Mitigating Denial-of-Service Attacks on VoIP Environment

Igor Jouravlev, University of Toronto

Abstract

IP telephony refers to the use of Internet protocols to provide voice, video, and data in one integrated service over LANs, BNs, MANs, not WANs. VoIP provides three key benefits compared to traditional voice telephone services. First, it minimizes the need fro extra wiring in new buildings. Second, it provides easy movement of telephones and the ability of phone numbers to move with the individual. Finally, VoIP is generally cheaper to operate because it requires less network capacity to transmit the same voice telephone call over an increasingly digital telephone network (FitzGerald & Dennis, 2007 p. 519). Unfortunately, benefits of new electronic communications come with proportionate risks. Companies experience losses resulting from attacks on data networks. There are direct losses like economic theft, theft of trade secrets and digital data, as well as indirect losses that include loss of sales, loss of competitive advantage etc. The companies need to develop their security policies to protect their businesses. But the practice of information security has become more complex than ever. The research paper will be about the major DoS threats the company's VoIP environment can experience as well as best countermeasures that can be used to prevent them and make the VoIP environment and, therefore, company's networking environment more secure.

Keywords

VoIP, Denial-of-Service

Introduction

Background

Voice over IP (VoIP) is one of the newest technologies that is being rapidly embraced by the market as an alternative to the traditional public switched telephone network (PSTN). VoIP is a broad term, describing many different types of applications – for example, hard phones, softphones, proxy servers, Instant Messaging clients, peer-to-peer clients. They are installed on a wide variety of platforms – Linux, Windows, mobile devices. These applications use a wide variety of proprietary and open protocols that depend heavily on the

preexisting data network's infrastructure and services. Therefore, VoIP security is as broad a subject as a number of devices and applications used in the VoIP environment in organizations. The current research paper is dedicated to VoIP security which becomes more important and more relevant nowadays. It is well known that the benefit of electronic communication come with proportionate risks. Critical business systems can be and are compromised regularly, and are used for illegal purposes. These systems constantly experience attacks that can cause substantial losses.

The following table describes losses that a company can experience from attacks on data networks (Porter, 2006, p. 3):

Table 1 Losses Resulting from Attacks on Data Networks

Direct Losses	Indirect Losses
Economic theft	Loss of sales
Theft of trade secrets	Loss of competitive advantage
Theft of digital assets	Brand damage
Theft of consumer data	Loss of goodwill
Theft of computing resources	Failure to meet contract obligations
Productivity loss due to data corruption	Noncompliance with privacy regulations
Productivity loss due to spam	Officer liability
Recovery expenses	Reparations

As we can see from the table the company simply can go bankrupt and default. Partially it can happen if the company doesn't have secure VoIP environment.

The following table describes the general levels of that can be attacked in a VoIP infrastructure (Porter, 2006, p. 240).

Table 2VoIP Vulnerabilities

Vulnerability	Description
IP infrastructure	Vulnerabilities on related non-VoIP systems can lead to compromise of VoIP infrastructure.
Underlying operating system	VoIP devices inherit the same

	vulnerabilities as the operating system or firmware they run on. Operating systems are Windows and Linux.
Configuration	In their default configuration most VoIP devices ship with a surfeit of open services. The default services running on the open ports may be vulnerable to DoS attacks, buffer overflows, or authentication bypass.
Application level	Immature technologies can be attacked to disrupt or manipulate service. Legacy applications (DNS, for example) have known problems.

According to Orans (2005), the common VoIP threats are network-based denial of service (DoS), eavesdropping, and signaling protocols. DoS attacks are especially problematic in a VoIP environment, because the network congestion that they introduce can make conversations unintelligible. In LANs and WANs, the threat can be mitigated by creating a separate virtual LAN for voice traffic and protecting it (via bandwidth reservation, for example) from malicious traffic that could overrun it. VoIP over the Internet remains a riskier proposition, due to the lack of QoS in Internet backbone networks (p. 2).

Another threat that is very has received a lot of attention due to the understandable fear that malicious people can listen in on our conversations is eavesdropping. Packet capturing, or "eavesdropping," is technically an issue within LANs, WANs and the Internet, although this risk is generally overhyped. The same eavesdropping techniques apply whether the intent is to capture data packets or voice ones. Therefore, the same precautions that organizations implement to protect data traffic against eavesdropping also apply to voice traffic (Orans, 2006, p. 2).

Signaling Protocols are also one of the threats to VoIP. These are used to establish communication sessions between two or more endpoints. Among the standards-based

protocols, Session Initiation Protocol (SIP) is becoming the most widely deployed solution. Orans (2006) argues that it is a relatively new protocol, and is just beginning to receive the detailed security analysis and scrutiny that will enhance its resistance to attack. Other signaling standards are H.323 and MGCP. SIP's versatility enables it to establish communications over LANs, WANs and the Internet, therefore presenting common risks in all environments (p. 2).

In the current paper we will consider DoS and DDoS attacks that are very problematic for the company. The paper pursues the goal to investigate different types of DoS and DDoS attacks and countermeasures that can be effectively used by the companies to ensure business continuity.

Objectives of Study

As was mentioned above, the common VoIP threats are network-based denial of service (DoS), eavesdropping, and signaling protocols. While such threats as eavesdropping and signaling protocols are important for a company to prevent, the most problematic is the denial of service attacks that are difficult to control. The objectives of the study is investigate what types of DoS/DDoS attacks a company can experience, what effective countermeasures can be implemented to prevent such attacks to ensure business continuity of the company, and give the management suggestions on the best practices of managing secure VoIP environment.

Problem Statement

The problem statement is as follows: investigate different types of DoS/DDoS attacks, malicious scenarios that can be implemented against a company’s VoIP environment

and efficient countermeasures that a company can implement to secure its VoIP and networking environment.

Research Questions

The research questions of the study are as follows:

- What are the types and malicious scenarios of DoS and DDoS that are the most problematic to the companies?
- What are the best countermeasures and solutions that a company and management should implement to secure it VoIP and networking environment?

These questions are important since they can generate and develop a knowledge base of a company for developing and improving business continuity plan and disaster recovery plan.

Scope of Study

This study only looks at DoS and DDoS attacks the company can experience, investigation of possible malicious scenarios and countermeasures that can be implemented against these attacks.

Definition of Terms

Definition and abbreviations of the terms used in the text is presented below.

ACL - Access Control Lists

ALG - Application layer gateway

AP - Access point

ARP - Address resolution Protocol is used to resolve the hardware address of a card to package the Ethernet data. It works at the data link layer

AS—Application server

ATM - Asynchronous transfer mode

Backbone - Main cable used to connect computers on a network.

Bandwidth - Indicates the amount of data that can be sent in a time period.

Botnet - networks of software agents that often lie dormant until triggered to create harm, typically through DoS

Broadband - Uses analog signals to divide the cable into several channels with each channel at its own frequency. Each channel can only transmit one direction.

CCF - Charging collection function

CVE - Common Vulnerabilities and Exposures

DDoS - Distributed denial of service

DHCP - Dynamic Host Configuration Protocol is used to assign IP addresses dynamically to network cards works at the application layer.

DMZ - Demilitarized zone

DNS - Domain Name System is used on the internet to correlate between IP address and readable names.

DNS - Domain name system

DoS - Denial - of - service

DSCP - Differentiated Services Code Point

DSL - Digital subscriber line

EAP - Extensible Authentication Protocol

ESP - Encapsulating Security Protocol

Ethernet - A network architecture that uses carrier - sense multiple - access with collision detection (CSMA/CD) for controlling access to the network media and baseband broadcasts. It uses star topology.

FTP - File Transfer Protocol

Gateway - A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Not the same as a default gateway used by a client to send packets to.

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

IAD - Internet access device

IBCF - Interconnect border control function

ICMP - Internet Control Message Protocol is used to perform network error reporting and status. It works at the transport layer.

I - CSCF—Interrogating CSCF

IDS - Intrusion detection system

IETF - Internet Engineering Task Force

IKE - Internet key exchange

IMS - IP Multimedia Subsystem

InterNIC - Internet Network Information Center, the authority for allocating internet addresses.

IP - Internet Protocol is used for software addressing of computers and works at the data link layer

IPS - Intrusion Prevention System

IPSec - Internet protocol security, developed by IETF, implemented at layer 3.

IPS - Intrusion prevention system

IPX - Internetwork Packet Exchange supports the transport and network layers of the OSI network model.

ISDN - Integrated Services Digital Network is a method of sending voice and data information on a digital phone line. Two 64Kbps B - channels with one 16Kbps D channel is provided with basic ISDN service

ISS - Internet Security Systems

ISUP - Integrated services digital network user

LAN - Local Area Network

MAC - Media Access Control address. Basically a network card unique hardware address.

MAN - Metropolitan area network refers to a network which connects several

NAT - Network address translation

NIC - Network interface card. Also called LAN adapters.

NIPS – Network - based Intrusion Prevention Systems

OSI - Open Systems Interconnect PBX – Private Branch Exchange

PCM - pulse code modulation

Protocol - A set of standards sets of standards that define all operations within a network. There are various protocols that operate at various levels of the OSI network model such as transport protocols include TCP, SPX.

PSK - Preshared key

PSTN - Public switched telephone network

QoS - Quality of service

Router - Routes data packets between two networks.

RTP - Real Time Transport Protocol

SA - Security association

SBC - Session border controller

SDP - Session Description Protocol

Sector

SG - Security gateway

SIP – Session Initiation Protocol

SMS - Short message service

SNMP - Simple Network Management

SRTP - Secure RTP

SSH - Secure shell

SSID - Service set identifier

SSL - Secure Sockets Layer

TLS - Transport Layer Security

TTLS - Tunneled transport layer security

UDP - User Datagram Protocol

VLAN – Virtual LAN

VoIP - Voice over IP

VPN - Virtual Private Networking.

WAN - Wide Area Network

WEP - Wired equivalent privacy

Wi – Fi - Wireless fidelity

WLAN - Wireless local area network

WPA - Wi - Fi protected access

Summary of Chapter

In this chapter it was shown that for business continuity of any company, it is important to maintain secure VoIP and networking environment. The common VoIP threats are network-based denial of service, eavesdropping, and signaling protocols. A company should develop, maintain and improve its strategies against malicious attacks. The company should know how these attacks can be organized, possible attack scenarios and effective countermeasures that can prevent these attacks. The study of such attacks and countermeasures are narrowed to DoS and DDoS attacks. The objectives of the study is investigate what types of DoS/DDoS attacks a company can experience, what effective countermeasures can be implemented to prevent such attacks to ensure business continuity of the company, and give the management suggestions on the best practices of managing secure VoIP environment.

Review of Literature

There is a lot of literature available that describe threats to the VoIP and networking environment of the company – from introductory description of attacks and threats to very detailed and technical analysis of them. It is worth mentioning the works of FitzGerald & Dennis (2007) where VoIP technology is described, Davidson et al. (2007) which provides fundamentals of VoIP technology and provides more detailed description of VoIP technology and overview of typical security requirements in the context of VoIP services (pp. 221 –

236). Porter (2006) and Endler & Collier (2007) provide detailed description of possible attacks, hacks and threats VoIP environment can experience. They provide detailed explanation of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks and countermeasures that can be effective in preventing such attacks (Porter 2006, pp. 240-248; Endler & Collier, 2007, pp. 121-147). Both books describe possible DoS/DDoS attacks, how these attack are organized, what kind of harm such attacks can bring and countermeasures that should be implemented in order to prevent these attacks. The information provided in these books will be analyzed in Chapter 4. Also, there are many interesting peer-reviewed papers that discuss DoS/DDoS attacks and measures for preventing them.

Peng et al. (2007) presented an extensive survey of denial of service attacks and the methods that have been proposed for defense against these attacks. In this survey, the authors analyzed the design decisions in the Internet that have created the potential for denial of service attacks. They review the state-of-art mechanisms for defending against denial of service attacks, compared the strengths and weaknesses of each proposal, and discussed potential countermeasures against each defense mechanism. The authors think that integrated approach can be used in solving the problem of distributed DoS. They note that DoS attack generally achieve their goal by sending large volumes of packets that occupy a significant proportion of the available bandwidth. Hence, DoS attacks are also bandwidth attacks. The aim of a bandwidth attack is to consume critical resources of in a network service. Possible target resources may include CPU capacity in a server, stack space in network protocol software, or Internet link capacity. By exhausting these critical resources, the attacker can prevent legitimate users from accessing the service (p. 4).

Kurapati (2007) argues that Voice over IP (VoIP) is vulnerable like any application on the Internet, since the IP network can easily be used to launch malicious attacks and cause service abuse. VoIP networks have thousands of unique vulnerabilities that can be exploited to launch a variety of attacks. These include deliberate application-specific assaults against the VoIP infrastructure, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Even more disruptive are unique service abuses that target end-users, such as stealth attacks and VoIP spam. Companies and organizations need to be aware of and effectively protect their network from these attacks against their infrastructure and the additional ones against end-users, which are unique to IP communications applications. These application-specific threats are in addition to attacks, such as call hijacking, fraud and eavesdropping, that are using encryption and authentication.

One of the interesting articles is the one of Gelenbe (2006) that discusses intelligent networks. In this article, the author presents a vision of Intelligent Network in which users dynamically indicate their requests for services and formulate needs in terms of quality of service and price. The author examines the need to dynamically protect the networked system from denial of service (DoS) attacks and propose an approach to DoS defense which uses the detection of violations of QoS constraints and the automatic throttling or dropping of traffic to protect critical nodes.

Molsa (2005) provides an interesting tutorial on DoS attacks, how they can be carried out in IP networks, and how one can defend against them. The author considers DDoS attacks as a subset of DoS attacks (p. 808). Before an attack is possible, a DoS program must first be deployed on one or more compromised hosts. The author argues that mitigation of DoS attacks requires thus defense mechanisms for both phases, though completely reliable

protection against DoS attacks is, however, not possible. There will always be vulnerable hosts in the Internet, and many attack mechanisms are based on ordinary use of protocols. Defense in depth is thus needed to mitigate the effect of DoS attacks. This paper describes shortly many defense mechanisms proposed in the literature. The goal is not to implement all possible defenses. Instead, one should optimize the trade-off between security costs and acquired benefits in handling the most important risks. Mitigation of DoS attacks is thus closely related to risk management. The author provides a list of known general reaction mechanisms (p. 825), defense mechanisms for the attack phases against flooding that include blocking, rate-limiting, connection tear-down, flood processing in another place, and IP hopping (p. 827).

Robb (2005) focuses on different organizations applying a mix of technologies and procedures to protect the infrastructure from viruses, worm and DoS attacks. The authors argues that antivirus programs are usually client based and have scanning tools on E-mail they defend against viruses. In worm attacks, firewalls and intrusion prevention system (IPS) appliances are used in the network as well as on the endpoint. DoS attacks are something completely different; there it needs high availability networks. The Weather Channel Interactive in Atlanta has IPSs on the Internet border, intrusion detection systems that filter in-bound E-mail for viruses and malicious content, traditional packet-based firewalls and a product for filtering instant messaging (IM) traffic (p. 25). The ConSentry box is just one of a new class of devices which use algorithms to analyze traffic, rather than using signatures of viruses or worms (p. 26).

According to Yocom (2004), IP-PBXs is the one, which supports 99 stations to offer many of the sophisticated features and endpoints available on higher-end products (p. 36).

Voice quality on these systems is good overall, although high latency was an issue on some of the softphones. Only Nortel BCM networks and interactive intelligence supported SIP phones and also includes firewall, virtual private networks (VPN), a DHCP server and router in one unit. So, the denial of service (DoS) attacks was implemented to determine what kind of attacks had got through a firewall or other security mechanisms and by incorporating management applications, ease of use, intuitiveness, real-time monitoring and reporting features are obtained and the installations process has easily achieved in this analysis. Thus powerful contact centers, service response, management and collaboration tools are the good reasons to consider IP-PBXs as a better bottom line (p. 42). The author argues that unless the buyers can see some clear return on investment (ROI) for buying into VoIP and feel secure in installing it, customer may be reluctant in replacing their old telephone systems.

According to Narayanaswarny (2002) a denial of service (DOS) attack is any malicious attempt to deprive legitimate customers of their ability to access services, such as a Web server (p. 38). DOS attacks fall into two broad categories: server vulnerability attacks and packet flooding attacks. Many wonder why network security problems have seemingly increased suddenly in seriousness and importance. The main reason, according to the author, is the unanticipated growth and success of ISPs (p. 39). The rapid growth of affordable, high bandwidth connection technologies offered by various ISPs has brought in every imaginable type of customer to the fast Internet access arena: corporations, community colleges, small businesses, and the full gamut of home users (Narayanaswarny, p. 39). Unfortunately, people who upgrade their bandwidth do not necessarily upgrade their knowledge of network security at the same time; all they see is what they can accomplish with speed. Few foresee the potential security dangers until it is too late. As a result, the Internet has rapidly become a

high-speed network with depressingly low per-site security expertise. Such a network is almost an ideal platform to exploit in various ways, including the mounting of DOS attacks. Architecturally, ISPs are ideally situated to play a crucial role in containing the problem, although they have traditionally not been proactive on security matters (Narayanaswarny, p. 39). The author of the article presents strategies on defending DDoS attacks that includes the following steps: ensure the integrity of the infrastructure, resist zombies in the infrastructure, implement appropriate router filters, disable facilities the customers may not need (pp. 40-42). The author also emphasize the importance of assisting customers during DDoS attacks, assessment of DDoS technologies protection against outgoing and incoming DDoS attacks (pp. 42 – 45).

Walters (2001) provides description of 10 ways to prevent denial of service attacks. Web site owners need to take specific steps to ensure their systems are protected from DoS (denial of service) and DDoS (distributed denial of service) attacks, which prevent legitimate users from accessing and using a site or particular service. In seeking to prevent DoS/DDoS attacks, every Web site has four areas of vulnerability: the gateway, the host, hardware/software, and personnel. The following recommendations address these four areas: (1) adopt a security policy and educate, educate, educate; (2) use multiple Internet service providers (ISPs); (3) practice good load balancing; (4) ensure redundancy (or "fall-over") in all network devices, servers and power sources; (5) protect your critical systems with a hardened firewall; (6) auto-check your Web site; (7) keep the system simple; (8) stay current on upgrades, updates, vendor advisors and security bulletins; (9) stay vigilant through testing and monitoring; and (10) be ready to respond (pp. 71-72).

Neumann (2000) analyzed risks of DoS attacks relating to the Internet. He argues that DoS attacks are like computer viruses, there exits no present preventive solutions. Distributed DoS are still more difficult to detect, as they come from various sources, that too, when they use spoofed IP addresses. Some common security advices include, installing and properly configuring firewalls, demanding cryptographic authenticators rather than reusable fixed passwords etc. As this problem is desperately in need of technological and operational approaches, the U.S. Federal Bureau of Investigation and the organization National Infrastructure Protection Center are taking role in trying to track down attackers (p. 136).

According to Hovav & D'Arcy (2003), the increase in security breaches in the last few years and the need to insure information assets has created an intensified interest in information risk within organizations and for insurance companies. Risk assessment is an important component in the establishment of security policies. However, very little is known of the financial impact and the risk associated with security breaches. The authors report the impact of Denial-of-Service (DOS) attack announcements on the market over a period of 4.5 years. The study was conducted using event study methodology. The results show that in general the market does not penalize companies that experience such an attack. However, there is an indication that the market penalizes “Internet-specific” companies more than the companies that are not Internet-specific. The results indicate that large companies who are not “Internet-specific” might be overreacting to the media hype and may be investing resources to prevent a problem that has marginal impact on their shareholder value (p. 97).

Methodology

The methodology is based on analyzing the information provided by researchers on DoS/DDoS threats and countermeasures that can be effectively used in preventing such

attacks. I have chosen books and peer-reviewed article available in EBSCPO database. I also analyzed the information provided in electronic research papers of such well known company as Cisco which is the leader in networking as well as electronic research studies of Computer Emergency Response Team of Carnegie Mellon University. These sources were chosen since they provide reliable and peer-reviewed information that can be used in further analyses and studies. These resources will be analyzed and synthesized to provide answers to the research questions. This type of research is known as secondary research. The purpose of such research is to synthesize the knowledge obtained earlier to solve practical problem. As it was shown before, DoS/DDoS is problematic for many companies, and many of them need to develop business continuity and disaster recovery plans for protecting their business operations and transactions. To be able to do so, it is important to analyze, compare, and synthesize knowledge and best practices contained in the peer-reviewed resources about possible DoS/DDoS attacks and effective countermeasures. To achieve this goal I will study such resources by analyzing the malicious scenarios undertaken by attackers, countermeasures against such practices, and make suggestions on the best approaches in securing the company's VoIP and networking environment, and, therefore, the company's assets.

Analysis of DoS and DDoS Attacks and Countermeasures

In this chapter analysis of malicious scenarios of DoS and DDoS is provided and the best countermeasures and solutions are explored for securing VoIP environment.

General Characteristics of DoS and DDoS Attacks

DoS and DDoS attacks violate the availability goal of computer security. An online site is available if a person or program can gain access to the pages, data, or services

provided by the site when they are needed. Technologies such as load-balancing hardware and software can help ensure availability. In an ordinary network-based denial of service attack, an attacker uses a tool to send packets to the target system. These packets are designed to disable or overwhelm the target system, often forcing a reboot. Often, the source address of these packets is spoofed, making it difficult to locate the real source of the attack (Farrow, n.d.).

In the DDoS attack, there might still be a single attacker, but the effect of the attack is greatly multiplied by the use of attack servers known as "agents". These agents are remotely controllable by the hacker. To get an idea of the scope of this attack, over 1,000 systems were used at different times in a concerted attack on a single server at the University of Minnesota. The attack not only disabled that server but denied access to a very large university network (Farrow, n.d.).

Distributed denial of service (DDoS) attacks depend on getting the DDoS client to run on a wide range of computers. The usual trick is to package it as a ‘Trojan horse’, a secretly malicious program that unsuspecting people will run. Robichaux (n.d.) suggests that people should think twice before running executable programs or attachments that they got from unknown sources. Someone who's trying to build an arsenal of DDoS clients doesn't want to waste time sending Trojans to well-educated security professionals. It is better to send them to people who will run the malicious code without a second thought, especially if they aren't likely to notice that their machine is infected.

Once a Trojan is activated, it registers its presence somewhere by sending TCP/IP packets to a well-known destination. These registration messages usually indicate the IP address of the zombied machine, and it may include some useful information about

bandwidth between the zombie and a selected target. Depending on the Trojan, it may attempt to disguise itself or stay hidden. The attacker can send a trigger command to one or all infected machines. The command instructs the Trojan to attack a designated target by sending a log of packets. The Trojan may also attempt to spread itself; many Trojans offer an attacker direct remote control of a compromised machine (Robichaux, n.d.).

Once the DDoS attack has been launched, it's hard to stop. Packets arriving at firewalls may be blocked there, but they may just as easily overwhelm the incoming side of the Internet connection. If the source addresses of these packets have not been spoofed, one should try to find and then contact the responsible parties and ask them to stop the agents. If the addresses are spoofed, one will have no way of knowing if they reflect the true source of the attack until you track down some of the alleged sources (Farrow, n.d.).

It is well known that an important goal for attackers is to hide the true sources of their attack traffic. One of the DoS attacks is called a distributed reflector denial of service attack, which aims to obscure the sources of attack traffic by using third parties to relay attack traffic to the victim. These innocent third parties are also called reflectors. Any machine that replies to an incoming packet can become a potential reflector. The DRDoS attack contains three stages. After the attacker has gained control of a certain number of “zombies,” instead of instructing the “zombies” to send attack traffic to the victims directly, the “zombies” are ordered to send to the third parties spoofed traffic with the victim’s IP address as the source IP address. DRDoS attacks have the ability to amplify the attack traffic, which makes the attack even more potent. In the following section, we use a real-world example to show the serious threat posed by DRDoS attacks (Peng, 2007, pp. 12-13).

Denial-of-service (DoS) attacks can affect any IP-based network service. The

impact of a DoS attack can range from mild service degradation to complete loss of service. There are several classes of DoS attacks. One type of attack in which packets can simply be flooded into or at the target network from multiple external sources is called a distributed denial-of-service (DDoS) attack. The DDoS attack can be represented using the following figure:

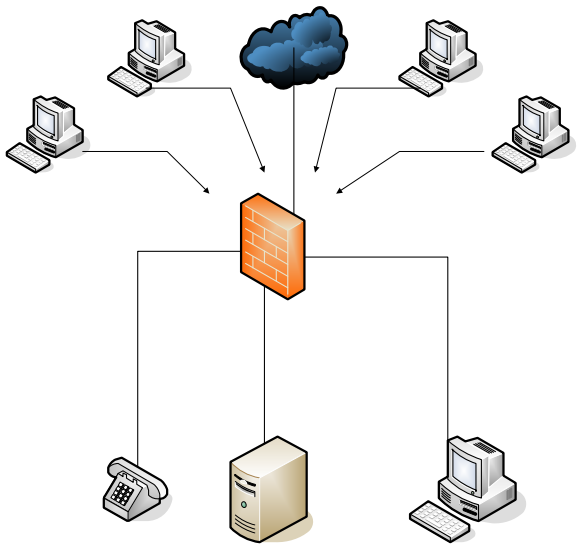

Figure 1A Distributed Denial-of-Service Attack

This figure shows that a network computer (e.g., a botnet) directs IP traffic at the interface of the firewall. Botnet are networks of software agents that often lie dormant until triggered to create harm, typically through DoS. The majority of malware has some botnet functions. That means that they allow for remote command and control via an obfuscated chain of authority. Botnets are not new, their use as an attack mechanism for DoS has been the biggest concern. Individual computers are initially infected by bot worms or super worms, each of which will connect back to an attacker when a new infection takes place. The attacker can use the infected computers to search out and infect other vulnerable hosts by exploiting vulnerabilities over the network or by sending virus attachment to random email recipients. The person who controls a large botnet is typically called a botherder. Law

enforcement agencies in different countries are starting to crack down on botherders, with some fairly high profile arrests. One such case is the arrest and prosecution of 21-year-old Christopher Maxwell, who controlled a botnet to launch DDoS attacks on the US Department of Defense, and California school district, and a Seattle hospital. As was noted by US Attorney's Office, "The creation and use of botnets is a growing problem in cyberspace. In simple terms, a botnet is created when a computer hacker executes a program over the World Wide Web that seeks out computers with a security weakness it can exploit. The program will then infect the computer with malicious code so that it becomes essentially a robot drone for the hacker (also known as a "botherder") controlling the botnet. The computer is ordered to connect to the communications channel where the botherder issues commands. Botnets can range in size from just a few computers to tens of thousands of computers doing the bidding of the botherder. (U.S. Attorney's Office, 2006,) "

As it is suggested by Williams et al. (2006), organizations need to implement effective DoS prevention mechanisms, and in many cases, this can come from an upstream provider. The threat from botnets is not only from DoS conditions; organizations should implement malicious code prevention mechanisms that include anti-spyware, personal firewalls and host-based intrusion prevention to protect the end points from initial infection and use as part of a botnet (p. 24).

The second large class of Denial of Service (DoS) conditions occurs when devices within the internal network are targeted by a flood of packets so that they fail taking out related parts of the infrastructure with them. Service disruption occurs to resource depletion-primarily bandwidth and CPU resource starvation. For example,

some IP telephones will stop working if they receive a UDP packet larger than 65534 bytes on port 5060.

The second class can be represented using the following picture (Porter, 2006, p. 243):

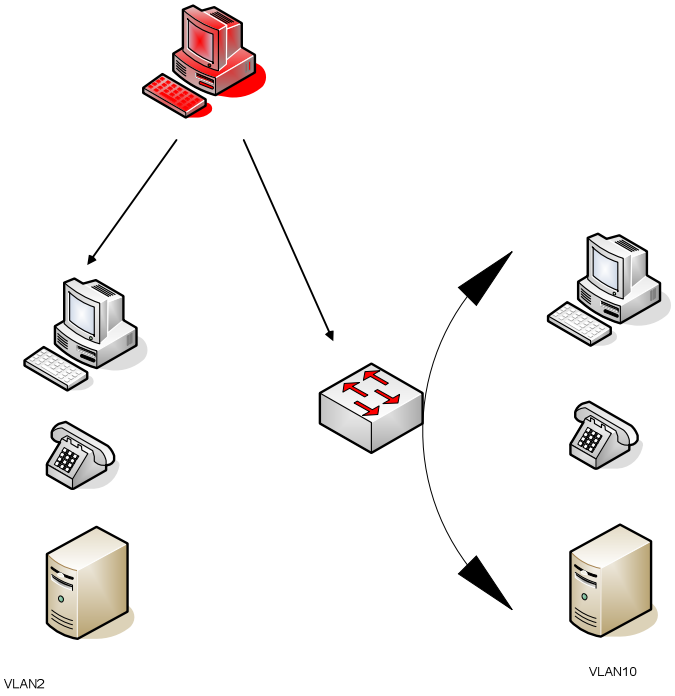

Figure 2: An Internal Denial-of-Service Attack

Neither integrity checks nor encryption can prevent these attacks. DoS or DDoS attacks are characterized simply by the volume of packets sent toward the victim computer; whether those packets are signed by a server, contain real or spoofed source IP addresses, or are encrypted with a fictitious key-none of these are relevant to the attack.

DoS attacks are difficult to defend against, and because VoIP is just another IP network service, it is just as susceptible to DoS attack as any other IP network services. Additionally, DoS attacks are particularly effective against services such as VoIP and other real-time services, because these services are most sensitive to adverse network

status. Viruses and worms are included in this category as they often cause DoS or DDoS due to the increased network traffic that they generate as part of their efforts to replicate and propagate (Porter, 2006, p. 243).

Consider first the internal DoS attack. The figure shows that VLAN 10 on the right is not affected by service disruption on the left in VLAN 2. By analyzing the Figure 2, we can see that this figure illustrated one critical weapon the security administrator has in thwarting DoS conditions – logical segregation of network domains in separate compartments. Each compartment can be configured to be relatively immune to the results of DoS in the others.

Also, point solutions will be also effective in limiting the consequences of DoS conditions. For example, because strong authentication is seldom used in VoIP environments, the message processing components must trust and process messages from possible attackers. The additional processing of bogus messages exhausts server resources and leads to a DoS. SIP or H.323 Registration Flooding is an example of this. In that case, message processing servers can mitigate this specific threat by limiting the number of registrations it will accept per minute for a particular address (and/or from a specific IP address). An Intrusion Prevention System (IPS) may be useful in fending off certain types of DoS attacks. These devices sit on the datapath and monitor passing traffic. When anomalous traffic is detected (either by matching against a database of attack signatures or by matching the results of an anomaly-detection algorithm) the IPS blocks the suspicious traffic. One problem with these devices-particularly in environments with high availability requirements-is that they sometimes block normal traffic, thus creating their own type of DoS.

Additionally, security administrators can minimize the chances of DoS by ensuring that IP telephones and servers are updated to the latest stable version and release. Typically, when a DoS warning is announced by bugtraq, the vendor quickly responds by fixing the offending software. Bugtraq is a mailing list hosted by Symantec SecurityFocus that serves as a vehicle for announcing new security vulnerabilities (SecurityFocus, 2007).

VoIP endpoints can be infected with new VoIP device or protocol-specific viruses. WinCE, PalmOS, SymbianOS, and POSIX-based softphones are especially vulnerable because they typically do not run antivirus software and have less robust operating systems. Several Symbian worms already have been detected in the wild. Infected VolP devices then create a new "weak link" vector for attacking other network resources. Compromised devices can be used to launch attacks against other systems in the same network, particularly if the compromised device is trusted (i.e., inside the firewall). Malicious programs installed by an attacker on compromised devices can capture user input, capture traffic, and relay user data over a "back channel" to the attacker. This is especially worrisome for softphone users (Porter, 2006, p. 245).

As was noted by Porter (2006), VoIP systems must meet stringent service availability requirements. He provides some example DoS threats can cause the VoIP service to be partially or entirely unavailable by preventing successful call placement (including emergency 911), disconnecting existing calls, or preventing use of related services like voicemail. Unfortunately this list is not but illustrates some attack scenarios.

Following Porter (2006) and Endler & Collier (2007), we will analyze these

attacks and countermeasures that can be helpful in preventing most of these attacks. The following types of attacks will be analyzed: flooding attacks, network availability attacks, and supporting infrastructure attacks.

Flooding Attacks

One of the preferred types of bandwidth flooding attacks is User Datagram Protocol (UDP) flooding because UDP source addresses can be easily spoofed by the attacker. Spoofing often allows an attacker the ability to manipulate trust relationships within an organization to bypass firewalls and other filter devices (for example, by crafting a DoS stream to appear as a DNS response over UDP port 53). Almost all SIP-capable devices support UDP, which makes it an effective choice of attack transport. Many VoIP devices and operating systems can be crippled if a raw UDP packet flood is aimed at the listening SIP port (5060) or even at random ports (Endler & Collier, 2007, p. 132).

An attacker can perform control packet flood; in other words, an attacker can flood VoIP servers or endpoints with unauthenticated call control packets, (e.g., H.323 GRQ, RRQ, URQ packets sent to UDP/1719).The attacker's intent is to deplete/exhaust device, system, or network resources to the extent that VoIP service is unusable. Any open administrative and maintenance port on call processing and VoIP-related servers can be a target for this DoS attack (Porter, 2006, p. 246).

The SYN flood attack exploits a vulnerability of the TCP three-way handshake, namely, that a server needs to allocate a large data structure for any incoming SYN packet regardless of its authenticity. During SYN flood attacks, the attacker sends SYN packets with source IP addresses that do not exist or are not in use. During the threeway handshake, when the server puts the request information into the memory stack, it will wait for the

confirmation from the client that sends the request. While the request is waiting to be confirmed, it will remain in the memory stack. Since the source IP addresses used in SYN flood attacks can be nonexistent, the server will not receive confirmation packets for requests created by the SYN flood attack. Each half-open connection will remain on the memory stack until it times out. More and more requests will accumulate and fill up the memory stack. Therefore, no new request, including legitimate requests, can be processed and the services of the system are disabled. Generally, the space for the memory stack allocated by the operating system is small, and even a small scale SYN flood attack can be disruptive. On the other hand, SYN floods can be also launched from compromised machines using genuine source IP addresses given these compromised machines are configured to ignore the SYN/ACK packets from the target (Peng, 2007, p 9).

Another attack known as IP Phone Flood DoS occurs when an attacker sends a very large volume of call data toward a single VoIP endpoint to exhaust that device's CPU, bandwidth, TCP sessions, and so on. Interactive voice response systems, telephony gateways, conferencing servers, and voicemail systems are able to generate more call data than a single endpoint can handle and so could be leveraged to flood an endpoint.

It is well known that the Internet Control Message Protocol (ICMP) is typically allowed through most firewalls and routers for diagnostic purposes (ping, traceroute, and so on). However, ICMP also provides the capability to send large amounts of ICMP traffic through the pipe as well. A more sinister use of ICMP traffic involves spoofing the source IP address and pinging broadcast addresses of a variety of networks that allow IP directed broadcasts (smurf attack). A smurf attack involves a flood of legitimate ICMP responses

from these networks to the victim who was spoofed. By overwhelming the victim's network bandwidth with spurious ICMP responses, most legitimate Internet applications will sputter under the attack (Endler & Collier, 2007, p. 133). As was noted by CERT (2000), “Both the intermediary and victim of this attack may suffer degraded network performance both on their internal networks or on their connection to the Internet. Performance may be degraded to the point that the network cannot be used. A significant enough stream of traffic can cause serious performance degradation for small and mid-level ISPs that supply service to the intermediaries or victims. Larger ISPs may see backbone degradation and peering saturation”.

These types of floods are also known as application flooding attacks. An established connection flood is an evolution of the TCP SYN flood attack, but a full connection is made to the targeted service or device and then quickly torn down. This attack may go even further to make an actual application request to try to overwhelm the target. In the case of a target web server, this could take the form of thousands of botnet zombie hosts hammering away at a web server with legitimate GET requests. For a SIP PBX, it could take the form of thousands of REGISTER/INVITE /BYE requests received at the same time, overwhelming the incoming connection queue. Or conversely for a SIP client, this attack could take the form of thousands of bogus incoming calls rendering your phone useless (Endler & Collier, 2007, p. 133).

Another attack scenario is oversubscription which means the applications’ bandwidth have exceeded the network capabilities. This can occur from any number of flooding DoS attacks or poor QoS management. However, worm and virus outbreaks within the network can easily consume all available bandwidth as a side effect of scanning for other vulnerable

hosts to infect. Even just a few worm-infected machines within an organization can clog all available bandwidth with the spurious traffic spewing from the victims (Endler & Collier, 2007, p. 133).

Endler & Collier (2007) consider also a much more advanced type of flooding attack that involves subverting the quality of service mechanisms within a network in order to degrade VoIP applications. Assuming that an organization's QoS technologies are configured to prioritize RTP traffic over all other traffic, this normally means that a simple internal flooding attack would be mostly ineffective. However, if an attacker can flood a phone, proxy, or PBX with legitimate looking RTP traffic, the QoS mechanisms would be unable to determine which conversations are bogus and which ones are real and deserve network priority. Depending on the QoS mechanism being applied, it may also be necessary for the attacker to know two actively talking parties in order to spoof the proper ports and sequence numbers (p. 134). According to Porter (2006), an attacker can modify non-VoIP-specific protocol control information fields in VoIP data packets to and from endpoints to degrade or deny voice service. For example, if an attacker were to change 802.1Q VLAN tag or IP packet ToS bits, either as a man-in-the-middle or by compromising endpoint device configuration, the attacker could disrupt the quality of service "engineered" for a VoIP network. By subordinating voice traffic to data traffic, for example, the attacker might substantially delay delivery of voice packets (p. 246).

Flooding Attack Countermeasures

Endler & Collier (2007) mention a number of countermeasures that can be effective in preventing the flooding attacks. They advise that the company adopts a defense-in-depth approach to protecting its VoIP-dependent devices, network components, and servers (pp.

134 – 136). They suggest considering the following countermeasures: differentiated services, hardening the network perimeter, hardening VoIP phones and severs, and use of VLANs (Endler & Collier, 2007, pp. 134 - 136).

The most common approach is called DiffServ for differentiated services. Network packets are tagged according to their priority based on the type of application they are. Network devices are then able to manage how they deliver and prioritize these incoming packets. The packet priorities can be tagged in a couple of ways. The differentiated services code point (DSCP) is applied at the IP layer. Equally as effective and more commonly used at the MAC layer are IEEE standards 802.1P and 802.1Q. 802.1P defines a scheme for prioritizing network traffic, and the 802.1Q (VLAN) header contains the 802.1P field, so VLANs are needed to implement QoS with 802.1P.

Another solution would be considering a number of vendors that sell appliances that can be deployed at the perimeter as well as at the core of the network. These appliances are able to detect and either block or rate-limit an active DoS or DDoS attack.

Hardening of the network perimeter is another approach. Much of the network equipment can be configured to resist the most basic DoS and DDoS techniques that attackers use. Cisco's analysts suggest the following strategy to defend DoS and DDoS attacks (Cisco, 2007):

1. Use the ip_verify_unicast_reverse_path interface command on the input interface on the router at the upstream end of the connection. This feature examines each packet received as input on that interface. If the source IP address does not have a route in the CEF tables that points back to the same interface on which the packet arrived, the router drops the packet.

2. Filter all RFC-1918 address space using Access Control Lists (ACLs).
3. Apply ingress and egress filtering using ACLs.
4. Use CAR to rate limit ICMP packets.
5. Configure rate limiting for SYN packets.

Endler & Collier (2007) suggest also hardening VoIP phones and servers; this approach includes some basic recommendations regardless of the particular vendor: the suggest changeing the default passwords and remove all guest and nonauthenticated accounts, disabling unnecessary services (telnet, HTTP, and so on), ensuring the device or operation system is up-to-date with the latest patches and/ or firmware, and developing a strategy for keeping up-to-date with patches (p. 136).

Finally, Virtual LANs (VLANs) can be used to segment network domains logically on the same physical switch. Many switches support the ability to create several VLANs on the same switch, which is a helpful component for protecting the core VoIP servers and devices against the typical DoS traffic threats that plague most traditional data networks, such as worm and viruses. Endler & Collier (2007) argue that it is not feasible to segment the entire VoIP infrastructure from the traditional data network, in part because of many shared dependencies on the underlying infrastructure such as DNS, DHCP, IFTP. Softphone VoIP applications that run on a user's desktop also make it challenging to separate your VoIP applications logically from the data network because a user's desktop typically needs to able to reach most of the network resources on the traditional data network (p. 136).

Network Availability Attacks and Countermeasures.

Another class of network DoS attacks are network availability attacks. These attacks involve an attacker trying to crash the targeted network device or underlying operating

system. Such attacks include stress testing with malformed packets (fuzzing), packet fragmentation leveraging vulnerabilities in the underlying application or operating system. Consider each of them and countermeasures that can be used in preventing and defending such attacks.

The TCP/IP stack implementations in different versions of Windows are unique enough that they can be differentiated in their responses to network traffic. The point is that all vendors implement their device IP stacks in various ways, in some cases varied across different versions of the same product. Some implementations are more robust than others and are able to handle a variety of error conditions. Most of the time developers don't take into account network input that deviates from "normal" traffic, which in some cases can lead to the device or application crashing upon processing it. To adequately test the robustness of a network stack implementation, it is useful to devise as many ‘evil’ test cases as possible that poke the bound of the support protocol. Bugs and DoS vulnerabilities can be found by crafting different types of packets for that protocol, containing data that pushes the protocol's specifications to the breaking point, otherwise known as fuzzing (Endler & Collier, 2007, pp. 136-137). One of the fuzzing tools is IP Stack Integrity Checker (ISIC). It is a suite of utilities to exercise the stability of an IP Stack and its component stacks (TCP, UDP, ICMP et. al.) It generates piles of pseudo random packets of the target protocol. The packets are then sent against the target machine to either penetrate its firewall rules or find bugs in the IP stack. ISIC also contains a utility generate raw ether frames to examine hardware implementations (PacketFactory, 2006).

Another way of attacking the networks is packet fragmentation. By fragmenting TCP and UDP packets in unique ways, it is possible to render useless many operating systems and

VoIP devices through resource consumption. There are many variations of fragmentation attacks; some of the most popular exploits include teardrop, opentear, nestea, jolt, boink, etc (Endler & Collier, 2007, p. 137). One of the examples of well-known fragmentation based vulnerabilities is ISS RealSecure 3.2.x Fragmented SYN Packets DoS Vulnerability. ISS RealSecure 3.2.x can be disabled remotely via fragmented packets with the SYN flag set. On NT, after crashing the service will restart, and generates an Application Log event. If the packets are continuously resent, detection is effectively halted while the service repeatedly restarts. On Solaris, the process crashes, all detection stops, and a report is generated to the console. Also, on Solaris it is possible to crash the process with a flood of unfragmented packets if certain flags (in addition to SYN) are set (SecurityFocus, 2007).

The other major category of DoS attacks on VoIP infrastructure involves an attacker leveraging vulnerabilities in the underlying application or operating system, which can lead to a system crash or overwhelming resource consumption. One of the examples of such attacks is a malicious self-replicating program known as the "Code Red" worm. It is targeted at systems running the Microsoft Internet Information Server (IIS). Several Cisco products are installed or provided on targeted systems. Additionally, the behavior of the worm can cause problems for other network devices. According to Cisco (2001), the following Cisco products are vulnerable because they run affected versions of Microsoft IIS: Cisco CallManager, Cisco Unity Server, Cisco uOne etc.

What kind of countermeasures can be suggested for preventing of network availability attacks? First of all, all the countermeasures listed in before can be applied here as well as to ensure network availability. Additional to these measures one more countermeasure can be added here – Network based Intrusion Prevention Systems (NIPS).

NIPS monitor and anlyze network traffic to detect intrusion. NIPS have a management interface that can configure rules. NIPS throws alarms when encountering suspicious activities. Optionally NIPS can be configured to perform actions such as resetting data connections, instructing router to deny future traffic from an offending host, and so on (Davidson et al. 2007, p. 233). NIPS also buy IT admins time to patch enterprise-wide by providing a sort of virtual patch for any exploits that may emerge soon after a new vulnerability is discovered in the public domain (Endler & Collier, 2007, p. 139).

Supporting Infrastructure Attacks and Countermeasures

An infrastructure attack aims to disable the services of critical components of the Internet. The result of an infrastructure attack is potentially catastrophic as the whole Internet can be affected (Peng, 2007, p. 14). Basic VoIP architecture elements such as phones, servers, and PBXs rely heavily on the supporting network infrastructure (DHCP, DNS, TFTP). If one of those support elements is attacked or taken offline, a side effect may be that VoIP applications are crippled or severely limited in usability. Many VoIP phones are configured, by default, to request an IP address dynamically every time they are turned on or rebooted. If the DHCP server is unavailable at the time they boot up, or the maximum number of IP addresses have already been allocated by that DHCP server, then the phone might not be usable on the network. DHCP is a broadcast protocol which means that REQUEST messages from DHCP clients such as IF phones are seen by all devices on the local network, but are not forwarded to additional subnetworks. If the DHCP server is present on a different network, DHCP forwarding must be enabled on the router. DHCP forwarding converts the broadcast message into a unicast message and then forwards the message to the configured DHCP server. DHCP forwarding is offered on most routers and layer 3 switches

(Endler & Collier, 2007, pp. 141-142).

There are some DHCP exhaustion countermeasures. DHCP servers can be configured so that not to lease addresses to unknown MAC addresses and also to untrusted network segments. According to Cisco (n. d.), DHCP snooping is a DHCP security feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch (p. 1).

DNS cache poisoning attacks involve an attacker tricking a DNS server into believing the veracity of a fake DNS response. The purpose of this type of attack is to redirect the victims dependent on that DNS server to other addresses; this type of attack has traditionally been used in phishing schemes to redirect a user trying to surf to their banking site to a fake site owned by the hacker. A DNS SRV record assists SIP phone dialing in much the same way that MX records help map email addresses to the appropriate mail servers. Some sites are beginning to use DNS SRV records to forward certain SIP requests to particular proxy

addresses, potentially outside of the organization. This has particularly dangerous implications if an attacker can poison these resource listings to redirect all calls going to your domain to her external proxy (Porter, 2006, p. 249; Endler & Collier, 2007, pp. 146-147).

According to Householder et al. (2002), name servers exposed to the Internet are subject to a wide variety of attacks (p. 1):

- attacks against the name server software may allow an intruder to compromise the server and take control of the host. This often leads to further compromise of the network;
- denial of service attacks, even one directed at a single DNS server, may affect an entire network by preventing users from translating hostnames into the necessary IP addresses;
- spoofing attacks that try to induce your name server to cache false resource records, and could lead unsuspecting users to unsavory sites;
- information leakage from a seemingly innocent zone transfer could expose internal network topology information that can be used to plan further attacks;
- a name server could even be an unwitting participant in attacks on other sites.

DNS cache poisoning is almost entirely avoidable by configuring the DNS server properly. This includes forcing it to scrutinize any forwarded DNS response information passed by other non-authoritative servers and dropping any DNS response records passed back that do not relate to the original query. Most recent DNS servers are immune to this attack in their default configurations (Householder et al., 2002, pp. 2-5; Peng et al., p. 13).

Summary, Conclusions, Recommendation

As we saw in the Chapter 4, DoS and DDoS attacks are the most difficult VoIP

related threats to defend against. There are a plethora of different types of DoS and DDoS attacks that can cripple the company's VoIP environment. Not only the company needs to protect its VoIP devices and services; it needs to protect data network and supporting infrastructure.

There are a number of scenarios that can be vulnerable, can damage the whole computer system of a company and thereby interrupt business process of the company. The packet switching nature of data networks allows multiple connections to share the same transport medium. That means that unlike telephones in circuit-switched networks, an IP terminal endpoint can receive and potentially participate in multiple calls at once. An endpoint can be used to amplify attacks.

We considered and analyzed the following types of attacks: flooding attacks, network availability attacks, and supporting infrastructure attacks. For each type of attacks there are countermeasures. It is important to know what countermeasures are good and in which situations. This can help develop business continuity plan as well as disaster recovery plan that can help not only to fix the problem, but also prevent most of them. The chapter should have practical implications for the company, although it is not possible to deploy security technologies to counter every possible threat. The company's networking analysts should be able to identify most of the threats the company can experience, assess the security risks that are specific to the company's network and address the highest priority risks first. That means not all DoS/DDoS attack should be considered, but those that are very risky for the company.

What is the practical benefit of conducted research? The practical benefit is that the analysts of the company should design and document risk assessment, an

operational plan, outlining critical DoS attacks, in order of priority. This document should guide the security technologies that are deployed and prioritize future implementations. The operational plan should also include and incident response plan outlining specific initial steps to take in case of a security breach. The plan should document internal policies such as password policies, access control, monitoring strategies, and be communicated to the key people who will be implementing, enforcing, or resolving these security issues.

As one of the practical recommendations that can be made is efficient allocation of the resources such as bandwidth to accommodate the maximum number of callers. This property can be violated by attackers who aggressively and abusively obtain an unnecessarily large amount of resources. Alternatively, the attacker simply can flood the network with large number of packets so that resources are unavailable to all other callers.

In addition, viruses and worms create DoS conditions due to the network traffic generated by these agents as they replicate and seek out other hosts to infect. These agents are proven to wreak havoc with even relatively well-secured data networks. VoIP networks, by their nature, are exquisitely sensitive to these types of attacks.

Remedies for DoS can be the following: include logical network partitioning at layers 2 and 3, stateful firewalls with application inspection capabilities, policy enforcement to limit flooded packets, and out-of-band management. Out-of-band management is required so that in the event of a DoS event, system administrators are still able to monitor the network and respond to additional events.

Security is an important consideration in designing and implementing VoIP

services. It encompasses almost every aspect of a network from Layer 2 devices to firewalls and Certificate Authorities. As we saw, a wide range of security technology exist that can be helpful for a company to protect, prevent and defend its VoIP environment. Assessing DoS, can help generate new knowledge and develop a knowledge base for a company to make better decision in securing its VoIP environment.

Strong security for any VoIP applications requires companies to analyze the security readiness of any application, networking device, critical infrastructure and end-user devise. Companies should test security infrastructure to make sure the company is protected. On the other side, companies can implement statistical or mathematical models to estimate how risky the attacks are.

For example, propagation of worms can be modeled well with the epidemic model describing the spread of infectious diseases. Epidemic model gives the average infection rate in a population where the infected individuals contact uninfected individuals with the average contact rate (Molsa, 2005, p. 810). The parameters can be estimated or calibrated given historical data, and can be used for practical estimations.

The analysis of the threats described above can help in developing, improving and refining risk assessment matrix. It is possible to create matrix of probabilities of asset/risks based on the available data or from approximate estimation. In this case various types of DoS/DDoS can be considered, and probabilities can be chosen based on statistical analysis of attacks data. Modeling can help investigate ‘what-if’ scenarios of possible DoS/DDoS attacks and how countermeasures would work to prevent them. The model can indicate if specific countermeasure is effective or not.

The first step would be to develop a model, and use it in calibrating of the model parameters. To calibrate the model parameters, it is important to conduct statistical analysis. Unfortunately, not all data can be available, but some assumptions can be made about distribution of the malicious DoS/DDoS attacks. This distribution can be used in simulation of possible attacks and testing how the company could respond to such attacks. Testing could help to analyze existing business continuity and disaster recovery plans that can then be improved based on the results of testing. Of course, it would be great if there is statistical data available. Additional research may be required for better estimation of probabilities.

Another approach is to assume, for example, that DoS/DDoS attacks are occurring according to the Poisson process. Statistical methods can help estimate the intensity of the process for running Monte Carlo simulation and assessing possible losses the company can experience. The result of such simulations will be a loss distribution of the company from the attacks VoIP and networking environment. Loss distributions can be estimated for each type of DoS as well for all types for specific time period.

Another problem is to estimate correlation different types of DoS and DDoS attacks. Statistical methods can help in estimation of the correlations. These correlations can be useful in estimation of the total loss distribution of the company. Correlation and loss distribution usually change over time, and it can incur additional problems in estimation of losses. Although methodology can be difficult to implement, it can be valuable for the company to estimate possible losses due to DoS/DDoS attacks that can affect the company's business and its operations.

Reference

CERT. (2000, March 13). Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. Retrieved November 25, 2007, from http://www.cert.org/advisories/CA-1998-01.html

Cisco. (2001, November 1). Cisco Security Advisory: "Code Red" Worm - Customer Impact. Retrieved November 23, 2007, from http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml

Cisco. (2007, July 11). Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks. Retrieved November 22, 2007, from http://www.cisco.com/warp/public/707/newsflash.html

Cisco. (n. d.). Configuring DHCP Snooping. Retrieved November 24, 2007, from http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/13ew/configuration/guide/dhcp.pdf

Davidson, J., Peters, J., Bhatia, M., Kalidindi, S. & Mukherjee, S. (2007). Voice over IP Fundamentals. 2nd Edition. Indianapolis, IN: Cisco Press.

Endler, D. & Collier, M. (2007). Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. New York, NY: McGraw-Hill.

Farrow, R. (n.d.). Distributed Denial of Service Attacks. Retrieved November 16, 2007, form http://www.microsoft.com/technet/archive/community/columns/security/netdef/denialof.mspx?mfr=true

FitzGerald, J. & Dennis, A. (2007). Business Data Communications and Networking. 9th Edition. Hoboken, NJ: John Wiley & Sons.

Gelenbe, E. (2006, September 11). Users and services in intelligent networks. IET Proceedings Intelligent Transport Systems, 153(3), 213-220.

Hersent, O., Petit, J.-P. & Curle, D. (2005). IP Telephony. Deploying Voice-over-IP Protocols. West Sussex, England: John Wiley & Sons.

Householder, A., King, B. & Silva, K. (2002, August). Securing an Internet Name Server. CERT Coordination Center. Retrieved November 22, 2007, from http://www.cert.org/archive/pdf/dns.pdf

Hovav, A., & D'Arcy, J. (2003, Fall). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. Risk Management & Insurance Review, 6(2), 97-121.

Kurapati, K. (2007, February 1). Protect against VoIP attacks. Communications News, 44(2), 40-41.

Miller, M.A. (2002). Voice over IP Technologies. Building the Converged Network. New York, NY: M&T Books.

Mir, N.F. (2007). Computer and Communication Networks. Upper Saddle River, NJ: Pearson Education Inc.

Mölsä, J. (2005). Mitigating denial of service attacks: A tutorial. Journal of Computer Security, 13(6), 807-837.

Narayanaswarny, K. (2002, May 1). ISPs and denial of service attacks. Information Systems Security, 11(2), 38-46.

Neumann, P. (2000, April). Denial-of-Service Attacks. Communications of the ACM, 43(4), 136-136.

Orans, L. (2005, June 25). A Taxonomy for Security Threats to VoIP Environment. Gartner Research.

PacketFactory. (2006). ISIC -- IP Stack Integrity Checker. Retrieved November 23, 2007, from http://www.packetfactory.net/Projects/ISIC/

Peng, T., Leckie, C., & Ramamohanarao, K. (2007, April). Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. ACM Computing Surveys, 39(1), 1-42.

Porter, T. (2006). Practical VoIP Security. Rockland, MA: Syngress Publishing, Inc.

Robb, D. (2005, December 1). Defending against viruses, worms and DoS attacks. Business Communications Review, 35(12), 24-27.

Robichaux, P. (n.d.). Distributed Denial-of-Service Attacks and You. Retrieved November 16, 2007, from http://www.microsoft.com/technet/archive/security/bestprac/ddosatku.mspx?mfr=true

SecurityFocus. (2007) Bugtraq. Retrieved November 21, 2007 from: http://www.securityfocus.com/archive/1

SecurityFocus. (2007). ISS RealSecure 3.2.x Fragmented SYN Packets DoS Vulnerability. Retrieved November 23, 2007, from http://www.securityfocus.com/bid/1597/discuss

Solomon, M.G. & Chapple, M. (2005). Information Security Illuminated. Jones and Bartlett Publishers: Sudbury, MA.

U.S. Attorney's Office. (2006, May 4). California Man Pleads Guilty in "Botnet" Attack that Impacted Seattle Hospital and Defense Department. Retrieved November 21, 2007, from http://www.usdoj.gov/usao/waw/press/2006/may/maxwell.htm

Walters, R. (2001, July 1). Top 10 ways to prevent denial of service attacks. Information Systems Security, 10(3), 71-72.

Williams, A.T., Hallawell, A. Mogull, R., Pescatore, J., MacDonald, N., Girard, J., Litan, A., Orans, L., Wheatman, V., Allan, A., Firstbrook, P., Young, G., Heiser, J. & Feiman, J. (2006, September 13). Hype Cycle for Cyberthreats, 2006. Gartner Research.

Yocom, B., Taylor, J., & Poletti-Metzel, D. (2004, April 1). Small lP-PBXs: another close race. Business Communications Review, 34(4), 36.

Yocorn, B., Brown, K., & Molle, C. (2002, April 1). Beyond basic VPNs. Business Communications Review, 32(4), 22-29.