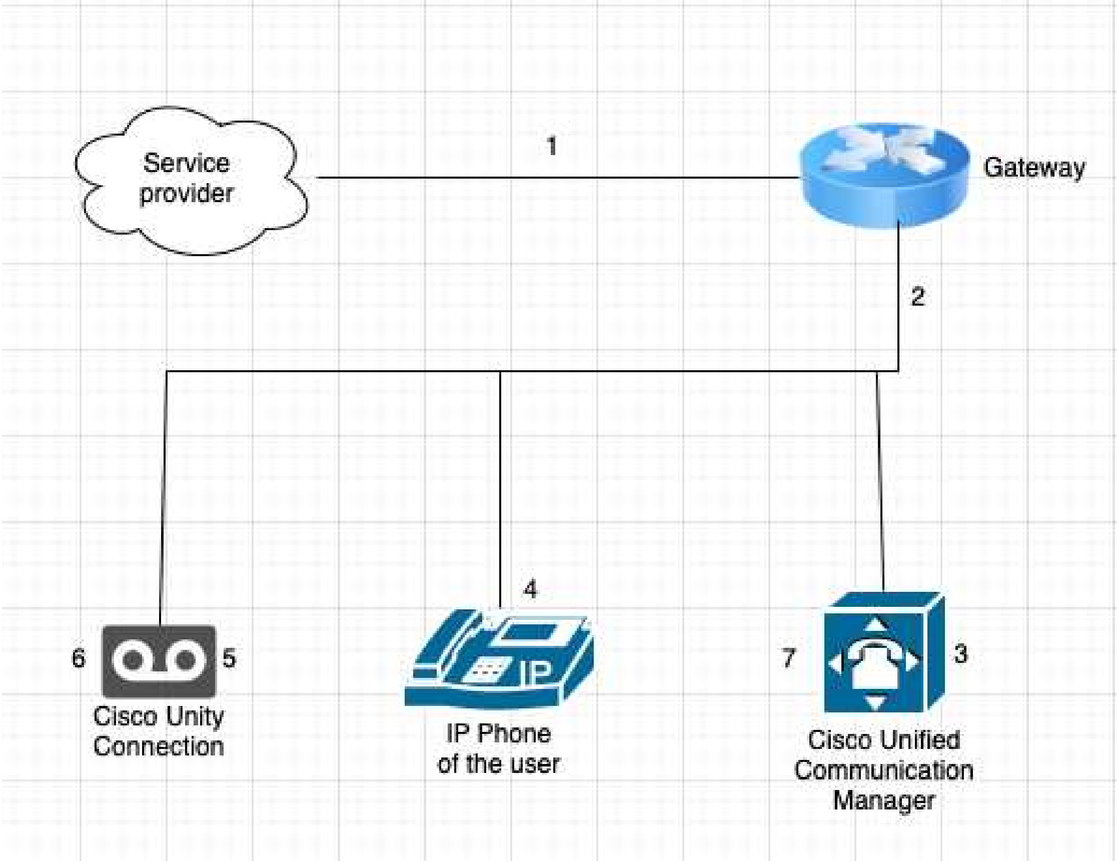
The Cisco Unified Communication Manager, or cucm-1, offers tools for managing calls, including call processing, dial plan management, directory services, and other things. In our configuration, it primarily serves as a call processing application for an enterprise that aids in call routing to the proper destination.

Cisco Unity connection (unity-1) is a unified messaging and voicemail solution by Cisco. It lets users access and manage messages from an email inbox, web browser, IM, IP Phone, or any other personal device.

The Integration between Communications Manager and Unity Connection is Session Initiation Protocol (SIP).

Reference:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/cucm_sip/b_cucintcucmsip.html

Under ideal circumstances, the call flow between Communication Manager and the Unity connection is relatively simple. The process of routing an external call to our system is described in full below.



1. The caller from the outside dials a DID (Direct Inward Dialing) that belongs to a user that is logged into a phone that is connected to Cisco Unified Communication Manager. The call is forwarded to our organization's gateway by the service provider.
2. As per the dial-peers configured on our gateway we either scrap the 10-digit number to a four-digit extension of our user or sends the call as it to our Call manager.
3. By default, Cisco Unified Communication manager routes the call based on the called number. The Unified Communication Manager routes the incoming call to the IP Phone that is set up with that number based on the data provided by the gateway.
4. The call rings several times on the IP Phone once it reaches there, but no one answers. Any unanswered call will be forwarded to voicemail after a certain number of rings according to the configuration of the Unified Communication Manager. The call will then be forwarded to Unity connection by the Unified Communication manager.
5. Unity Connection answers the call and uses the IP Phone's extension to take a message. All the extensions configured on the call manager to have voicemails are listed in a database maintained by Unity Connection. A caller's message is recorded by Unity Connection and then saved.
6. Unity Connection then detects a fresh voicemail for the IP Phone and transmits the message waiting indicator (MWI) on code to the communications manager. When there is a voicemail, the message wait indicator (MWI) assists in turning on the phone's light and blinking the message symbol on the IP Phone.

7. The IP Phone then receives this notification from Unified Communication Manager. In order to notify the user of a new message, IP phones now display an MWI.

The Problem: Toll Fraud

Unsecured or inadequately secured PBX and VoIP cloud communications services are vulnerable to hackers and fraud, resulting in service disruptions, downtime, call quality issues, and direct financial loss. Voice over IP is vulnerable to attacks, just like any other network technology. According to the Communications Fraud Control Association (CFCA) Fraud Loss Survey Report, there was a loss of US$39.89 billion in the year 2021, an increase of nearly 28% from 2019 to 2021.

Organizations are migrating from legacy telecommunications to Voice over IP (VoIP), allowing for greater flexibility, resilience, and overall cost savings. The Session Initiated Protocol (SIP) is widely regarded as the most important VoIP protocol in the business-to-business market, but its proper implementation and configuration are not always well understood. Failure to configure SIP systems correctly has resulted in significant fraud exploiting a variety of vulnerabilities, with billions of dollars stolen from businesses of all sizes each year through PBX Hacking via the medium of Toll Fraud. Toll Fraud is one of the most common attacks that enterprises face where attackers try to find a path to their Service Provider resources, so they can use that infrastructure to place free long- distance telephone calls. The reason for these Toll Fraud attacks is not just simply to illegally make a phone call on a given company's infrastructure without any cost, it can also take a far more serious aspect in which once accessed, the Toll Fraudster adds the affected company's system to a fraudulent dialer-server, and where they are fraudulently selling public calling cards using its resources or can ask sensitive information from customers by wrapping around their number with enterprise numbers. The Amount of money stolen in this event often goes beyond EUR 1 million [8]. Due to the number of Toll Fraud attack calls using up all of the unit's resources, Toll Fraud can also result in a Denial of Service type of attack when and if the application's licence or resources are maxed out. At that point, the unit is unable to make or receive calls until the resources have been released.

Certain Linux-based tools such as Kali Linux are typically used for scanning IP addresses and use them as a target for DoS attacks, hacking or Toll Fraud. Similarly, open-source Asterisk servers are often used by Toll Fraud attackers for internet-based SIP calls.

The IP-PBX systems or related VoIP applications, such as voicemail servers, video conferencing servers, etc., are not topology-aware servers, hence they have no influence over events that take place outside of their platforms. Therefore, the only way to stop rogue calls from entering the device, being processed, consuming call licences, being recorded in the Call Search History, using up CPU cycles, etc. is by blocking the traffic at the external firewall, that is, as it enters the network, preventing it from being routed to these systems at all.

Restricting Toll Fraud

Toll fraud in the enterprise could occur due to negligence of users or due to misconfiguration of the devices in the enterprise. We could follow below mentioned best practices to avoid the toll fraud [9]:

a. Regularly modify your system passwords. Setting mandatory password ageing and logoff notification during login administration for these logins, you must set passwords during setup. Make sure the password-resetting process is well-regulated.
b. Deny system access to unauthorized users using authorization codes.
c. Prevent external callers from pressing unexpected digit combinations when given prompts or restrict access to dial tones on auto attendants.
d. Depending on the needs of the business, restrict access to the ability to make international calls or restrict access to only certain locations.
e. Keep an eye out for strange patterns in system activity and traffic and review Call Detail Reports (CDR) on daily basis.
f. Users of the system should be made aware of toll fraud so they can respond accordingly.

In addition to the aforementioned best practices, we also need to check that our devices are configured correctly because an attacker could exploit a gap on any of the possible hops in the call path. The principles and configurations of our lab devices that we should keep in mind for each device to defend our business against toll fraud assaults are covered in the next section.

Restricting Toll Fraud on Cisco Unified Communication Manager

Class of Service (CoS):
We don't want to leave our communications manager wide open and let anyone to use it to call long distance or international lines. We can specify who is barred from dialing certain lines using classes of service. Therefore, we use this to regulate who can call what numbers when and how. Additionally, we may ensure that calls with the same number are routed differently for each user and/or site by using various gateways.

Let's imagine we have a phone at the front desk of our company or even in a common area. Since it is in the open, we'll want to make sure it is restricted. We may even suggest that only internal calls and 911 can be made by anyone from that phone. This limits the phone's ability to place long distance calls. Unlike the phones at our employees' workstations, which can call both internal and exterior extensions. According to the phone and the needs the phone has, that is how we need to plan several service classes.

Ideally, we want to route calls to the same number differently depending on the time of day. Another choice is to indicate that the call should go somewhere else between 5 and midnight and here is where it should go between 9 and 5.

There are different components that we can use to implement CoS on our Communications Manager to prevent toll fraud [10]:

a. **Partitions and calling search spaces (CSS)**
   Calling search spaces contains the list of partitions. Partitions are set up, then applied to extensions. The same partitions are configured for directory numbers that share comparable reachability characteristics. The partitions are then listed in a calling search space that will specify which partitions are accessible to a specific device. The calling search space is then applied to the device.
   Simply said, from the standpoint of a directory number or an IP phone, Calling Search Spaces describe "who I can call" while Partitions define "who can call me."
   The flexibility to implement segmentation and control to the number that can be called, or vice versa, is therefore made possible by partitions and calling search spaces together.
   As a best practice, either turn off Call Forward All or only allow it for an extension that is internal to our network. Additionally, only internal partitions should be able to use Call Forward Busy and Call Forward No Answer.

b. **Time-of-Day Routing**
   We can make some partitions accessible only during specific hours of the day by using time schedules and time periods. Thus, it permits some partitions to be active for a set amount of time each day, beyond which time they automatically become inactive. Helps limit after-hours calls to local, national, and international lines.

c. **Client Matter Codes (CMC) and Forced Authorization Codes (FAC)**
   CMC and FAC make it possible for us to control call access and accounting. For billable clients, CMC helps with call accounting and billing, while Forced Authorization Codes limit the kinds of calls that specific users may make. Client matter codes require the user to enter a code to identify the call as being related to a particular client call. For call accounting and billing purposes, you can assign client matter codes to clients, students, or other demographics. Before the call, the Forced Permission Codes feature compels the user to submit a legitimate authorization code. Thus, used to regulate access to long-distance and international calls. Calls processed by the FAC and CMC are recorded in the CUCM Call Detail Records (CDR).

d. **Block off-net to off-net transfers**
   We can classify a call to be either “OnNet” or “OffNet”.
   Calls made within your own network of telephony devices are often referred to as "OnNet" calls. This usually refers to calls between devices that are set up by the cluster itself within a CUCM cluster of devices.
   Conversely, calls made to devices outside of your local network of devices are referred to as "OffNet." It is an OffNet call, for instance, if you are calling from your cluster to any external PSTN device (such as a cell phone).
   “Block OffNet to OffNet Transfer” is a cluster-wide setting on Cisco Unified Communications Manager that enables us to stop users from forwarding external

calls to additional external numbers.This parameter specifies values as "True" or "False".
External calls cannot be forwarded to another external device when the option is set to "True." False is the value specified by default. Using the Service Parameter Configuration window, you can change the "Block OffNet to OffNet Transfer" service parameter.
When the service parameter "Block OffNet to OffNet Transfer" is set to "True," a notification indicating that the call cannot be transferred appears on the user phone when a user attempts to transfer a call on an OffNet gateway or trunk.
By doing this, the chance that the functionality will be abused to make international calls from our system is reduced.

e. **Ad hoc conference restriction**
When the initiator of an ad hoc conference call hangs up, the call is terminated. All of the resources allotted to the conference are released by Cisco Unified Communications Manager. Cisco advises that you set this service option to "Never" in order to take use of the extra capability that advanced ad hoc conferencing offers. A meeting could be unintentionally ended in any other situation. However, This parameter ensures that the other parties (such as external users) cannot initiate a call to another external number.

Toll Fraud Prevention on Call Manager Express

For SIP line side on Unified CME, Unified CME 12.6 enforces security and toll fraud prevention. The Toll Fraud Prevention feature in Unified CME Release 12.6 is improved by imposing security on the SIP line side of Unified CME. The feature upgrade protects the Unified CME system from potential SIP line-side toll fraud exploitation by unauthorised users.
Toll Fraud Prevention on Unified CME for secure calls over SIP lines has some important features, including [11]:

a. All the **REGISTER** messages from SIP lines to be processed.
b. **REFER** message from SIP lines to be processed only on Primary CME, when Secondary CME is enabled (Refer-To: urn:X-cisco-remotecc:token-registration).
c. All the SIP line messages that are triggered from the endpoints to Unified CME are authenticated.
d. If the IP address of the endpoint is not part of the IP address trusted list, the call is not placed through Unified CME.

All line side endpoints must register with Unified CME as part of the configuration for toll fraud protection on Unified CME 12.6. The **ip address trusted authentication** configuration blocks unauthorized calls from the line side, this is enabled by default in Unified CME. In the **iptrust-list** configuration mode, input the IP address or subnet of the trusted phone to manually set your Unified CME endpoints as trusted.

Below are some CLI commands that can be used [11]:

a. To verify the manually added IP address of CME endpoints:
   sh run | s voice service voip

b. The "show ip address trusted list" command shows a list of IP addresses that are trusted. The following lists contain a display of the trustworthy IP addresses:
   - **Dial Peer**: Provides information on the IP addresses of the phones that are set up using the dial-peer setup option (only applicable for trunk side).
   - **Configured IP Address Trusted List:** Provides details on the manually configured IP addresses that are trusted.
   - **Dynamic IP Address Trusted List:** Provide information on the registered phones' IP address. This list was first released with Unified CME 12.6.
   - **Server Group:** Gives information about the phones' IP addresses that are set up in the server-groups configuration mode.

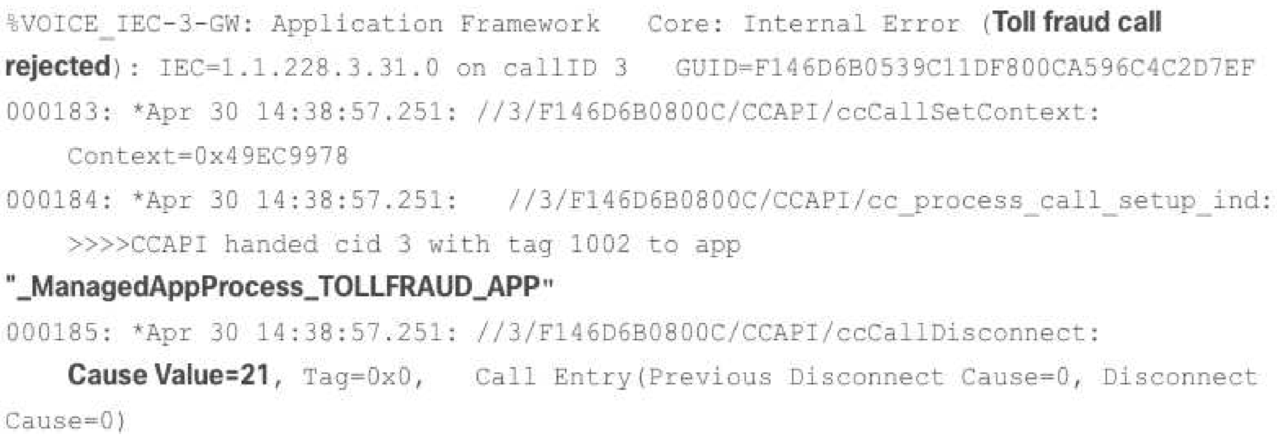
c. Execute the command **"show ip address trusted check <ip address**>" on Call Manager Express, to see the details pertaining to a given phone.

d. In sip configuration mode, the CLI command "**silent-discard untrusted**" discards SIP requests from untrusted sources. On Unified CME, this command is turned on by default.

Toll Fraud Prevention on Cisco Gateways

Cisco IOS voice gateways running Cisco IOS 15.1(2)T and later by default have an application active that helps thwart efforts at toll fraud. The router automatically adds the destination IP address(es) designated as an IPv4 target in a VoIP dial peer to the trusted source list as a result of this capability. Prior to IOS 15.1(2)T, the voice gateway's default behaviour was to accept call setups from all sources. The default configuration will treat a call setup from any source IP address as a genuine and trusted source to start up a call for as long as voice services are active on the router. A router running IOS version 15.1(2)T or later boots with a toll-fraud protection programme, thus any destinations configured as IPv4 targets in a VOIP dial-peer will instantly be included to the trusted source list.

The Q.850 disconnect cause value of 21—which denotes "Call Rejected"—will be produced by the TOLLFRAUD APP if the call is being rejected. To get the cause value, run "**debug voip ccapi inout**" on the CLI of the gateway. It is also possible to enable voice iec syslog to further confirm whether the call failure was caused by the toll-fraud protection. This setup will print out that the call is being denied owing to toll call fraud, which is frequently useful for identifying the gateway's point of failure. The following debug output serves as an example of the CCAPI and Voice IEC output: [12]



```
%VOICE_IEC-3-GW: Application Framework   Core: Internal Error (Toll fraud call
rejected): IEC=1.1.228.3.31.0 on callID 3   GUID=F146D6B0539C11DF800CA596C4C2D7EF
000183: *Apr 30 14:38:57.251: //3/F146D6B0800C/CCAPI/ccCallSetContext:
    Context=0x49EC9978
000184: *Apr 30 14:38:57.251:   //3/F146D6B0800C/CCAPI/cc_process_call_setup_ind:
    >>>>CCAPI handed cid 3 with tag 1002 to app
"_ManagedAppProcess_TOLLFRAUD_APP"
000185: *Apr 30 14:38:57.251: //3/F146D6B0800C/CCAPI/ccCallDisconnect:
    Cause Value=21, Tag=0x0,   Call Entry(Previous Disconnect Cause=0, Disconnect
Cause=0)
```

Class of Restriction (CoR)

A Cisco voice gateway feature called Class of Restrictions (CoR) makes it possible to assign calling privileges or classes of service (CoS). Although it can be used with any dial peer, it is most frequently utilised with Cisco Survivable Remote Site Telephony (SRST) and Cisco CallManager Express. Similar to CUCM partitions and CSSs is the class of restriction (CoR). Either dial peers or ephone-dns on a voice gateway implement CoR. It is analogous to constructing a CUCM partition using the "**dial-peer cor custom**" command as opposed to a CUCM CSS using the "**dial-peer cor list**" command. CoR can be used on SIP and H.323 gateways as well as in SRST mode on a gateway. [13]

Understanding Call Handlers on Unity Connection

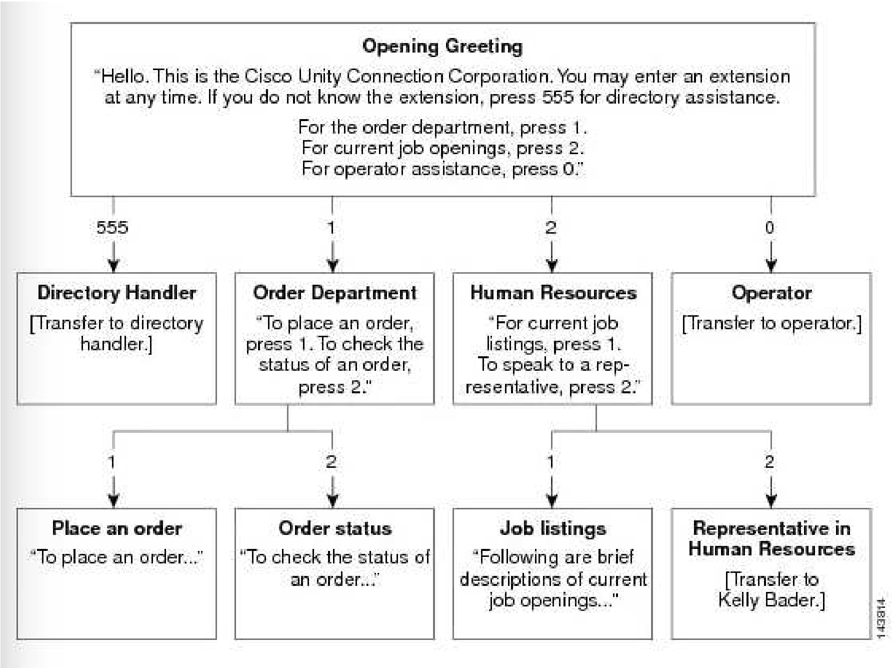
In Cisco Unity Connection, a call handler can perform a variety of tasks. A call handler can collect messages, transmit calls to other call handlers or users, play prerecorded announcements, and answer calls [14].

The following are some uses for call handlers:

1. **As an automated attendant**—A call handler can be utilized to answer and direct calls instead of a human operator by playing greetings and reacting to DTMF's. We can also setup a menu for the caller (for example, "For Sales, press 1; for Service, press 2; for our business hours, press 3.").
2. A call handler can be used to provide information that consumers commonly ask for by providing **preset audiotext** (for example, "Our normal business hours are Monday through Friday, 8 A.M. to 5 P.M.").
3. For the organization, a call handler can be utilized to take messages (for instance, "Our customer service personnel are all extremely busy. We will call you back as soon as we can. Just leave your name, phone number, and account number ").

4. A call handler can be used to transfer calls to another call handler, an operator (for instance, after hours, you could transfer calls to a technical assistance call handler directly to the person who is on call's mobile phone), or both.
5. We may make schedules for the greetings that are played at different times of the day and the extensions to which calls are routed at particular times of the day.

An overview of how the call handler functions is shown in the figure [15] below:


Opening Greeting
"Hello. This is the Cisco Unity Connection Corporation. You may enter an extension at any time. If you do not know the extension, press 555 for directory assistance.
For the order department, press 1.
For current job openings, press 2.
For operator assistance, press 0."
555
1
2
0
Directory Handler
[Transfer to directory handler.]
Order Department
"To place an order, press 1. To check the status of an order, press 2."
Human Resources
"For current job listings, press 1. To speak to a representative, press 2."
Operator
[Transfer to operator.]
1
2
1
2
Place an order
"To place an order..."
Order status
"To check the status of an order..."
Job listings
"Following are brief descriptions of current job openings..."
Representative in Human Resources
[Transfer to Kelly Bader.]
143814

One of the following approaches can be used in Cisco Unity Connection (CUC) to transfer calls to Cisco Unified Communications Manager [16]:

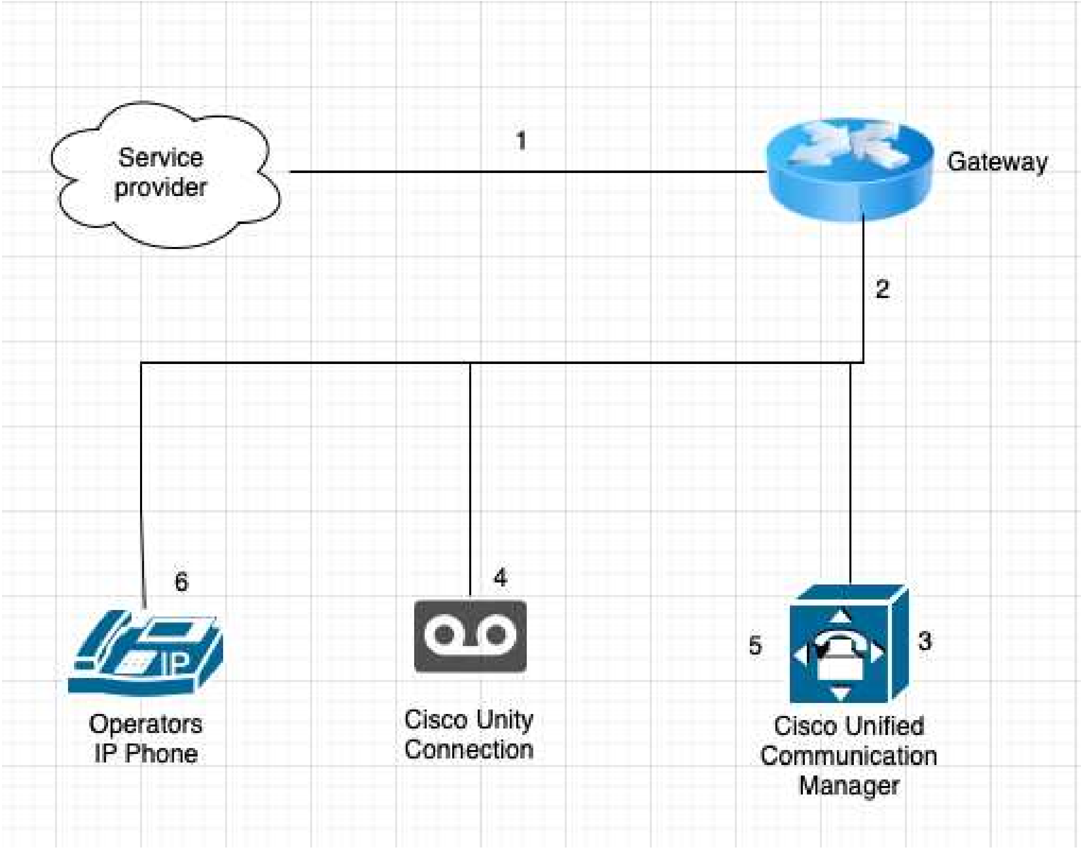
1. To place a call outside of CUC, set up the call action "**Transfer to Alternate Contact Number**" under "**Caller Input**." To transfer the call, dial the appropriate digit while on the line.
   To use this option, remember to take the following things into account:
   - Through the CUC Admin page, only administrators can activate this feature and choose the extension number. This option cannot be enabled by users. However, if an administrator makes this option available, users can do so through the Telephone User Interface (TUI).
   - When a user modifies their extension number through a TUI, the restriction table is checked.
   - When an administrator modifies the extension number via the CUC admin interface, the restriction table is not checked.
2. If the Greeting page's "Allow Transfers to Numbers Not Associated with Users or Call Handlers" check box is selected, dial any number. Only when the "Default System Transfer" restriction table allows it, CUC executes the transfer.

3. After the greeting, select Conversation. Two different kinds of conversations can be utilised for this:
    - **Caller System Transfer**: Callers are asked to input the number they want to be transferred to during this exchange. Only when the Default System Transfer restriction table allows it, CUC executes the transfer.
    - **User System Transfer:** Callers are instructed to access CUC after this conversation. CUC prompts the caller to enter the number they want to transfer to after they have entered their user ID and PIN. Only when the transfer is approved by the transfer restriction table linked to the user is it carried out by CUC.
4. While the Call Handler's Greeting is playing, call any User or Call Handler's extension. To transfer the call to any number, the User's or Call Handler's Transfer Rules can be changed.
5. To transfer the call to the Transfer Rules of any User or Call Handler, use the After Greeting action of the User or Call Handler. To transfer the call to any number, the User's or Call Handler's Transfer Rules can be changed.

The following integration needs had to be met in order to make the call from Unity Connection to an outside number using Communication Manager:

- The SIP trunk's Rerouting CSS must have the partition of the Route Pattern to the PSTN number.

General overview of the Call Flow:



1. The caller dials a DID (Direct Inward Dialing), which can either be our front desk number or can divert to our organization's IVR. The service provider routes the call to the gateway of our company.
2. We forward the call to a specific extension set up on our call manager in accordance with the dial-peers defined on our gateway.
3. The call has now been forwarded to the communication manager, who, in accordance with the default logic, verifies the called number in the call details to direct the call to the legitimate party. In this instance, the called number would be an extension that would direct the call to Unity Connection and trigger the call handler on it.
4. Call landed on the call handler of Unity Connection. We have set up the call handler's Caller Input so that if an outside user pushes 0, the call will be routed to an operator. Calls from Unity will be forwarded back to Unified Communication manager in accordance with the transfer rules set up in the Call Handler.
5. The Operator's extension number will be included in a redirect message that Communication Manager receives from Unity. The call will then be forwarded to the operator's IP phone via the communication manager.
6. Call reaches the operator's IP phone, rings a few times, and in the event that no one answers, is then again forwarded to Unity connection for voicemail.

Minimizing toll fraud at Unity Connection

Voicemail calls can be transferred to the PSTN using Cisco Unity Connection. This function can be used to commit toll fraud. Cisco Unity Connection comes with predefined restriction tables, that can be used to control the access to long distance phone numbers. [17]

Default Fax	Restricts numbers for fax delivery.
Default Outdial	Restricts numbers for message notifications. Also restricts the user extensions that Unity Connection dials when the phone is selected as the recording.
Default System Transfer	Restricts numbers that can be used for Caller system transfers, which allow unidentified callers to transfer to a number that they specify. For example, callers may want to dial a lobby or conference room phone that is not associated with a Unity Connection user. By default, the table does not allow Unity Connection to dial any numbers.
Default Transfer	Restricts numbers for call transfers.
User-Defined and Automatically-Added Alternate Extensions	Restricts the numbers the users can use to create alternate extensions for themselves through interfaces such as the Cisco Personal Communications Assistant or via an API call. Also restricts numbers from being offered as alternate extensions. For example, you might block a lobby or conference room extension so that users who frequently call Unity Connection from those shared phones are not automatically prompted to add the number as an alternate extension
Excluded Extensions for Automatically Added Alternate Extensions	Restricts numbers from being offered as alternate extensions. For example, you might add a lobby or conference room extension so that users who frequently call Unity Connection from those shared phones are not automatically prompted to add the number as an alternate extension.

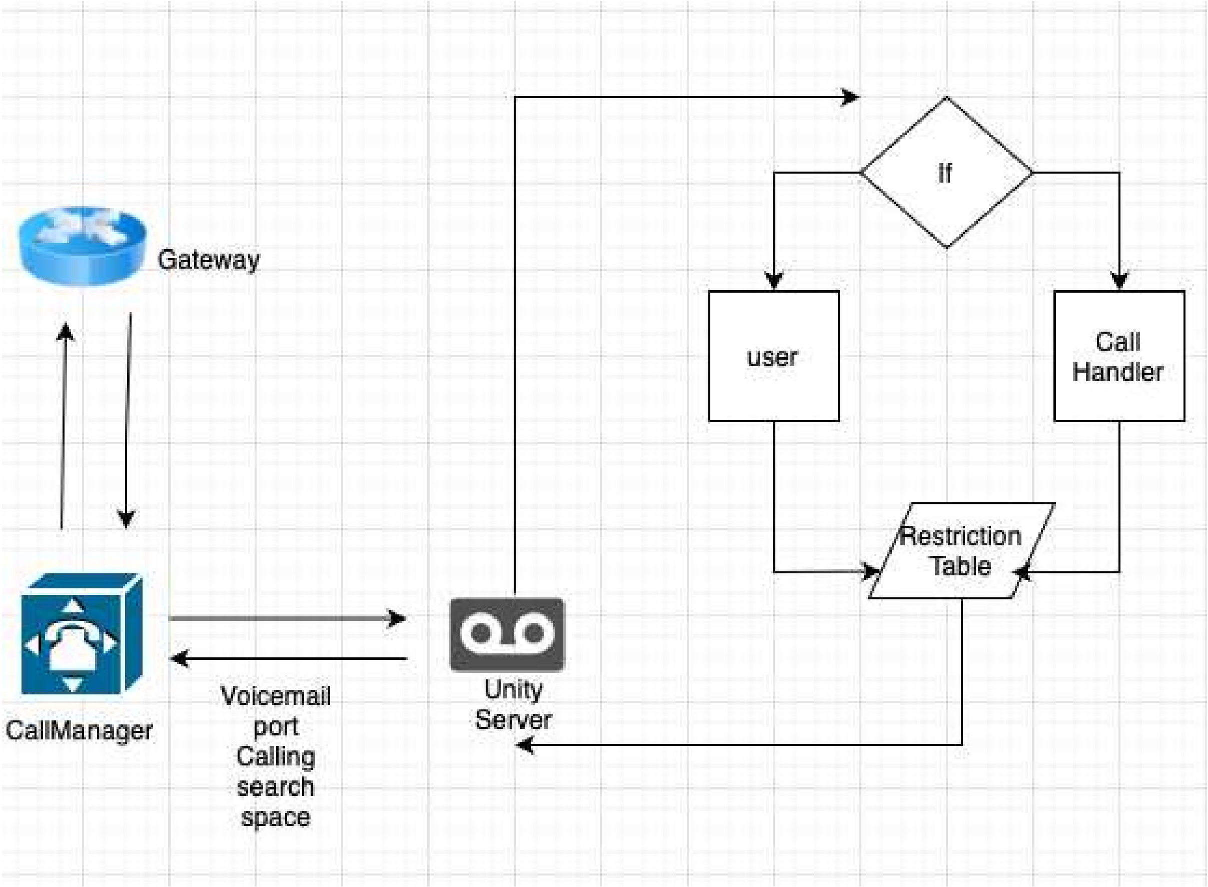
Restriction tables Transfer to alternate contact number:

After the number is defined by the user, it is not checked against the restriction table when the actual call transfer takes place. The check only happens when the number is defined by the user. Modifications to the Restriction Table in order to block the number defined by the user will still allow the call to be transferred as the number is already defined.

Call flow that we used in the lab:
The call originates from the PSTN and is transferred from the Communication Manager to the Unity Connection where a user or a Call Handler would answer it. Once the call is transferred from the user or call handler, the Restriction Table rules will filter it. If the call gets through this filter, it will next attempt to contact the Communication Manager via the Unity Connection voicemail port. This port is connected to the Calling search space, which acts as a second filter to determine whether or not the call can reach long distance numbers.

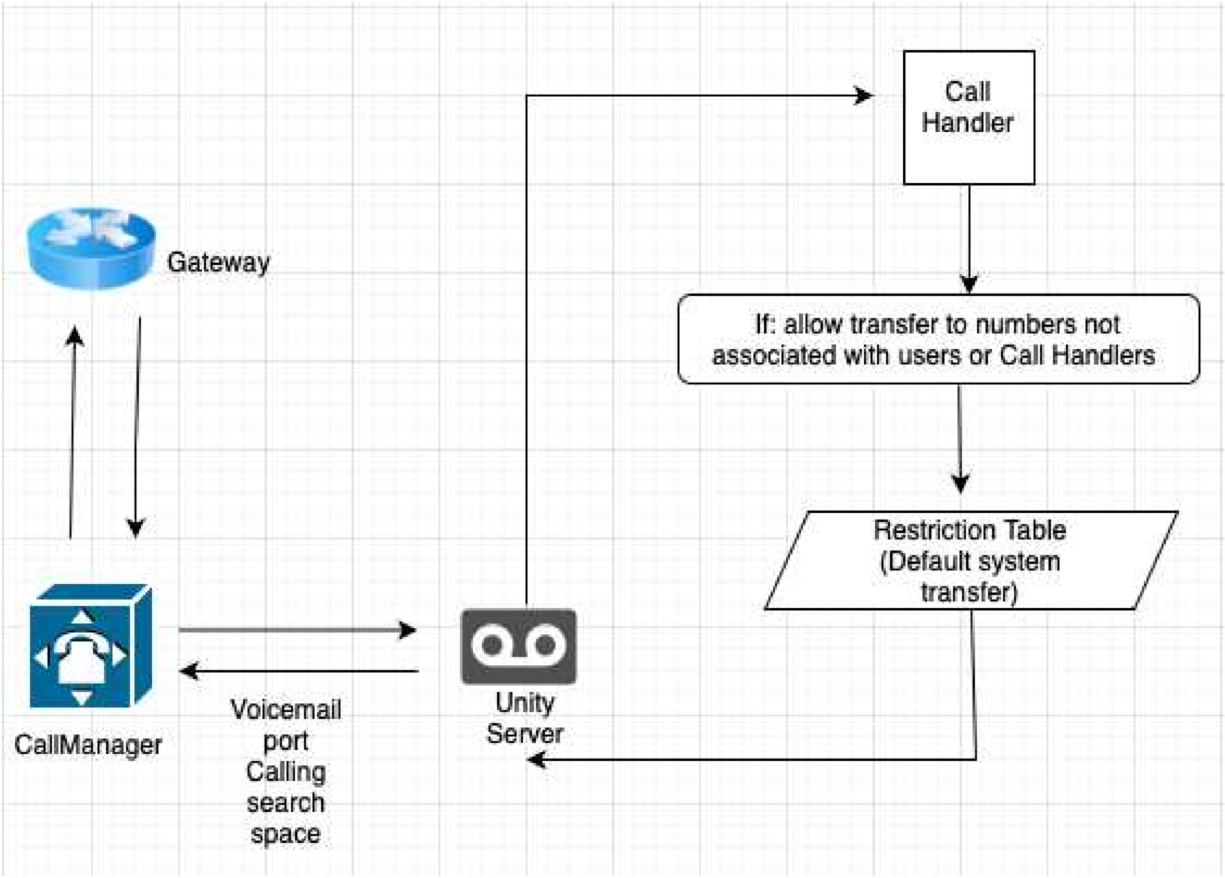
Call Manager Calling Search Space:

As the ultimate filter to stop calls from being phoned out even after the Unity Connection has already been bridged, it is crucial to be able to block long distance numbers for the Voicemail port calling search spaces.



Toll Fraud Scenarios Explained

1. **Call Handler Transfer to External number**

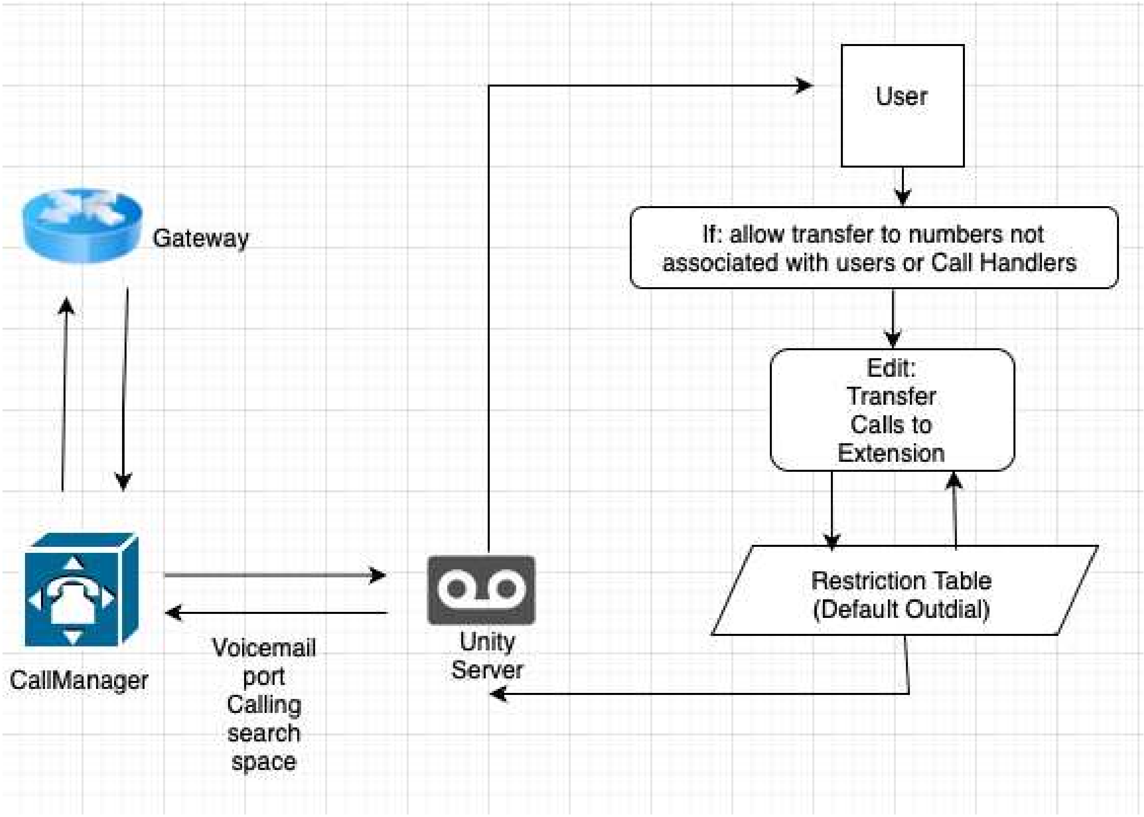

Call Handler
Gateway
If: allow transfer to numbers not associated with users or Call Handlers
Restriction Table (Default system transfer)
CallManager
Voicemail port Calling search space
Unity Server

The caller will be able to commit toll fraud in this situation by doing the following:

The company's main greeting is played when a call from the PSTN is received, and the caller is then instructed to dial the number they wish to be transferred to. In this scenario, if the Default System Transfer Restriction table does not specifically state to prohibit this long-distance number, the call will be transmitted.

Disabling the Call Handler greeting option "**Allow Transfers to Numbers Not Associated with Users or Call Handlers**" is yet another technique to stop this Toll Fraud using this method. Moreover, make sure this is unchecked for all the greeting choices accessible for that Call Handler.

2. Unity Connection user Transfer rule


User
If: allow transfer to numbers not associated with users or Call Handlers
Edit: Transfer Calls to Extension
Restriction Table (Default Outdial)
Gateway
CallManager
Voicemail port Calling search space
Unity Server

If a long-distance number already exists in the Extension field, the user can update that value and can continue to change it to accommodate new long-distance numbers.

In this instance, a user altering this voicemail user option.They have the choice to call from the TUI or use the Cisco PCA (personal Communicator assistant) to alter the transfer extension.Additionally, there are third party hacking servers that allow fraudsters to figure out user passwords and then they further log in via TUI from the PSTN and change the transfer numbers. Locking this long-distance number from the Default Outdial restriction table is advised to prevent this.

In addition, we can verify that no one has a long-distance number in the Transfer field and, if so, remove that number from that field.

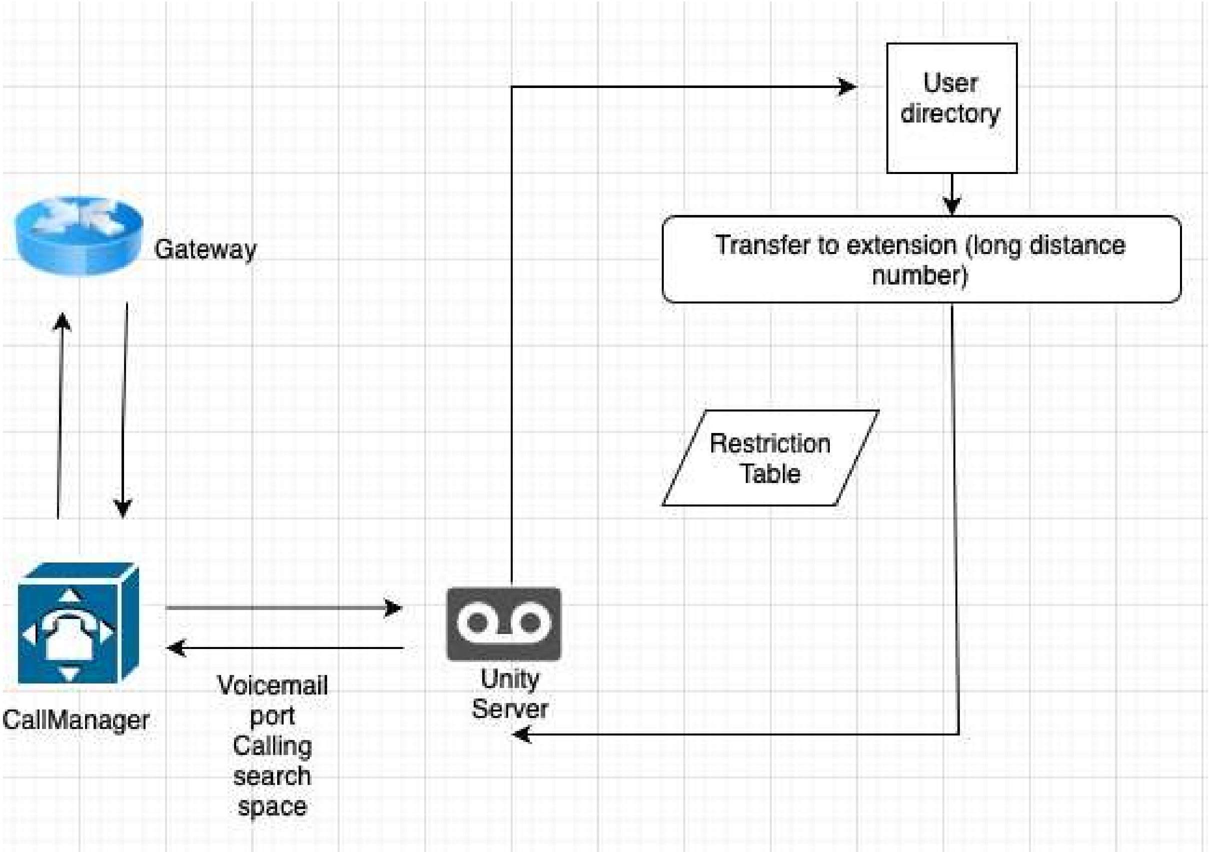
This CLI SQL query will list the user with alternated number:

```
run cuc dbquery unitydirdb select gu.alias, gu. dtmfaccessid, t.transferoptiontype,
t.extension from ww_globaluser as gu inner join ww_callhandler as ch on
ch.recipient_globaluserobjectid=gu.objectid inner join ww_transferoption as t on
ch.objectid=t.callhandlerobjectid and t.extension NOT in (select dtmfaccessid from
```

ww_globaluser where dimfaccessid != 'null') and textension NOT in (select dimfaccessid from ww_callhandler where dtmfaccessid != 'null')

Once this restriction table is configured to lock long distance number them user will not be able to edit their transfer to extension rule and add a long-distance number.

3. **Unity Connection user Transfer rule bridge**


User directory
Gateway
Transfer to extension (long distance number)
Restriction Table
CallManager
Voicemail port Calling search space
Unity Server

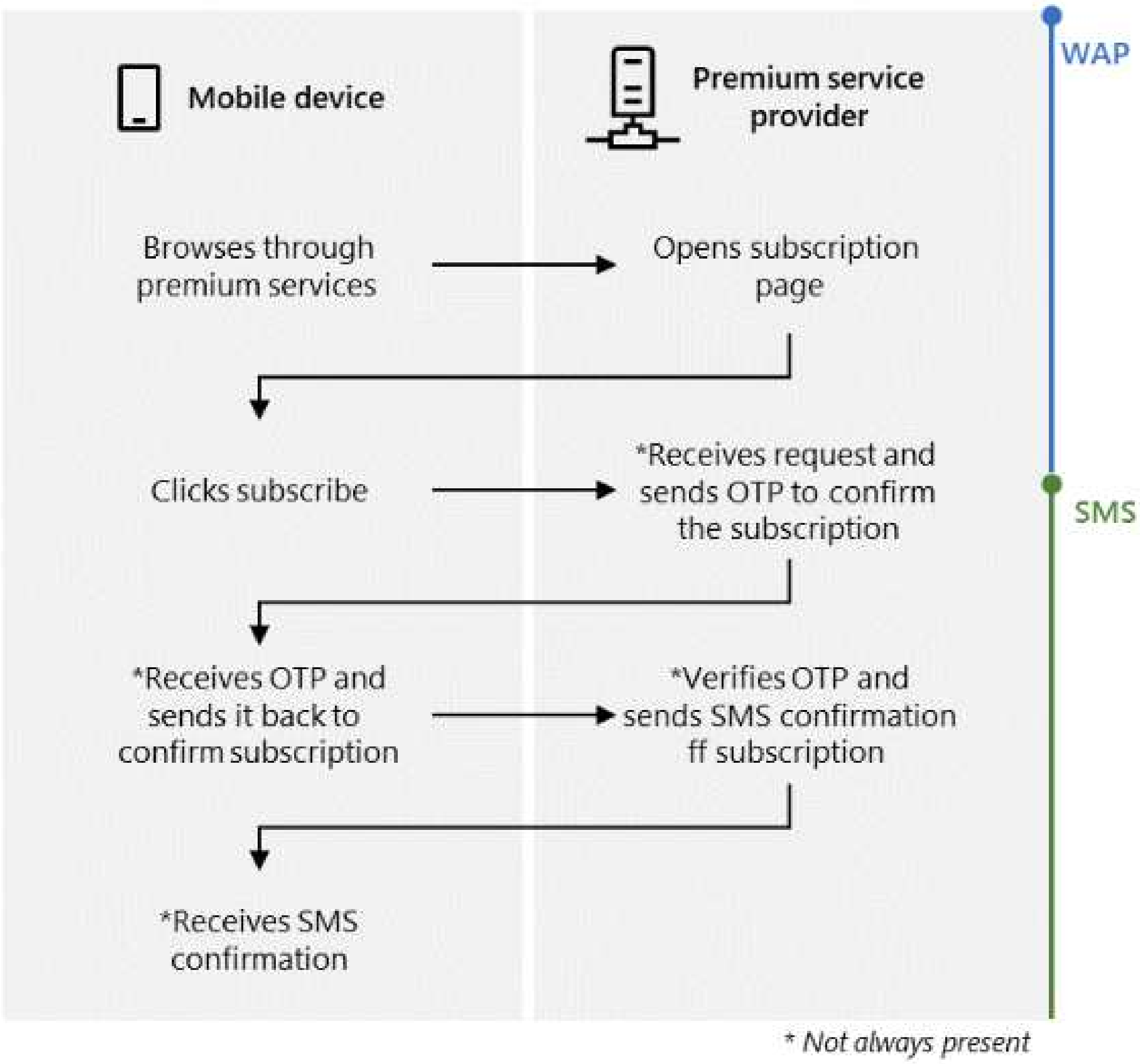
The long-distance number will not pass through any restriction tables if it is already defined in the Transfer calls to Extension.

In this case, the user transfer to extension, the field has already been defined with a long-distance number. The user is now reached by the called number and then dialed in to the directory handler and is further transferred to the long-distance number after having previously been bridged.

Toll Fraud Malware on Microsoft Teams for Android [18]

Carrying out toll fraud on an enterprise network is not the same as attempting to carry out toll fraud on a personal device like cell phone. Toll fraud has received attention since Joker, the first major malware family, was discovered in the Google Play Store in 2017. To further understand this malware on mobile devices, we must comprehend how the attackers utilize the billing mechanism.

Wireless Application Protocol (WAP) is the most common type of billing in toll fraud. WAP billing allows consumers to purchase content from Wireless Application Protocol (WAP) sites and have it charged to their mobile phone bill. It is a payment method other than debit or credit cards and premium SMS for billing. With WAP billing, consumers can purchase mobile content without having to register for a service or enter a username or password. The user clicks on a link and agrees to make a purchase before downloading content. [19]


Mobile device
Premium service provider
WAP
SMS
Browses through premium services
Opens subscription page
Clicks subscribe
*Receives request and sends OTP to confirm the subscription
*Receives OTP and sends it back to confirm subscription
*Verifies OTP and sends SMS confirmation ff subscription
*Receives SMS confirmation
* Not always present

Microsoft considers a subscription to be fraudulent if it is obtained without the user's consent. In the case of toll fraud, the malware performs the subscription on the user's behalf in such a way that the overall process is unnoticeable via the following steps:

a. Disable Wi-Fi or wait for the user to switch to a mobile network.
b. Without user intervention, navigating to the subscription page.
c. Subscription button should be clicked automatically.
d. Detect and trace the OTP, if required.

Before performing these steps, the malware performs a significant and permissionless inspection to identify the subscriber's country and mobile network using mobile country codes (MCC) and mobile network codes (MNC)

The following are some of Microsoft's recommendations for mitigating the threat of toll fraud malware for end users:

a. Install apps only from the Google Play Store or other reliable sources.
b. Allowing SMS permissions, notification listener access, or accessibility access to any application without a clear understanding of why the application requires is a bad idea.
c. To detect malicious applications on Android, use a solution such as Microsoft Defender for Endpoint.
d. If a device is no longer receiving updates, it is strongly recommended that it be replaced with a new device.

Microsoft has discovered that attackers frequently take the following steps to keep their apps in the Google Play Store:

1. Use open-source applications that fall into popular categories and are easily trojanized. Personalization (such as wallpaper and lock screen apps), beauty, editor, communication (such as messaging and chat apps), photography, and tools are the most popular application categories (like cleaner and fake antivirus apps).
2. Upload clean versions of the application until it receives enough installs.
3. Update the application so that malicious code is loaded dynamically.
4. Separate the malicious flow from the uploaded application for as long as possible to go undetected.

These applications share characteristics such as excessive use of permissions that are inappropriate for the application's usage, a suspicious developer profile, or a large number of negative reviews or complaints.

Conclusion

Since the invention of the telephone system, toll fraud has been one of the most common types of telephony attack. Every business, and even individuals, do not want to be surprised at the end of the month by an unusually high telephone bill. Voice over Internet Protocol (VOIP) PBX systems are susceptible to a variety of attack vectors, including:

1. Default passwords: If the PBX system's default passwords are not changed, attackers can easily gain access and make unauthorized calls.
2. Weak passwords: Passwords that are easy to guess or crack can expose the system to attack.

3. Toll fraud occurs when attackers use the PBX system to make unauthorized long-distance or international calls, causing significant financial losses to the organization.
4. DoS attacks: An attacker can flood the PBX system with traffic, causing it to crash or become unresponsive.
5. Malware can infect the PBX system and steal data, disrupt service, or gain unauthorized access.
6. Phishing attacks: Using social engineering techniques such as phishing emails or phone calls, attackers can trick users into disclosing sensitive information or downloading malware.
7. Eavesdropping: Attackers can intercept and listen in on PBX system calls, potentially gaining access to sensitive information.
8. Attackers can intercept and manipulate data sent through the PBX system, potentially altering call routing, or stealing sensitive information.

These fraud cost the global economy US$28.3 billion in 2019, accounting for 1.74% of global telecom revenues, according to the Communications Fraud Control Association (CFCA), and according to Google Play, the Joker malware accounted for 34.8% of installed Potentially Harmful Application (PHA) in the first quarter of 2022, ranking second only to spyware [20].

To secure VOIP PBX-based systems, change system passwords on a regular basis, enable mandatory password ageing and logoff notifications, and manage the password-resetting process. To prevent unauthorized system access, use authorization codes, and restrict external callers from pressing unexpected digit combinations or dial tones on auto attendants. Limit access to making international calls or to specific locations based on business needs. To increase awareness and appropriate responses, monitor system activity and traffic for unusual patterns, review Call Detail Reports (CDR) daily, and educate system users about toll fraud.

Businesses can reduce the occurrence of toll fraud on every device that participates in the call flow. They can use partitions, calling search space, time-of-day routing, client matter codes, and forced authorization codes to prevent toll fraud in their Unified Communications Manager. Access to specific routes and destinations can be controlled by partitions, whereas calling search space restricts access to authorized users or devices. Businesses can use time-of-day routing to restrict calls to specific destinations based on the time of day, and CMC and FAC require users to enter a code to make certain types of calls or calls to specific destinations. Cisco IOS voice gateways running IOS 15.1(2)T and above have a toll-fraud protection program that adds destination IP addresses to the trusted source list. This default feature was not present in earlier versions, which accepted call setups from all sources, treating any source IP address as genuine and trusted for call setup as long as voice services were active hence it is always recommended to upgrade your devices to latest and stable versions. Finally, in order to limit toll fraud on Unity Connection, a series of measures aimed at preventing unauthorised access and monitoring system activity must be implemented. These measures include assigning specific user groups to Automated Attendant and Call Handler menu options, using authentication rules to prevent unauthorised access, configuring voice recognition to verify user identities and limit access to specific features based on their roles, and monitoring system activity. Businesses can reduce the risk of unauthorized calls and toll fraud on their systems by implementing these features.

The aim of this capstone project is to present a comprehensive analysis of the different aspects of toll fraud. It proposes that toll fraud can be effectively mitigated by implementing appropriate policies, monitoring the system on a regular basis, and educating end users. The project explains in detail what toll fraud is, the potential risks it poses to an organization, and explores various scenarios that demonstrate how toll fraud can be perpetrated. The project also outlines strategies and best practices that administrators and end users can use to prevent toll fraud.

References

[1] A. Froehlich, CCNA Voice Study Guide IIUC Exam 640-460, Wiley Publishing, Inc..

[2] C. C. Expert, “Signal Attenuation and Noise,” 1 September 2022. [Online]. Available: https://www.ccexpert.us/telecommunications/signal-attenuation-and-noise.html.

[3] Diffen.com, “Analog vs. Digital,” [Online]. Available: https://www.diffen.com/difference/Analog_vs_Digital.

[4] J. C. M. Valentine, CCNA Voice 640-461 Official Certification Guide.

[5] vhadmin, “The Traditional PBX Is Dying,” December 2017. [Online]. Available: https://www.crescentcx.com/the-traditional-pbx-is-dying/.

[6] IETF, “RFC 3261: SIP: Session Initiation Protocol,” June 2002. [Online]. Available: https://www.ietf.org/rfc/rfc3261.txt.

[7] M. a. Baqari, “H323 Call Flow,” Cisco, 03 12 2019. [Online]. Available: https://community.cisco.com/t5/collaboration-knowledge-base/h323-call-flow/ta-p/3160014.

[8] C. Gibson, “Toll fraud, international revenue share fraud and more: How criminals monetise hacked cell phones and IoT devices for telecom fraud,” [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/cytel_fraud_intelligence_notification.pdf.

[9] Avaya, “Preventing toll fraud,” Avaya, 05 December 2016. [Online]. Available: https://documentation.avaya.com/en-US/bundle/AdministeringAvayaAuraCM_R8.1/page/Preventingtollfraudtop15tipstohelp.html.

[10] Cisco, “CCIE Collaboration Quick Reference: Cisco Unified Communications Security,” Cisco, 2 July 2014. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2218297&seqNum=10.

[11] Cisco, “Cisco Unified Communications Manager Express System Administrator Guide,” Cisco, 28 August 2022. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmetoll.html#id_87011.

[12] S. Holl, “Understanding Toll Fraud Enhancements in 15.1(2)T,” 03 December 2019. [Online]. Available: https://community.cisco.com/t5/collaboration-knowledge-base/understanding-toll-fraud-enhancements-in-15-1-2-t/ta-p/3123167.

[13] Cisco, “Configuring Class of Restrictions (COR),” Cisco, 31 October 2007. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/42720-configuring-cor.html.

[14] Cisco, “Call Handler Settings,” Cisco, [Online]. Available: https://www.cisco.com/en/US/docs/voice_ip_comm/unity/3x/administration/guide/313/SAG_0200.html.

[15] Cisco, “System Administration Guide for Cisco Unity Connection Release 10.x,” Cisco, 3 April 2019. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx/10xcucsag080.html.

[16] Cisco, “Troubleshoot Toll Fraud via Unity Connection,” Cisco, 1 September 2015. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/119337-technote-cuc-00.html.

[17] Cisco, “Managing Restriction Tables,” Cisco, [Online]. Available: https://www.cisco.com/en/US/docs/voice_ip_comm/connection/1x/administration/guide/acm080.html.

[18] M. 3. D. R. Team, “Toll fraud malware: How an Android application can drain your wallet,” Microsoft, 30 June 2022. [Online]. Available:

https://www.microsoft.com/en-us/security/blog/2022/06/30/toll-fraud-malware-how-an-android-application-can-drain-your-wallet/.

[19] Wikipedia, “WAP billing,” [Online]. Available: https://en.wikipedia.org/wiki/WAP_billing.

[20] Google, “Android ecosystem security,” Google, [Online]. Available: https://transparencyreport.google.com/android-security/store-app-safety.