Kadri Luhasalu

Fighting against VoIP Frauds, Using Proactive Network Scanning

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Degree Programme

Thesis

7 April 2014

Abstract

Author(s) Title Number of Pages Date	Kadri Luhasalu Fighting against VoIP Frauds, Using Proactive Network Scanning 38 pages 7 April 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialization option	Data Networks
Instructor(s)	Janne Salonen, Principal Lecturer Aivo Koger, Information Security Expert at Elion Enterprises Ltd.

The aim of this study was to examine proactive network scanning as a solution to the most general VoIP frauds in an enterprise environment. This study was assigned by Elion Enterprises Ltd.

The study examined the VoIP network in detail – the components, protocols and how they work, in order to understand the vulnerabilities that are exploited during VoIP frauds. The most popular and most damaging frauds were listed and explained.

From there, the study focused on the first steps in attacking and protecting the VoIP network – footprinting, scanning and enumerating.

In the last part of the study, the scanning was tested on a real Elion Enterprises Ltd. network segments. The results were analyzed – many open ports were found and gained access to, which means the system can be attacked very easily. The study recommended using proactive scanning against attacks and frauds as a basic intrusion prevention system, which can be build into a better system in the future as attacks become more advanced every day.

Keywords	VoIP, SIP, fraud, scanning

Contents

List of Abbreviations

ARP *Address Resolution Protocol*. Links network layer addresses into link layer addresses.

AS *Autonomous System*. Collection of connected IP routing prefixes under control of one or more network operators.

ATA *Analog telephony adapter*. A device used to connect analog phones to digital telephone system such as VoIP.

DID *Direct Inward Dialling*. Individual numbers provided by VoIP providers to their subscribers.

DISA *Direct Inward System Access*. Ability to access internal featured from an outside telephone line.

DNS *Domain Name System*. Hierarchical naming system for computers that translates domain names to numerical IP addresses.

DSL *Digital subscriber line*. Provides Internet access by transmitting digital data over the wires of a local telephone network.

FAQ *Frequently asked questions*. Listed questions and answers, all supposed to be commonly asked in some context.

GUI *Graphical user interface*. An user interface that allows users to interact with electronic devices though graphical icons and visual indicators.

HTML *Hypertext Markup Language*. Main markup language for creating web pages and other information that can be displayed in a web browser.

ICMP *Internet Control Message Protocol*. Used by network devices to send error messages indicating that a requested service is not available or host cannot be reached. Also used to relay query messages.

IP *Internet Protocol*. The main communications protocol that relays datagrams across network boundaries.

IP PBX *Internet Protocol Private branch exchange*. System that connects telephone extensions of a company to outside public telephone network and mobile networks.

ITSP *Internet telephony service provider*. Company that offers VoIP services to end-users or other ITSP.

IVR *Interactive voice response*. Allows a computer to interact with humans through the use of voice and DTMF tones input via keypad.

LAN *Local area network*. Computer network that user interconnects in a limited area.

MAC *Media access control address*. An unique identifier assigned to network interface for communications on the physical network segment.

OS *Operating system*. A collection of software that manages computer hardware resources and provides common services for computer programs.

PSTN *Public Switched Telephone Network*. Aggregate of the world's circuit-switched telephone networks that provide infrastructure and services for public telecommunication.

RIR *Regional Internet registry*. An organization that manages the allocation and registration of Internet number resources within a particular region of the world.

RTP *Real-time Transport Protocol*. Defines a standardized packet format for delivering auto and video over IP networks.

RTCP *RTP Control Protocol*. Provides out-of-band statistics and control information for an RTP flow.

SBC *Session border controller*. Device deployed in VoIP networks to exert control over the signalling and the media streams involved in setting up, conduction and tearing down telephone calls.

SIP *Session Initiation Protocol*. Signalling communications protocol used for controlling multimedia communication sessions such as voice and video calls over IP networks.

SNMP *Simple Network Management Protocol*. Internet-standard protocol for managing devices on IP networks.

TCP *Transmission Control Protocol*. Provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to LAN, intranet or the Internet.

TDM *Time-division multiplexing*. Method of transmitting and receiving independent signals over a common signal path.

TFTP *Trivial File Transfer Protocol*. Used for automated transfer of configuration or boot files between machines in local environment.

TOS *Terms of service*. Rules which one must agree to abide by in order to use a service.

TTL *Time to live*. A mechanism that limits the lifespan of data in computer or network to prevent a data packet from circulating indefinitely.

UDP *User Datagram Protocol*. Enables computers to send datagrams on an IP network without prior communications to set up special transmission channels or data paths.

VoIP *Voice over IP*. A methodology and group of technologies for the delivery of voice communications and multimedia sessions over IP networks.

1 Introduction

VoIP is now the most used technology for enabling people to communicate. It is used heavily by both service providers and consumers. It is a relatively new technology and with any new technology, the security has not yet reached a mature level and vulnerabilities are found constantly. Because of the number of VoIP vulnerabilities, telecom companies lose billions every year to frauds exploiting these vulnerabilities.

The subject was chosen with the help of the security expert in Elion Enterprises Ltd. After some network monitoring, it was realized how common VoIP frauds have became and how little protection there is against them. So the idea of developing a basic intrusion prevention system against the VoIP frauds, which involves proactive scanning of their VoIP devices was therefore chosen and approved.

As VoIP frauds exploit VoIP vulnerabilities, to understand VoIP vulnerabilities, firstly one has to understand VoIP systems. So the first part of this study is about VoIP in general - how it works and what components are needed. In the second part, some common VoIP frauds and their technical aspect are explored.

Then the start of an attack is explained, i.e the information gathering. This part was divided into footprinting, scanning and enumerating. In order to know how to defend against a hacker, one needs to understand how the hacking process works.

Finally the study gives the solutions against the attacks that lead to VoIP frauds and introduces a scanning technique in the company environment. A scanning tool and the scanning techniques discussed in the scanning part of the information gathering were implemented.

The aim of the study is to give a basic VoIP fraud prevention platform to the named company, which they can use to build it into a more elaborate and more efficient system in the future.

2 Understanding VoIP

Voice over IP or VoIP is a family of technologies that enables voice applications and telephony to be carried over an Internet Protocol (IP) network – Internet. These technologies include protocols, hardware and software standards and computer programs.

In the traditional telephone network (PSTN) circuit-switched connections are used, which means that when a call is made, a dedicated circuit is received from one telephone to the other. VoIP uses packet-switched environment, where multiple computer devices share a single data network. They communicate by sending packets of data to one another. The contents of these packets – payload – are snippets of the voice conversation.

For voice to take packet form, the audio portion of the call needs to be converted from analog to digital, cut into packets, sent across the network, reassembled and converted from digital back to analog. The conversion is done by encoders and decoders – codecs.

Placing a VoIP call on data network involves a call setup and a conversation. VoIP protocols are required during both phases:

- Call setup protocols such as H.323, SIP, SCCP, MGCP and Megaco/H.248. These setup and take down calls using IP protocols TCP and UDP.
- Voice streaming protocols such as RTP, RTCP and SCTP. After call is set up, exchange of encoded voice data occurs using two data flows, one in each direction, to let both participants speak at the same time.

The hardware and software requirements for VoIP are (1, p. 2-23):

- IP PBX
- VoIP gateway
- Softphones or hardphones

There are many ways these elements are connected in a VoIP network, one example is provided in Figure 1 (2, p. 1).

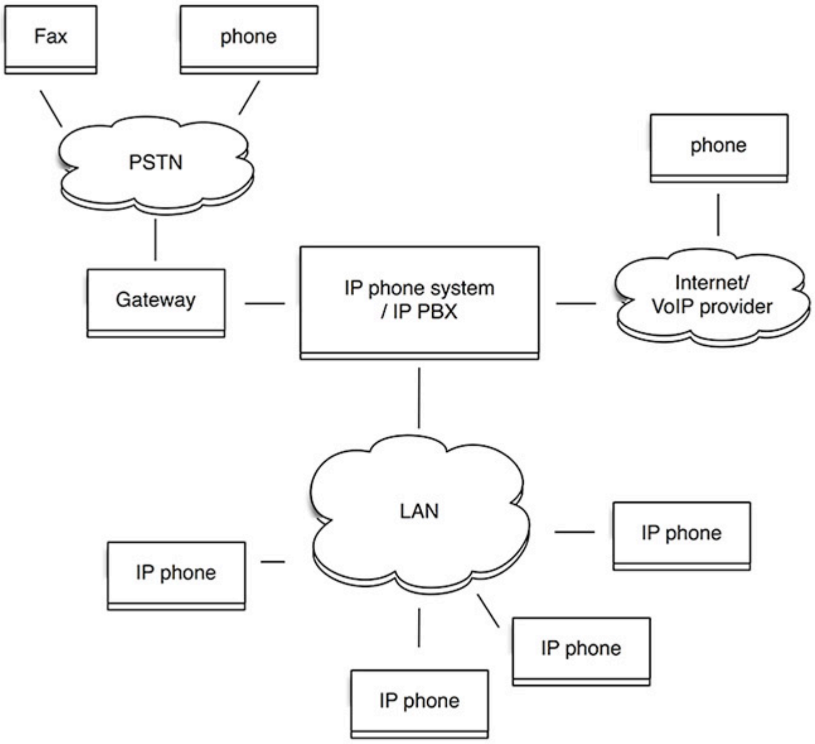


Figure 1. How VoIP works (2, p. 1).

In the old days, when all calls went over the PSTN, companies would buy trunks from their service provider. These trunks were usually called Time-Division Multiplexing (TDM) trunks. These were dedicated lines or bundles of circuits, which were needed to route calls outside the company's premises. These trunks would be between the gateway and PSTN network in Figure 1.

Nowadays most companies use SIP trunks. SIP trunking offers another way of connecting the company IP PBX to the PSNT without the need of dedicated lines and gateways. SIP trunks allow multiple signal types travel over the same pipeline. SIP trunking is supported by the IP PBX or PBX that has SIP enabled port. As SIP trunk is software and IP -based, it is much easier to manage remotely and therefore cheaper for the service provider (3, p. 1-2, 5-10).

VoIP is mainly used because it low costs to the companies. Even though implementation can be expensive, the overall cost savings in the future pay off. Instead of supporting two networks now only one network is supported, making the management and maintenance less expensive and easier. Cost savings also come from bypassing toll

charges also known as long distance charges and all the extra services that were charged in PSTN.
Another benefit of VoIP is its flexibility. VoIP can be used with a Smartphone, old analog phone or computer and are connected to the same PBX system anywhere in the world where there is Internet connection.

These are only some VoIP benefits, but as all things, there are also disadvantages, the biggest being weak security compared to the old PSTN (4, p. 7).

2.1 Protocols

Before a VoIP call can take place, signalling protocols ought to be employed to a certain session and to uphold and conclude the established session. Currently a dominant VoIP signalling protocol is the Session Initiation Protocol (SIP). Media stream protocols are also needed to carry the voice over IP networks. The most used media stream protocol is Real-Time Transport Protocol (RTP) alongside with Real-Time Control Protocol (RTCP).

2.1.1 SIP

SIP is an application layer session protocol used for establishing, manipulation and tearing down call sessions between one or more callers. SIP works with any system, operating system or infrastructure of the IP network and is used in VoIP, video conferencing, virtual reality and multiplayer games. It is preferred over other signalling protocols such as H.323, because it is ASCII- or text-based protocol, which makes it more lightweight and flexible, but also less secure.

SIP uses other protocols to provide basic functionality such as:

- Session Description protocol (SDP) which defines parameters for the media session.
- Real-time Transport Protocol (RTP), which transports the media.
- RTP Control Protocol (RTCP), which transmits control data for the RTP stream.

- Compressors/Decompressors (CODECS), which encode and compress the media.

A SIP Uniform Resource Indicator (URI) is how users are addressed in the SIP world:
Sip:user:password@host:port;uri-parameters?headers

SIP architecture consists of five core components:
User Agent (UA) – is any client application or device that initiates a SIP connection. A session is initiated by User Agent Client (UAC) sending a request with SIP to User Agent Server (UAS). Client application can be IP phone, a soft phone, Smartphone, Instant Messaging client, mobile device or it can even be a gateway that interacts with the PSTN.

Proxy server – is a server that receives SIP requests from various user agents and routes them to next hop. Usually there are at least two proxies. It can provide such functions as network access control, security, authentication and authorization.

Redirect server – directs incoming requests from other clients to contact an alternate set of URIs. It offloads processing load from proxy servers. It also has the ability to split the call to several locations, so that it rings at all of them at the same time.

Registrar server – server that registers the location of a user agent who has logged onto the network by obtaining the location info of the user (IP address, username, port etc.) and associates it with their username on the system. It creates a directory of all those who are currently logged onto the network and where they are located.

Location server – used by redirect server or proxy server to find the destination caller's possible location.

The SIP proxy, registrar and redirect servers are usually implemented on one system, usually the IP PBX.

SIP implements various request types to build a session:
INVITE – initiates a conversation.
BYE – terminates existing connection between two users in a session.
OPTIONS – obtains information on the capabilities (SIP messages and codecs used) of another user agent.

REGISTER – registers user agents SIP and IP address with Registrar server.
ACK – confirms a session.
NOTIFY – sends updates information on a user agent's current status – online, offline, busy etc.
REFER – transfers calls and contacts to external resources.
SUBSCRIBE – indicates the desire for future NOTIFY requests
CANCEL – cancels a pending INVITE request, but does not stop completed connections.
BYE – terminates a session.

SIP responses are used to answer SIP requests. They are three-digit codes, where first digit indicates the category of the response and other two digits indicating the action taken by the SIP device.

A typical SIP call flow with SIP requests and responses are seen in Figure 2. In this case SIP proxy is used, because SIP phone A does not the location of SIP phone B. If the location is known, servers are not asked (5, p. 58-61).

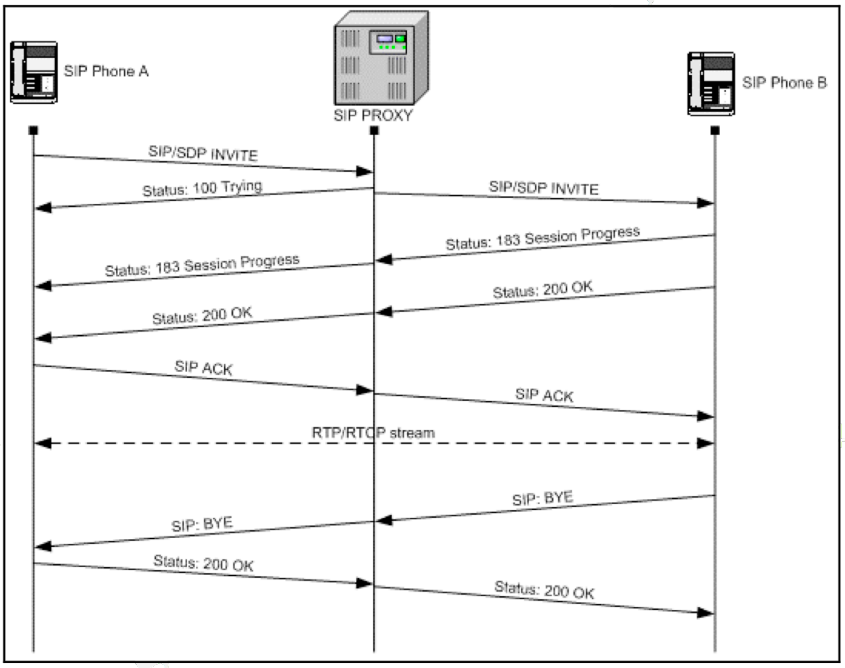


Figure 2. SIP call ladder (5, p. 61).

SIP is the protocol of choice when using VoIP, but it is difficult to secure. It was designed without serious security concerns in mind and more security flaws are emerging. VoIP networks do not have a closed communication, which makes communication medium vulnerable to all kind of attacks - attacks specific to VoIP as well as attacks specific to SIP.

2.1.2 RTP

The RTP is used virtually by every vendor to transport real-time data such as audio and video. It is a simple protocol, providing only payload type of identification, sequence numbering, time stamping and delivery monitoring in its header. These are used for reconstructing the original data, dealing with missing, duplicate or out-of-order datagrams. All fields in the header sip inside the UDP payload. RTP includes the RTCP, which is used to monitor the quality of service and give information about the participants in an ongoing session (1, p. 21).

For better security Secure RTP (SRTP) and Secure RTCP (SRTCP) can be used, which provide encryption and authentication (5, p. 47).

2.2 Devices

The basic components of VoIP systems include the core processing server – IP PBX, end-user devices such as hardphones or softphones and a gateway for translation between different technologies. Often Session Border Controllers (SBC) are listed as VoIP components, which provide real-time, session-based traffic control at the signalling (call control) and transport layers (media control), but they are not needed to make the VoIP system work.

2.2.1 IP PBX

Adding voice data to IP networks, which is based on the client/server model of computing, means adding another set of servers that provide voice services. An IP PBX is the VoIP core server, often called call processing server. It provides similar functions as the traditional PBX of the PSTN. VoIP clients register with the IP PBX server and when they wish to make a call, they ask the IP PBX to establish the connection. IP PBX has a directory of all phones/users and their addresses and connects an internal call or route an external call via VoIP gateway or VoIP service provider to desired destination.

IP PBX can be a hardware object or software system, but typically software-based such as Asterisk. Organizations deploy IP PBXs as single server, cluster of servers or server farm with distributed functionality (1, p. 23-25).

2.2.2 VoIP Gateway

VoIP gateways are devices that translate between protocols and provide translation between incompatible interfaces. Usually they provide a connection between the VoIP network and the PSTN. Even though networks that have only VoIP phones are growing, there are still PSTN users, which makes it necessary to connect them to make call to each other. Gateways are usually capable of supporting a large numbers of different protocols to handle the variety of signalling and data protocols that are needed to communicate between the VoIP network and the PSTN (1, p. 25-26).

Analog telephony adapter (ATA) can be used to connect analog telephones to VoIP networks. This is a simple home-user implementation of VoIP gateway. It has a phone interface (analog or digital) connected to a phone and Ethernet interface connected to the Internet (4, p. 75).

2.2.3 Hardphones and Softphones

End users can initiate and receive VoIP calls using variety of VoIP phones and consoles. VoIP phones can be either hardware-based devices – hardphones or software-based devices – softphones.

Hardphones, also known as IP phones are digital phones that make data connections to IP PBX with Ethernet LAN connection using patch cable or wireless link. They have an IP address just like a computer.

Softphones are computers that have software programs installed that permit telephone-style communication. They appear on Windows, Linux or Mac desktop as graphical user interfaces (GUI) that often resemble a telephone and require a microphone and speakers. Softphones are primarily targeted to mobile users, who use them to connect to the company's network over a secure connection, which makes it possible to receive and make calls through the company's IP PBX (1, p. 26-27).

2.3 Services

VoIP service is the service from a company that allows making and receiving VoIP calls. These companies are called VoIP service providers or Internet telephony service providers (ITSP). This can be free or paid service. Depending on the needs, there are different types of VoIP services:

- Home phone replacement residential services

In this case analog phones are used. An ATA is sent to the subscriber, which is plugged to the analog phone and other side to DSL line. Service is paid monthly. Most common residential VoIP service providers in Europe are 1VOC, iTalkWorld and Svanto.net.

- No-monthly-bill services

  A subscriber buys a special hardware to make unlimited calls. The devices can be hubs and a scouts, modified ATAs or jacks. The scout is the device that is connected to a traditional phone set, as these are usually used in this case. A jack is a small and handy device that is plugged into the computer with USB plug. Three device-based VoIP providers are Phonegnome, ooma and MagicJack (6, p.1).

- Software-based services

  A VoIP application is installed on your computer and registered with the service. The application (softphone) is used to make and receive calls. Calls are free for the people using the same service, calls to analog and mobile phones cost. These applications are usually offered for free with the VoIP service. For example Skype is a software-based service.

- Mobile VoIP services

  These are software-based services for mobile phones, tablets and other portable devices. The set up is the same – installing a VoIP application with the service. Mobile phones or tablets need to be connected to the Internet thought Wi-Fi or other means. Most common mobile VoIP services are Skype, Fring, Yahoo, GoogleTalk, Viber, Yeigo etc.

- VoIP services for business

These are based around internal networks and IP PBXs. They offer many business-related features and outsourcing for the VoIP system's management and hosting. VoIP service providers for businesses vary depending on the region, for example in northern Europe most common VoIP business providers are 1Pipe Telecom, 1VOC and CallForwarding.

In order to use VoIP, one has to choose suitable service provider and register with it just like one registers with the Internet service provider or the phone service one gets from a PSTN line telecom (7, p. 1; 8, p. 1).

3 Fraud Types

Voice network security has been an issue in companies for years, but because of the recent proliferation of VoIP in both the service provider and company networks, the threats have increased. In addition to packet vulnerabilities, VoIP has its own vulnerabilities coming from new protocols and network components: SIP and SIP trunks, softphones, Smartphones, IP PBXs etc. Products are released to the market without well thought-out security. In addition VoIP does not have a dominant standard and dozens of proprietary protocols make the matter worse. Therefore attacking a VoIP network is fairly easy.

When a hacker targets a voice network, they can have many motives. It may be to disrupt operations, threaten a business to extort money, harass individuals, steal or trick users into giving up personal information, sell merchandise or services, listen to conversations to get valuable information or steal money, to name a few. The focus in this study is the issue that most companies and businesses face and want to eliminate – VoIP fraud.

VoIP fraud is exploiting voice network vulnerabilities for making money. The 2011 global fraud loss estimate is over 29 million Euros. Approximately 1,88 % of telecom revenues were lost (9, p. 112-114).

There are very many VoIP frauds; the top fraud methods reported in 2013 by the Communications Fraud Control Association (CFCA) were PBX hacking and subscription fraud (10, p. 4).

3.1 Toll Fraud

Toll fraud is the largest threat affecting most companies and no company is immune. The smaller companies are especially at risk, as they do not have the necessary time and expertise to secure their VoIP systems.

Toll fraud ranges from minor abuse by employees by inflating company usage bills to organized toll fraud, where hackers make money by selling and abusing the long-distance capabilities of companies.

Toll fraud is popular because it is very profitable. Profits like 100 000 Euros are not uncommon. Another incentive is that toll fraud is not always detected until large amounts of money have been lost (9, p. 112-114).

There are three areas within a company VoIP deployment that are most vulnerable to toll fraud:

- PBX/Voicemail/Application Servers

These are susceptible to security breaches due to their often weak or no password protection. Also policy enforcement on these systems is limited – they allow redirects, transfers and forwards to long distance, international toll or premium-rate numbers without good authorization.

- PSTN connectivity

Sometimes service providers employ weak authentication on SIP trunks, which makes it easy to bypass SBCs and media gateways.

- User/Device authentication

Companies that deploy phones over extended networks or low security networks such as Internet, are vulnerable to exploitation, because these phones can be lost, stolen or gained access to by guessing or “brute forcing” weak credentials. Then hackers are ready to make calls as the authorized user or exploit the user identity associated with the credentials (11, p. 2).

There are many types of toll frauds, such as internal toll fraud, dial-through fraud and international revenue sharing fraud. They all share a common trait – they usually exploit IP PBXs by entailing calls dialled out of the company PBX to expensive destinations. This is why most toll frauds are called PBX frauds (9, p. 112-113).

3.1.1 Internal Abuse of Phones

Internal long distance abuse occurs when company staff abuse fax lines for voice and unrestricted phones or use services they are not entitled to. This abuse seems minor, but it still costs company money and if unnoticed, it can add up over time into a large sum.

Many fax machines in companies have minimal or no calling restrictions. Some fax machines bypass the IP PBX completely, which means no calling records are saved by the IP PBX, so if someone does not pay close attention to phone bill, this abuse may not be noticed.

For this fraud all that is needed is to disconnect the analog line from the fax machine and plug it to any analog phone and you have a dial tone within a second or two. Once this has happened, you can call anywhere as long as you want. Even if the fax machine does go through the IP PBX, there probably are no limits on the destination number or duration of the call. IP PBX does not differentiate fax from voice, so they will not be able to detect a voice call over fax.

Company phones might have some restrictions, but some phones can be found which do not – executive phones, sales phones, telemarketer phones for example do need to make long distance calls, so they are not usually restricted (9, p. 114-116).

3.1.2 Dial-Through Fraud

This is a two-leg attack, often called “hairpinning” of the call. It relies on calls that have two legs – the incoming call dialled into the IP PBX from outside, and an associated outgoing call dialled out into the PSTN at the expense of the company. The manual or automated inbound call is hair-pinned outbound to the international number. Now expensive international calls can be made (12, p. 3).

The service that is typically abused in this scenario is Direct Inward System Access (DISA). DISA is a dial-through feature on Cisco Unified Communications Manager (CUCM), which is Cisco equivalent to IP PBX that allows an external user to make an inbound call and gain access to VoIP services – IP PBX, mailbox, voicemail or outbound dial tone. Access to these services is usually protected with a password, but these are often very weak and not changed very often. Hackers can identify the service and password through automated testing, social engineering or an insider. When access is found, passwords are provided to hackers, who abuse the company service.

Because DISA is not enabled by default on the CUCM, to be able to launch a dial-through fraud is to enable DISA on the IP PBX. This means hackers will have to compromise the IP PBX by logging in and gaining administrative access (9, p. 120-122).

Dial-through fraud can be made both on the TDM trunk and the SIP trunk. The available attack surface is larger if you use SIP trunking in your company, because SIP has many vulnerabilities and configuration weaknesses on its endpoint. Hacker can exploit the SIP trunk endpoint with open source software tools such as SipVicious, cause the IP PBX to accept incoming calls from a rouge SIP endpoint and forward calls to expensive destinations (12, p. 4).

The motive for a dial-through fraud can be the reselling of low-cost long distance and international calls on the streets. Calls are made by disposable cell phones to mask the call origin and receive cash from the users on the street, making calls very difficult to trace. Another motive for dial-through fraud is to launch International Revenue Sharing Fraud, which is the most common motive (9, p. 120-122).

3.1.3 International Revenue Sharing Fraud and Premium Rate Services

International revenue sharing fraud, shortly IRSF, is the most damaging and the most common VoIP fraud scenarios. According to CFCA, IRSF accounts for almost 4 billion Euros in losses a year.

IRSF abuse carrier interconnect agreements. The hacker partners with a local carrier that charges high rates for call termination and agreement to share revenue for any traffic generated by the hacker. The international carrier that delivers the last mile is obliged for paying the final destination Telco. Common destinations are the West African countries, UK mobile numbers and satellite phones.

A typical scenario is that the hacker first obtains the Premium Rate Numbers (PRN). These PRNs allow callers to access some form on value added information or entertainment service. Callers to the PRNs are charged much higher rate than normal traffic and generate profit for both International Revenue Share Provider (IRSP) and content supplier. The revenue share from PRNs varies by country, but can range between 30%-80% above the net tariff.

After acquiring a PRN from an IRSP, the IP PBX is compromised, automated inbound call generator is used to create the company calls to PRNs. The revenue is shared with the service provider, international carrier and the third party - the hacker (13, p. 2).

There are many forms of IRSF such as voice mail hacking, call forwarding and blind call transfers.

Voice Mail hacking was an early form of communication fraud. The hacker just needs to find a end-user device with an easy to break password. After the password is guessed, they exploit the “Call Back” feature, which allows a user to immediately return a missed call. The hacker calls the phone number, leaving the IRSF number as the “call back” number. When a user logins to their account, they return the missed call to the IRSF number. Once the call is connected, hacker can attempt to leave it up as long as possible, often hours or days.

A call forwarding and blind call transfers are more sophisticated attack that involves hacking into the IP PBX. In call forwarding attack after the hacker have guessed the users password in the IP PBX, they login to the IP PBX, configure call forwarding to an expensive long distance destination to profit from IRSF. Then the hacker will call the telephone number over either the PSTN or VoIP of the hacked account, which forwards the call for IRSF. And example of call forwarding attack is provided in Figure 3.

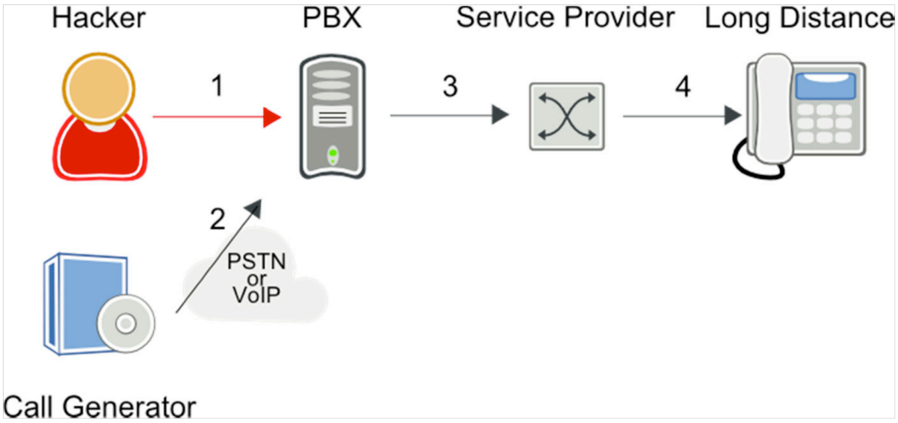


Figure 3. Call forwarding attack (14, p. 5).

The Blind Call Transfers are for doubling IRSF while making the fraud more difficult to detect. In this case, the hacker hacks to the IP PBX again to make international calls. The IP PBX sends SIP INVITE to service providers switch, the switch routes the call to international number for IRSF. Then the hacker instructs the IP PBX to blind transfer the call to another international number for IRSF and then hangs up. The call between the two international destinations remains in place. The call stays up until the carrier shuts it down. This is called double IRFS with one phone call (14, p. 3-7). A blind call transfer is shown in Figure 4.

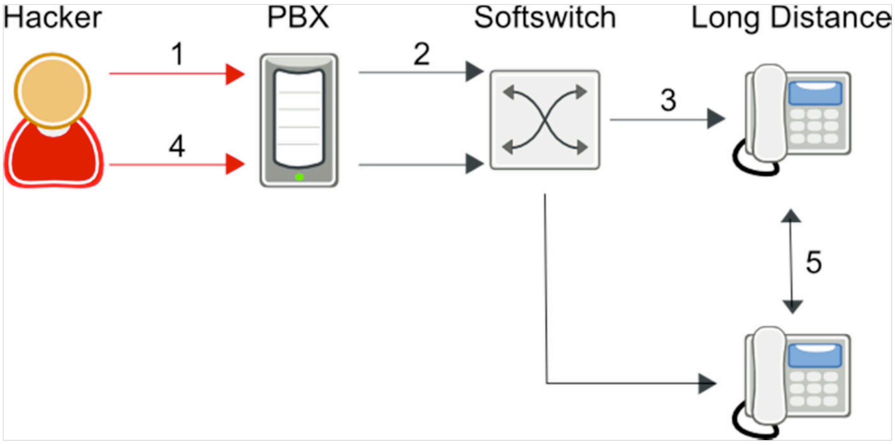


Figure 4. Blind call transfers (14, p. 7).

In all of these scenarios, call generation is mentioned. There are several call generation tools available for this written in C, Python, Java and shell script. If the IP PBX uses Asterisk, one solution is to use Asterisk call files. They are structured files, which can be used to automatically place calls if moved to the appropriate directory. This solution is one of the simpler ones and requires very little technical knowledge (15, p. 1).

3.2 Subscription Fraud

Subscription fraud is the signing up for a service using false or stolen identification with no intention of paying the bill. The fraudster can set up multiple accounts or causing multiple subscribers to be billed for the used services. This might generate big losses to the operators. This fraud is detected at some point though the billing process.

This kind of fraud is usually used for call selling or intensive self-usage. In case of call selling, it can be done in many ways. For example, the call can be sold by renting the phone for fixed sum or by setting up a shop where customers can use it as a payphone.

Subscriber fraud commonly occurs with cell phones and is the most common forms of telephone frauds – it accounts for 47% of funds lost due to telephone fraud (16, p. 1).

4 Attack and Defence

Before any attack can take place against a company, hackers need to go through three phases: footprinting, scanning and enumeration. These can be summed up as the collection of information about the target, ranging from simple website checking to a small attack to gain more precise info.

These are the steps security experts also have to go through to secure their networks – in order to know how to secure a system, it is necessary to know the vulnerabilities. So this is called attack and defence for that reason. This study focuses on the external point of view, as the inside abuse is reducing.

4.1 Footprinting

Footprinting is also called profiling or initial information gathering. It is the first step in hacking any network or system. The aim of footprinting is to gather information about the infrastructure of a target network only from information which access is free and authorized. The information gathered is for example IP addresses, network address ranges, subdomain names, administrative contacts, technical contacts, physical location, remote access capabilities etc. With this the hacker makes a unique profile – a footprint - about the target, analyzes it and then picks the most appropriate methods and tools to hack into the system or network. This speeds up the whole hacking process and increases the chance of success.

Everyone can have access to information by spending little time and effort. Some valuable information is publicly accessible for anyone, anytime and anywhere and it can’t be protected. So to assess a company’s external security posture, the first thing is to find out what information potential hacker may already know about you. This can be done with open-source search, search engines or WHOIS (9, p. 20; 17, p. 1-3).

4.1.1 Open-Source Search

The initial information that can be gathered is with open-source search, meaning public website search. The information found with this search is often believed to be harmful, because its main purpose is to help promote, educate and market to external visitors. Therefore it is also easily obtainable and does not result in legal implications.

Visiting the company’s website and browsing through the pages of the site can uncover the platform which the web server is currently running on, the web servers software or the scripting language used if the site is serving dynamic pages. The hacker can view HTML source code of the pages to seek hidden comments or directory structure. There are also offline-browsing utilities such as Teleport Pro, HTTrack, Wget, Quicky Browser to download and mirror the entire site as well as directory structures for offline viewing and auditing (17, p. 6-9).

After viewing the technical side of the website, the hacker can focus on the informational side. The starting points for hacker to launch and attack can be:

- Organizational structure and company locations
- Help and tech support
- Job listings

Most companies and universities provide contact information for everyone in the Office of the President. Getting the names of high-ranking people in an organization may prove helpful in guessing usernames or social engineering for other information.

In addition to the company's own website information, there are other websites that specifically provide information about a website, such as Hoover's Online. They provide the company's location, address, phone numbers, website and customer information. Getting employees names and emails gives lots of opportunities for attacks. For example, combining an employee name with a little social engineering, the hacker can call the help desk, pretend he works there and password be reset or changed.

With emails additional information about the company's email server can be gained by sending a non-existent email address to the email server. It will bounce back to the hacker and give him information in its header – email server address and version (18, p. 95).

News and periodical articles can be also useful and can include partnerships, major organizational purchases and other information what is happening in the company. Websites such as Google News, Dogpile and Business Journal Tracker can provide articles about a certain company.

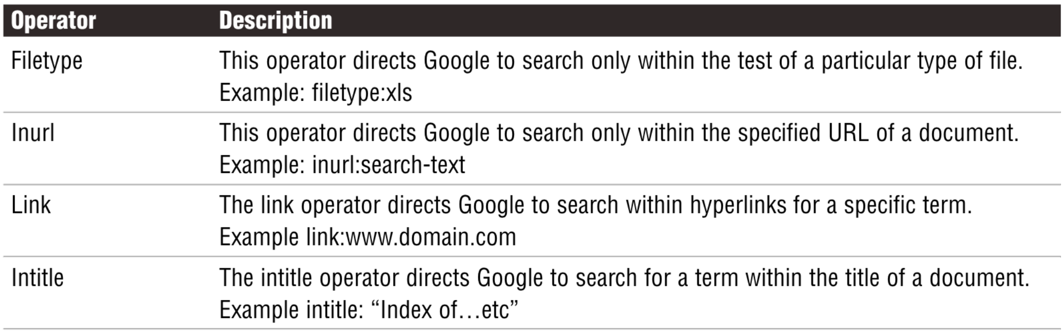
Location information attained from the website is useful in understanding the flow of traffic between VoIP call participants and finding locations to get within range of an office building to attack the VoIP traffic going over wireless networks.

Some larger companies offer an online knowledgebase or FAQ for their users. These can contain very valuable information such as phone types, default PIN numbers for voicemail and remotely accessible links to web administration. This information can be cross-referenced against several free online vulnerability databases to find any security holes.

Job listings on company networks contain information about the technologies used within the company. The hacker just has to look for the needed qualifications. For example, the target operating system and environment, how emails are managed, what database servers are used can be obtained. From this information it can be guess what ports the company is using and later scan them.

4.1.2 Search Engines

Search engines are the hacker's most popular tools. A hacker can simply utilize the advanced features offered by a service such as Google, Yahoo!, Bing, Ask and returned results can show a lot of potential information related to the target – abandoned web sites, past events, target's partner, press releases and case studies, related articles etc. With the use of Boolean expressions, they can collect even more sensitive information such as web-based VoIP logins seen in Figure 5 (17, p. 8).



Operator	Description
Filetype	This operator directs Google to search only within the test of a particular type of file. Example: filetype:xls
Inurl	This operator directs Google to search only within the specified URL of a document. Example: inurl:search-text
Link	The link operator directs Google to search within hyperlinks for a specific term. Example link:www.domain.com
Intitle	The intitle operator directs Google to search for a term within the title of a document. Example intitle: "Index of…etc"

Figure 5. Typical Boolean expressions for search (18, p. 11).

For VoIP attacks and frauds, finding out internal phone numbers and extensions is very helpful. Finding these numbers requires just a search. For example, to find a customer service number form a specific site, you just have to type this to a search engine:

customer service site:www.site.com

With this one can also find one- or two-number prefixes that is unique to that site, fax numbers, DID numbers etc. Direct inward dialing (DID) numbers are numbers VoIP providers provide to their subscribers. DID is not required for outbound calls, it is only needed to allow PSTN users to directly reach users with VoIP phones. DID numbers are assigned to gateways. DID is used with SIP trunks, as it is SIP trunking feature.

Once the hacker has obtained a specific number, he can try calling them after normal working hours to hear the factory default main greeting, hold music or voicemail message. Simply by listening to the recording can help the hacker to narrow down the system running. Recorded transcripts and messages can be found on several websites and the system that uses them (9, p. 22-31).

Most VoIP devices provide web interfaces for administrative management and for users to modify their personal settings such as voicemail, PIN and forwarding options. These sites should not be exposed to the Internet in order to prevent brute-force attacks. Searching these web pages is easy with for example with Google. To find CUCM installations exposed to the Internet, simply type:

Unurl: “ccmadmin/showHome.do” site:site.com

Many Cisco IP phones come installed with a web interface. To find these exposed to the Internet, type into Google:

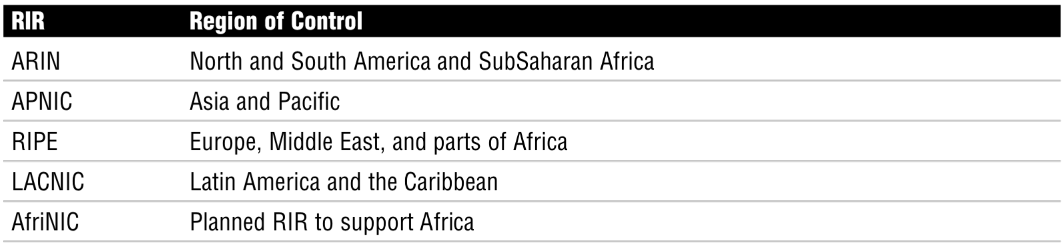
Inurl:”NetworkConfiguration” cisco

For some other web-based VoIP phone or IP PBX, there are other search terms, which are easy to find in the Internet.

Another good search engine is Shodan. Although it limits searches based on membership, it can still provide results on specific queries. Shodan searches IP addresses and finds all the devices connected to the Internet such as routers, traffic cameras or VoIP devices (9, p. 33-35).

4.1.3 WHOIS and DNS

Every connected computer on the Internet is assigned a unique address – IP address. The IP address space, AS numbers and other Internet numbering resources are distributed, allocated and managed by the four RIRs in the world. Thus, RIRs are usually where the hackers first look for information about the company or owner of a block of IP addresses. Figure 6 shows the regions and the corresponding abbreviations.



RIR	Region of Control
ARIN	North and South America and SubSaharan Africa
APNIC	Asia and Pacific
RIPE	Europe, Middle East, and parts of Africa
LACNIC	Latin America and the Caribbean
AfriNIC	Planned RIR to support Africa

Figure 6. RIRs and their corresponding regions (18, p. 14).

To locate a certain computer on the Internet, not the IP address is needed, but the domain name. Anyone who wants to register a domain name must provide some personal, geographical or contact information to the domain name providers also called registrars. Registrars submit and store the provided information in a central database called the registry or WHOIS database. The information is used to verify the owner or registrant of the domain name. This information is publicly accessible for the many reasons – enforcing the trademark and intellectual property laws, facilitating the law enforcement to control illegal activities on the Internet etc.

So after gathering the initial basic information from open-source search, the next thing hacker would do, is to find the IP address and domain name of the target. This information will be searched with WHOIS from the WHOIS database. Information stored in the WHOIS database can be dig up by using a WHOIS client. WHOIS client is built-in and available in almost every Linux platform.

To get the IP addresses and domain names, there are many ways. For example, searching the RIR websites (in this case the Europe region from Figure 6) with the whois command for a certain company name, it gives you the IP addresses used in that company:

```
# whois “company string”@whois.ripe.net
```

WHOIS searches will not always provide all of the IP ranges in use by a company. In this case, the company has outsourced their web and DNS hosting. In this case WHOIS lookup on a DNS domain can be used rather than the company name:

```
# whois company.com
```

Alternatively, some websites offer a free WHOIS domain lookup service that resolves the correct information regardless of the country of the original DNS registrar. For example www.allwhois.com is that kind of website. Information displayed there is the company address, administrative contact, technical contact and name servers (17, p. 9-19; 9, p. 36-38).

4.2 Scanning

The second phase of hacking is scanning. The information discovered in the footprinting phase is still at a basic level. The hacker needs to get more information about the target and for this, he needs to probe and communicate with the target. Scanning differs from footprinting because it comes with a higher risk of being exposed. This is why this phase needs more consideration and caution of what will be done.

There are four commonly encountered scanning objectives:

1. Determining whether system is alive
2. Discovering open ports
3. Identifying network services
4. Detecting operating system

This list does not cover everything there is about scanning, scanning may differ depending on the hacker (17, p. 1-2).

4.2.1 Determining Whether System Is Alive

One of the first steps is to discover if individual systems are alive, meaning they can be reached from the Internet. Systems in such cases are hosts and devices. To do this, the hacker needs to perform an automated ping sweep on a range of addresses and network blocks to see if there is any response. The address range can be a compilation of phone numbers or IP addresses discovered in the footprinting phase. Pinging a range of IP addresses manually can take hours if not days to complete, that is why hackers use automated pinging process, which pings huge numbers of hosts or IP addresses in a short amount of time.

Ping is commonly used as a network diagnostic tool and is included in most operating systems. Pings uses ICMP ECHO REQUEST packets to a target system in attempt to elicit an ICMP ECHO_REPLY indicating the target system is alive. If there is no ICMP echo reply packet returned, the ping assumes the target host is dead or non-existent.

There are many different scanning tools such as nmap, fping, Angry IP scanner, SuperScan etc., but the most respected and well-known port scanner is the nmap. It is open-source utility that works on Linux, Windows and Mac operating systems and can be used from command line or GUI frontend called Zenmap. Because it has many different unique features, you can adjust your scanning with optimal results. It is used by many systems and network administrators for network inventory, managing service upgrade schedules and monitoring host and service uptime. In this example nmap in Linux is used to show a standard ping sweep, which means sending type 8 ICMP packet to a range of IP addresses (9, p. 44; 17, p. 14):

```
# nmap –sP (IP range)
```

ICMP allows conducting many different types of queries, not just the ICMP ECHO REQUEST, which is type 8 ICMP query, cf. Table 1. There are also specific tools for sending other types of ICMP packets, for example SuperScan, hping, icmpenum and icmpscan to name a few. These types of queries are used when the target system has blocked the ICMP ECHO REQUEST packets (9, p. 46).

Packet type	**Description**
0	Echo reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

Table 1. ICMP packet types (9, p. 46-47).

Not all systems allow ICMP through their firewall and routers as a security measure. Administrators rather block scanning than allow a diagnostic tool to be useful for a potential hacker. For this reason several types of scanning techniques have been developed:

- ARP sweeps
- TCP ping scans
- SNMP sweeps
- Wardialing

Address Resolution Protocol (ARP) provides the mechanism for hosts and devices to maintain mappings of IP and Ethernet addressing, also known as MAC addresses. This is necessary, because Ethernet-aware switches and hubs are typically unaware of the upper-layer IP addressing schemes. By using ARP broadcast frame to request MAC addresses though a large range of IP addresses on the local LAN, hackers can see which hosts are alive on the local network. To perform ARP pings in Linux command line:

```
# arping –I (interface) –c (IP address)
```

TCP ping scans involve taking advantage of the behaviour of the TCP/IP handshake and other general TCP/IP connection flags. Hacker sends a TCP SYN or ACK flagged packet to a commonly used TCP port on the target host. A returned RST packet indicated that a host is alive on the target IP address. Using nmap on Linux and sending a SYN packet to port 80:

```
# nmap –Pn-PS –p80 (IP address)
```

Simple Network Management (SNMP) sweeps mean scanning using the SNMP protocol. This protocol is usually used to monitor and manage network devices. It has three versions, the first version being the least secure. SNMP is disabled by default, but when enabled, network administrators still forget to change the default community strings, which are cleartext passwords. When this default string is used, SNMP scans return a lot of sensitive data. Tools for SNMP scanning are nmap, SoftPerfect, SNScan (9, p. 48-53).

Wardialing is a technique of using a modem to automatically scan a list of telephone numbers. This is used to uncover more information about the active numbers discovered in the footprinting phase, including active numbers within the known ranges, fax numbers within the company, modems and DISA numbers. Besides discovering active hosts on the network, wardialing is also useful for detecting repeat dial tones and especially IP PBX devices that allow through-dialing, for they can be basis of full-scale phone and VoIP frauds.

Besides the range of phone numbers of the target, hackers need a software to dial a list of phone numbers to detect the responses. This software is called a war-dialer. There are many war-dialers available both commercial and non-commercial ones. Most older war-dialers use a modem to wardial calls (Toneloc, THC-SCAN, SecureLogix Telesweep Secure, Sandstorm PhoneSweep), but the latest wardialer WarVOX uses VoIP, which is much more efficient and less expensive (9, p. 64).

WarVOX was released in 2009 and runs on Ubuntu and BlackTrack Linux and has the ability to capture, store and classify a wide range of interesting lines, not only modems, but faxes, voicemail boxes, IP PBXs, loops, dial tones, IVRs and forwarders.

Installation for WarVOX can be found from their website, current release is the WarVOX (1.0.0). As it uses VoIP to wardial, hacker must choose a VoIP provider in the configuration process. In the configuration process, hacker also needs to specify the range of phone numbers, duration of the call, the maximum number of outgoing lines and source caller ID. The last three can be randomized (19, p. 1).

4.2.2 Discovering Open Ports

After discovering what hosts or devices are alive, the next step is to find out open ports on those remote hosts. A port is a point of entry to a system, providing a means for authorized users communicating and exchanging data with the system though the listening network service. For the hacker, it is potential point of vulnerability where they try to exploit and gain unauthorized access to the system.

In port scanning, the hacker will attempt to send out a network packet also known as request for connection to a particular TCP or UDP port on the target system and wait for response. TCP and UDP are the primary two protocols that support VoIP services, but these can be also used to discover other types of services also, like DNS, SMTP etc. (17, p. 16).

The two most effective scan types are TCP SYN scan and UDP scanning. The TCP SYN scan is also referred as half-open scanning. A SYN packet is sent to open a real connection and the response is examined. The hackers use automated scanning tools or so called port-scanners to handle and speed up the verification of TCP and UDP ports. One of the pioneers of implementing various port scanning techniques is Fyodor, who incorporated these techniques to his nmap tool. To launch a TCP SYN scan:

```
# nmap –sS (IP address)
```

After scanning with nmap, nmap responses hold port states that can be:

- Open – The port is actively accepting TCP connections or UDP packets. Finding these is the primary goal of port scanning.
- Closed – The port is accessible, but there is no application listening on it.
- Filtered – Nmap cannot determine weather the port is open, because packet filtering prevents its probes from reaching the port. Packet filtering could be from firewalls or router rules.
- Unfiltered – The port is accessible, but nmap is unable to determine whether it is open or closed.
- Open|filtered – Nmap places ports in this state when it is unable to determine if a port is open or filtered.
- Closed|filtered - Nmap places ports in this state when it is unable to determine if a port is closed or filtered.
- Tcpwrapped – If the TCP Wrapper is used for firewall, this response indicated that external entity is not authorized to connect to the port (9, p. 55-58).

There are many other port scanning techniques such as TCP Connect, TCP FIN, TCP NULL, TCP ACK, TCP Xmas Tree, TCP Windows, TCP RPC scans. As can see, most scanning techniques exploit TCP, because TCP offers more opportunity for the hacker to manipulate than UDP. TCP offers robust communications – it establishes a connection with 3-way handshake and terminates the session using 4-step shutdown. (18, p. 114).

In UDP scan, an empty UDP packet is sent to every targeted port and the responses, which are error messages are examined. If the port is open, the UDP packet is discarded and there is not response. When ICMP Port Unreachable response is received, the port is closed. UDP tends to generate more false positive results, because it is simple connectionless protocol that does not guarantee the delivery of UDP packet (17, p. 30).

4.2.3 Identifying Network Services

Even though the hacker could indentify the services listening on a particular open port with different port scanning techniques, there is more information that could be required such as the exact software application used for providing the service and its version. With this information, the hacker can proceed to vulnerability mapping – the attempt to identify the associated vulnerabilities of the network service.

Banner grabbing is the most effective way to identify the software application and the version. It sends a packet to a port and then analyzes the response returned by the port to look for a string – banner message – that advertises or gives away information about the software. This can also be done with nmap:

```
# nmap –sSV –p (IP address)
```

Nmap has many options found from help or man pages in Linux. With different options you can find out the owner of the process that is bound to that particular port or decoy to target so the real scan is not noticed etc.

Alternatively the hacker can use other port scanners to find the services and version such as strobe, netcat, amap etc. Banner grabbing can be also done manually using Telnet or netcat, with no need of using tools, but just the Linux command line:

```
>telnet (IP address) (port)
# nc –v –n (IP address) (port)
```

This shows how simple it is to find out information about an open port (17, p. 46-47).

4.2.4 Detecting Operation System

The hacker should be able to detect the Operation System (OS) of the remote host in order to do the vulnerability mapping, because vulnerabilities and exploits are very dependent on the OS version (17, p. 48).

There are two ways in which the hacker can attempt to identify the targeted devices:

- Passive stack fingerprinting
- Active stack fingerprinting

Passive stack fingerprinting is the first choice for the hacker, which is basically monitoring aka sniffing packers as they come by. These packets are examined for certain characteristics that are specific to a certain OS (18, p. 122).

First the hacker needs to setup a sniffer and initiate a connection to the target host for the sniffer to capture the packets exchanged. Then the hacker analyzes several TCP header attributes:

- Time-to-Live (TTL)
- Window Size
- Don’t Fragment Bit
- Type of Service (TOS)

These attributes are compared with a OS fingerprint database, comprising a wide range of know OS fingerprints, to find out which OS has the same attributes. There are again many OS databases available, such as p0f, ettercap, siphone etc.

Passive stack fingerprinting is stealthy and supposedly undetectable, but it has its drawbacks. The analyzed TCP header attributes may be altered or changed by the target host or intermediary devices – firewalls and proxy servers – and therefore are not accurate, thus making the OS guess wrong (17, p. 54-56).

Active stack fingerprinting is more powerful than passive stack fingerprinting which involves sending a crafted network packet to a remote system to elicit an unique response from the TCP/IP stack of the underlying OS. The unique response is referred as OS fingerprint or signature and it identifies one OS from another. The fingerprint is then compared to an OS database and the OS that matches is the underlying OS. The most common active stack fingerprinting methods are:

- FIN Probe
- Bogus Flag Probe
- ISN sampling
- IPID sampling
- TCP initial window size
- ACK value
- TOS
- TCP options
- Fragmentation handling
- Don’t Fragment Bit
- ICMP Error Message Quenching
- ICMP Error Message Quoting
- ICMP Error Message Echo Integrity

Although with active stack fingerprinting accurate and detailed information can be gained about the OS, it is not stealthy in nature, so he may be exposed to the remote intrusion detection system or firewall system when sending a crafted network packet to the remote host.

Again there are very many security tools that are capable of detecting a remote OS such as queso, nmap, Winfingerprint and Xprobe. Nmap is the tool of choice as it is one of the most feature-rich free fingerprint tools out there. Nmap database can fingerprint hundreds of different OSes. Fingerprinting with Nmap is initiated by running the tool with the –O option:

```
# nmap –O (IP address)
```

With this command, nine tests are done – 7 different modified TCP packets are sent to TCP ports, one UDP packet to UDP port and finally TCP sequenceability test is performed. The anwers are examined and the best guess for the OS is given using percentages.

Nmap is challenged by a tool called Xprobe. Xprobe 2 is a Linux-based active OS fingerprinting tool what uses mixture of TCP, UDP and ICMP to slip past firewalls and avoid IDSs. It relies on fuzzy signature matching – the targets are run though a variety of tests, the results are totalled and the user is presented with a score that tells the probability of the targeted machine's OS (17, p. 48-54).

4.3 Enumeration

The next and last step in information gathering is enumeration. It involves probing the identified services more fully for known weaknesses. It has higher level of intrusiveness and is easily noticed and logged. Enumeration is heavily dependent on the previous step, which was scanning. Often port scanning and enumeration is bundled together.

Enumeration involves getting such information as user account names, oft-misconfigured shared resources, older software versions with known security vulnerabilities etc.

One of the most common enumeration is against SIP protocol. Targeting SIP proxy or location server will provide user registration and presence. There are several methods, which rely on studying the error messages returned: SIP REGISTER, OPTIONS and INVITE username enumeration. These involve knowing the valid usernames and extensions of SIP phones and the registration or proxy servers. This information was gained in the footprinting and scanning steps (for example with open-source and wardialing).

4.3.1 REGISTER Username Enumeration

This involves gaining information about valid accounts registered on the VoIP network using error messages from SIP proxy or registration servers. Hacker sends SIP REGISTER requests to the proxy or registration server with the specified extension and checks for the response status code if and extension is valid. When the 401 Unauthorized or 407 Proxy Authentication Required or 200 OK is received, the SIP account username was valid. If 403 Forbidden is received, the SIP account username was invalid.

4.3.2 INVITE Username Enumeration

This is the noisiest and least stealthy method for SIP username enumeration, because it involves ringing the targets phone. Sending an SIP INVITE request, also meaning initializing a call to target with valid user usually generates 100 Trying and 180 Ringing messages, which means the SIP username extension was valid. When 404 Not Found is received, it means the SIP username extension was invalid. INVITE requests can be sent directly to phones if their IP addresses are known. This way the proxy or registration server is bypassed and the call in not logged.

4.3.3 OPTIONS Username Enumeration

The OPTIONS method is the most stealthy and effective methods from these three. The OPTIONS is used to advertise supported message capabilities and legitimate users. Depending if the received message was 200 OK or 404 Not Found, you can differentiate the valid and invalid SIP username extensions (9, p. 81-95).

Gaining SIP extensions with these methods can be time-consuming, so there are several tools to automate this process, the most known of them is SIPVicious. It is a suite of command-line tools that works on Linux, Mac and Windows platforms. The suite of tools includes (20, p. 1):

- Svmap – SIP scanner that lists SIP devices found on a IP range.
- Svwar – identified active extensions on a PBX.
- Svcrack – an online password cracker for SIP PBX.
- Svreport – manages sessions and exports reports to various formats.
- Svcrash – attempts to stop unauthorized svwar and svcraxk scans.

For extension scanning, the svwar.py tool is used, which supports REGISTER, INVITE and OPTIONS scans. The commands are as follows:

```
./svwar.py –e (Extension) (IP address)
--method=(REGISTER or INVITE or OPTIONS)
```

There are several other tools to use to scan SIP extensions such as sipsak, SIPSCAN. Knowing the exact extension assigned to a phone fives a hacker vital information to brute force voicemail credentials, spoof SIP credentials or calls etc. (9, p. 95-96).

4.3.4 Enumeration of Other VoIP Support Services

Hackers can also enumerate other services that support VoIP, such as TFTP servers, SNMP and VxWorks devices.

Majority of phones rely on a Trivial File Transfer Protocol (TFTP) server for downloading their configuration settings. TFTP is insecure, because it requires no authentication to upload or fetch a file. The IP address of the TFTP server can be found out by listening to UDP port 69, where the TFTP service usually listens:

```
# nmap –sU –T4 –p69 (IP address range)
```

The next step is getting the MAC address of the VoIP phone, because the configuration files are often a derivate of the phone’s MAC address, for example when Cisco 7942 phone is used. Guessing the file name, pulling the files off the TFTP server with tftpbrute.pl and reading it with TFTPUtil for example, typically gives you information about IP address of the IP phone’s gateway, the software version, weather the phone is using SIP or SCCP, the user ID and password if they are available on the phone.

With Simple Network Management Protocol (SNMP) you can get the configuration information such as vendor type, operation system, MAC address, ports in use. This can be done if SNMP version 1 is used, as it is very insecure protocol. For this the SNMP feature has to be turned on, as it is by default turned off:

```
# nmap –sU –p 162 (IP address range)
```

Then with SNMP probing tool such as SNMP-Probe or snmpwalk the configuration can be enumerated.

Many IP phones are developed on embedded real-time operation systems, for example VxWorks. Before the phone is shipped, some vendors forget to turn off the diagnostic feature of VxWorks, which allows for administrative debugging access to the device. This can be exploited by the hacker to access read and write memory and power cycle of the device. With this hackers can steal data, backdoor the running firmware image and take control over the phone. VxWorks listens to port 17185, so to see if it is on, using nmap use:

```
# nmap –sU (IP range) –p 17185
```

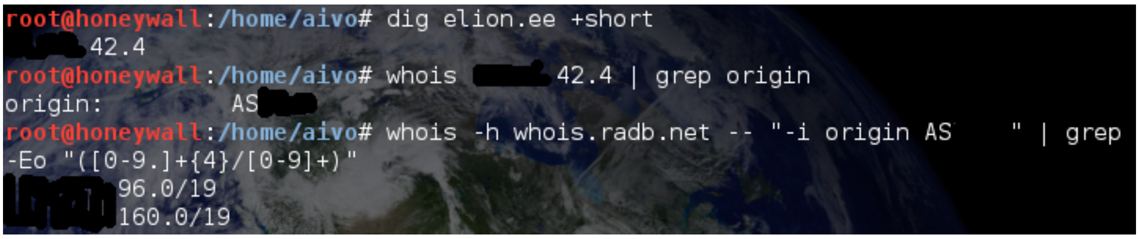
These methods are only a handful of the most common enumeration methods out there. But these are already enough to gain enough information to launch a full attack or fraud (9, p. 98-102).

5 Setting up Basic Scanning

Because there is not that much one can do against footprinting, the focus in this study was on the protection against scanning, which is also scanning. Usually this is the first step that is needed to start securing VoIP network – setting up basic scanning to eliminate any entrance points to the system.

Going through the steps in the attack and defence scanning chapter, a small network segment was scanned with nmap in the company at hand to see if weaknesses were found, focusing mainly on open SIP ports.

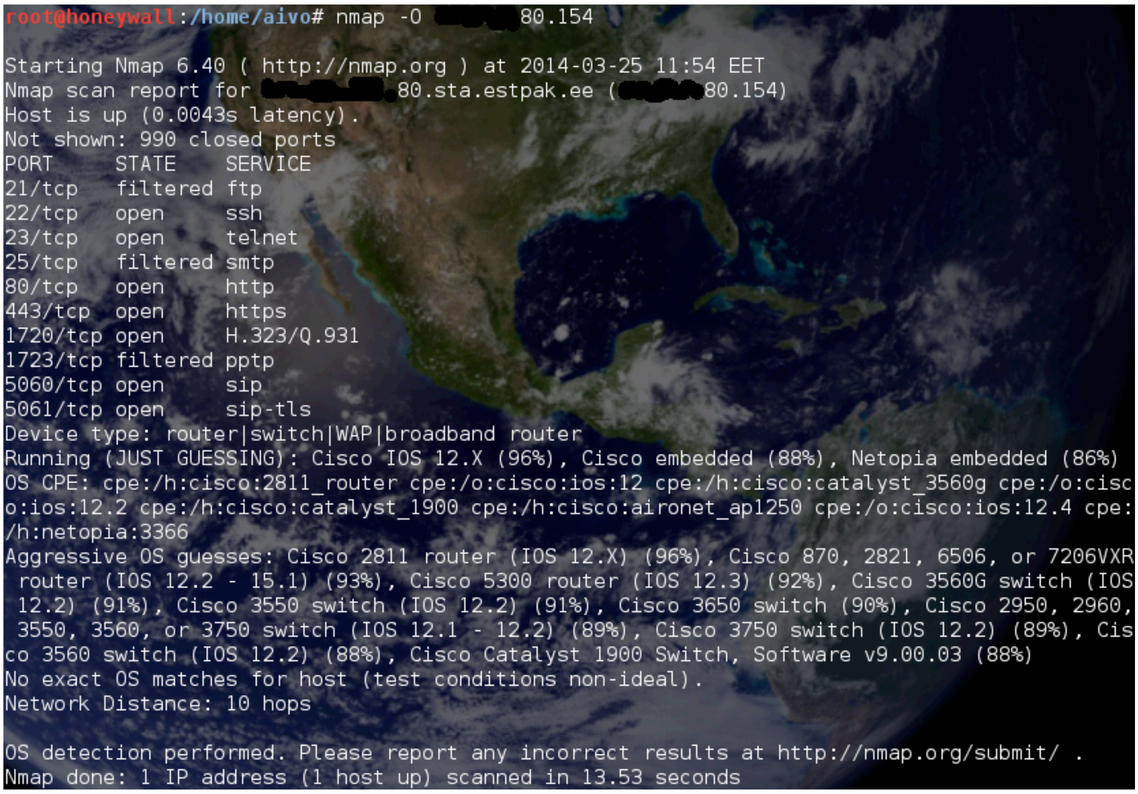
The first thing was to find the IP address for the company hostname. In this case, the dig command in Linux was used, which is usually used for querying DNS name servers. The next thing was to get the AS number for the company with WHOIS command. With the AS number, WHOIS database could be seen to list the IP-address blocks used in the company. The whois.radb.net database was used, which is one of the biggest Internet routing registry and the IP addresses were grepped out. These commands can be seen in Figure 7.



```
root@honeywall:/home/aivo# dig elion.ee +short
[redacted]42.4
root@honeywall:/home/aivo# whois [redacted]42.4 | grep origin
origin:         AS[redacted]
root@honeywall:/home/aivo# whois -h whois.radb.net -- "-i origin AS     " | grep
-Eo "([0-9.]+{4}/[0-9]+)"
[redacted]96.0/19
         160.0/19
```

Figure 7. Acquiring the IP addresses of the company.

After acquiring the IP-addresses, the X.X.0.0/17 block of IP addresses was scanned and the X.X.80.154 was chosen to fingerprint it with the nmap. Fingerprinting showed the open ports, the services running on those ports, gave the guesses for the underlying OS and the version (cf. Figure 8).

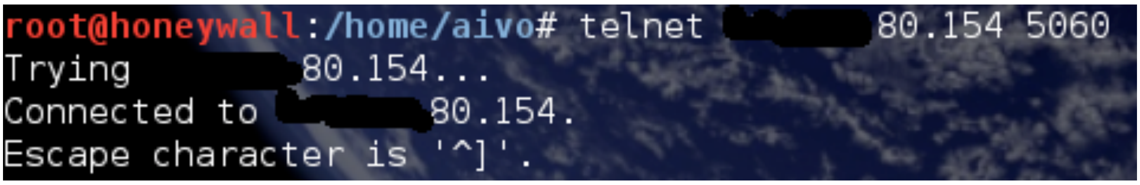


```
root@honeywall:/home/aivo# nmap -O [redacted]80.154

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-25 11:54 EET
Nmap scan report for [redacted]80.sta.estpak.ee ([redacted]80.154)
Host is up (0.0043s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   filtered smtp
80/tcp   open     http
443/tcp  open     https
1720/tcp open     H.323/Q.931
1723/tcp filtered pptp
5060/tcp open     sip
5061/tcp open     sip-tls
Device type: router|switch|WAP|broadband router
Running (JUST GUESSING): Cisco IOS 12.X (96%), Cisco embedded (88%), Netopia embedded (86%)
OS CPE: cpe:/h:cisco:2811_router cpe:/o:cisco:ios:12 cpe:/h:cisco:catalyst_3560g cpe:/o:cisc
o:ios:12.2 cpe:/h:cisco:catalyst_1900 cpe:/h:cisco:aironet_ap1250 cpe:/o:cisco:ios:12.4 cpe:
/h:netopia:3366
Aggressive OS guesses: Cisco 2811 router (IOS 12.X) (96%), Cisco 870, 2821, 6506, or 7206VXR
 router (IOS 12.2 - 15.1) (93%), Cisco 5300 router (IOS 12.3) (92%), Cisco 3560G switch (IOS
 12.2) (91%), Cisco 3550 switch (IOS 12.2) (91%), Cisco 3650 switch (90%), Cisco 2950, 2960,
 3550, 3560, or 3750 switch (IOS 12.1 - 12.2) (89%), Cisco 3750 switch (IOS 12.2) (89%), Cis
co 3560 switch (IOS 12.2) (88%), Cisco Catalyst 1900 Switch, Software v9.00.03 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```

Figure 8. Fingerprinting with nmap.

For more precise information one can go over the nmap commands in the scanning chapter, but in this case, nmap fingerprinting gave us all the information needed. Open SIP ports were found as well as the guess for the OS, which is Cisco IOS version 12.X router.

As SIP enabled devices are usually listening on UDP/TCP ports 5060 and 5061, the focus was on those ports and trying to access them.



```
root@honeywall:/home/aivo# telnet [redacted]80.154 5060
Trying [redacted]80.154...
Connected to [redacted]80.154.
Escape character is '^]'.
```

Figure 9. Telnet into the open port.

Figure 9 shows that the open SIP port was gained access to, which is what all hackers look for. From there you can hack the SIP device may it be an IP PBX, SIP phone or another SIP-enabled device and a VoIP fraud can be launched.

6 Conclusion

The study only scraped the world of VoIP frauds and the possibilities of preventing them. The list of VoIP frauds keeps getting longer and the methods become more elaborate every day. It seems VoIP security was just an after-thought and security experts are always one step behind, picking up the scraps and trying to ease the damage.

Companies are not really focusing on VoIP security, due to lack of resources or employees as can be seen from the amount of money lost to VoIP frauds. Even the company at hand did not have anybody securing the VoIP network. Due to this millions can be lost in a big scale fraud and only after that, it is realized that something must be changed.

The study presented a basic scanning technique, which is the first step in securing the VoIP networks, not considering a security policy. A lot of hackers are stopped with simple scanning and reducing the security holes uncovered. The study went through the steps that a hacker does and that a security expert has to in order to realize how vulnerable the VoIP network really is.

The scanning technique uncovered many security holes for the company at hand and it is fairly easy to access the network and do damage before it is discovered. To prevent this from happening in a real scenario, companies should have more security experts focusing on the VoIP devices and network – scanning them and locking up security holes that can be exploited.

References

1 Walker, John Q. Hicks, Jeffrey T. 2004. Taking Charge of Your VoIP Project. USA: Cisco Press.

2 How do IP phone systems work? 2014. Web document. <http://askozia.com/voip/ip-phone-systems/>. Read 5.03.2014.

3 Magnusson, Janne. SIP trunking benefits and best practices. Web document. <https://www.ingate.com/files/white_paper_What_is_SIP_Trunking_A.pdf>. Read 4.03.2014.

4 Porter, Thomas. Practical VoIP Security. 2006. Canada: Syngress Publishing, Inc.

5 Persky, David. 2007. VoIP Security Vulnerabilities. Web document. <http://www.sans.org/reading-room/whitepapers/voip/voip-security-vulnerabilities-2036>. Read 3.01.2014.

6 Unuth, Nadeem. Device-Based VoIP - Ridding Your VoIP of Monthly Bills. Web document. <http://voip.about.com/od/servicesandsolutions/a/ooma-phoneg-mj.htm>. Read 12.03.2014.

7 Unuth, Nadeem. What is VoIP service? Web document. <http://voip.about.com/od/servicesandsolutions/a/What-Is-Voip-Service.htm>. Read 12.03.2014.

8 VoIP service providers. 2014. Web document. <http://www.voip-info.org/wiki/view/VOIP+Service+Providers+Business+Europe>. Read 12.03.2014.

9 Collier, Mark. Endler, David. 2014. Hacking Exposed: Unified Communications & VoIP. USA: McGraw-Hill Education.

10 2013 Global Fraud Loss Survey. 2013. Web document. <http://www.cvidya.com/media/62059/global-fraud_loss_survey2013.pdf>. Read 27.02.2014.

11 Sipera Systems. The security challenge: Combating VoIP & UC Fraud. 2011. Web document. <http://www.sipera.com/webfm_send/167>. Read 12.02.2014.

12 VibeSec. PBX Toll Fraud Prevention. Web document. <http://vibesec.com/resources/WP-FRP_Using_Vigilance_for_Fraud_Prevention.pdf>. Read 11.02.2014.

13 Case study: International revenue share fraud. 2008. PDF-source. <http://www.agilisinternational.com/assets/IRSF.pdf>. Read 12.02.2014.

14 VoIP theft of service: protecting your network. 2013. PDF-source. <http://www.phonepower.com/Contact/News/PressReleases/2013-voip-theft-of-service.pdf>. Read 13.02.2014.

15 Asterisk auto-dial out. 2013. Online source. <http://www.voip-info.org/wiki/view/Asterisk+auto-dial+out>. Read 12.02.2014.

16 Subscriber fraud explained. Online document. <http://fraud.laws.com/cellular-phone-fraud/subscriber-fraud>. Read 3.03.2014.

17 Footprinting and Scanning: Encored. 2005. Online source. <http://www.ecqurity.com/resources-white-papers.html>. Read 26.02.2014.

18 Preparing for Certified Ethical Hacker Exam: Footprinting and Scanning. PDF-source. <http://ptgmedia.pearsoncmg.com/images/9780789735317/samplechapter/0789735318_CH03.pdf>. Read 27.02.2014.

19 WarVOXIntroduction. 2013. Online document. <http://www.warvox.org/>. Read 27.02.2014.

20 SIPVicious summary. Online document. <https://code.google.com/p/sipvicious/>. Read 2.03.2014.