WHITE PAPER

TEXAS INSTRUMENTS

Safeguards Against Denial of Service Attacks for IP Phones

By Amritpal Mundra
Design Engineer, DSP Systems
amrit@ti.com

By Maneesh Soni
Design Engineer, DSP Systems
msoni@ti.com

Communications
Infrastructure
and Voice Group

Denial of Service (DoS) attacks on computers and infrastructure communications systems have been reported for a number of years, but the accelerated deployment of Voice over IP (VoIP) services both in homes and businesses increases significantly the susceptibility of residential subscribers and enterprise users to this type of security breach.

The stringent time-sensitivity of voice services makes VoIP communications particularly vulnerable to DoS attacks. Often, the introduction of even the slightest amount of delay or latency in a VoIP communication channel can decrease voice quality significantly, leading to subscriber dissatisfaction and discontinuance of service or to complete disruption of VoIP service.

Introduction

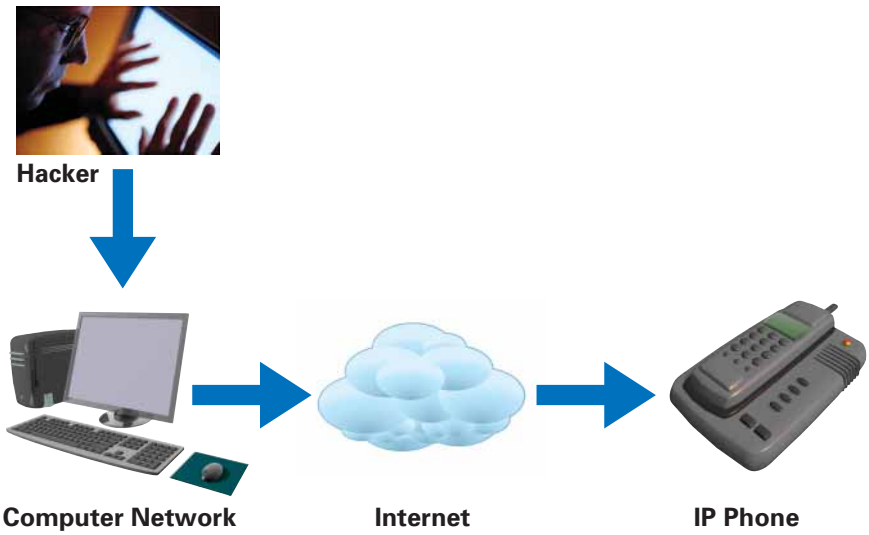
Because an IP phone is a device similar to computers, servers or gateways on an IP network, they can be victimized by malformed packets or packet flooding in a DoS attack, impairing or completely disrupting the ability of the phone to provide the level of service expected by the subscriber or user. Once security mechanisms are compromised by a DoS attack, more serious security breaches such as fraud, service abuse or data theft could follow. The quality of a VoIP service and its reliability depends on quickly an attack is recognized and subsequently isolating the DoS traffic at the point of entry into a device such as an IP phone.

This white paper describes how DoS attacks on IP phones and other customer premise equipment (CPE) such as residential gateways take place. In addition, the critical importance of deploying robust defenses against these attacks is explained and several defense strategies are proposed.

Concept

DoS attacks refer to lapses in security when an IP phone is occupied by processing redundant data sent by a malicious node at an extremely high rate. This pointless processing consumes system resources and CPU time, leading to the phone's inability to sufficiently handle legitimate service requests or to its providing poor voice quality.

For instance, an IP phone can be attacked by sending TCP SYN packets at a high rate. The targeted phone responds to these packets by allocating a block of memory to receive the dubious information through the IP communications connection. In this sort of DoS attack, the hacker sends the SYN packets with altered parameters at a high and the phone ends up exhausting all of its available memory. The result is that the phone is not able to process legitimate requests for service, effectively denying what could be very critical VoIP services. The picture becomes even more threatening with distributed denial of service (DDoS) attacks, where the attacker uses multiple computers to launch a coordinated DoS attack against a targeted device. In this case, the attacker is able to multiply the effectiveness of the DoS attack significantly by channeling the resources of multiple and often unwitting accomplice computers to serve as attack platforms.

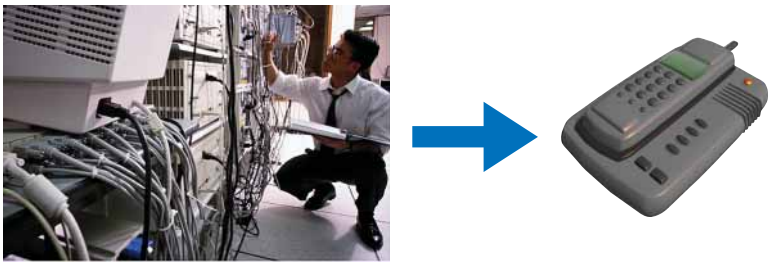


An IP phone could also be attacked by a ping response storm, during which the hacker posts a broadcast ping request packet spoofing the return path of the targeted phone. This causes a high ingress surge of ping response packets at the targeted phone, occupying all of its resources with processing the storm requests.

Another type of DoS attack preys on the vulnerability of protocol software. The attacker uses sophisticated tools and data patterns to create data packets intended to exploit loopholes, thereby paralyzing the resources of the targeted phone. There is also a DoS attack known as configuration altering attack, where the attacker alters the configuration of the VoIP system by editing the routing tables. This is intended to either misdirect the data packets, or create a scenario where the system does not work with the VoIP call manager, thereby leading to denial of service. As the scope and reach of the Internet grows, so does the risk of being the victim of a DoS attack, especially for an application like voice which requires consistent and reliable bandwidth for a quality call.

Friendly Fire

A "friendly fire" DoS attack occurs when an IP phone becomes the victim of an unintended attack. Friendly fire typically happens when high volumes of protocol-learning packets are exchanged among various nodes on a certain network. A centrally located device becomes exposed to the heavy traffic, depleting its resources because it must process these useless chunks of data. This problem is often caused by mismanagement of network resources by a system administrator.



Heavy Traffic Over Ethernet **IP Phone**

Safeguards

Ships are safe in harbors, but sitting in a harbor is not what ships are built to do. For an IP phone to provide high quality voice communications, it is necessary to adopt strategies to overcome DoS attacks.

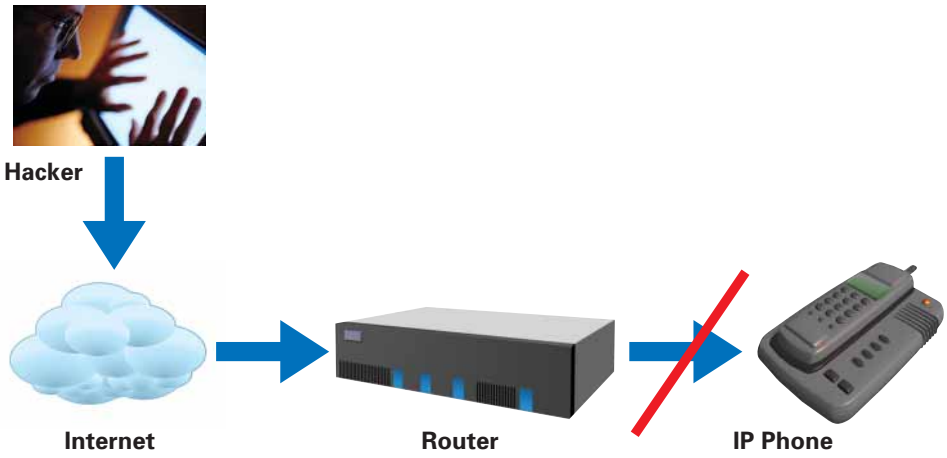
Router-Based DoS Firewalls

In this scenario, an IP phone is plugged into a trusted network which is well segregated from the general traffic on the Internet by a firewall installed on a router and equipped with DoS handling tools. The firewall absorbs the DoS attacks, protecting the IP phone from an attack originating from the network. However, this strategy works best only in small networks where all nodes are trusted nodes. Moreover, the cost of deployment increases significantly if a firewall must be installed in every router.

DoS Defense-enabled IP Phones

As local area networks (LAN) increase in deployment, especially for enterprises, universities and other large organizations where a large number of nodes share the same network, it becomes impractical to guarantee the safety of an IP phone since many DoS attacks are generated within a supposedly closed network with a spoofed network address.

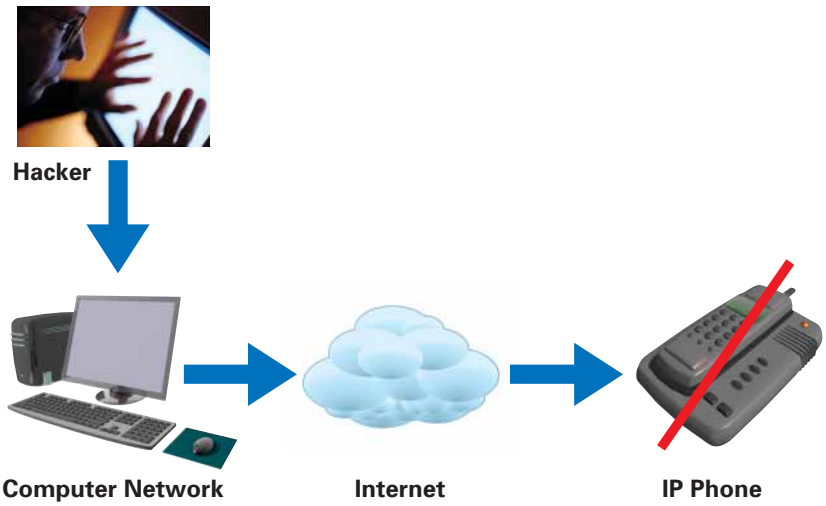
This leads to the conclusion that the best defense against a DoS attack on a particular IP phone must be based on that phone itself. That is, the IP phone should inherently identify and resist DoS attacks without compromising its voice quality.



This strategy gives service providers and private enterprises the flexibility to simply connect an IP phone to a LAN or directly to the Internet without additional security protection other than the protection provided by the phone itself. Phone-based DoS security will ultimately reduce the overall cost of DoS safeguards significantly.

One example of DoS security built into IP phones could be a section of hardware logic which would inspect incoming packets to the phone at wire-rate. This hardware would identify and isolate incoming traffic streams that match certain known DoS attack patterns that are defined in a set of rules. These rules can be automatically updated or altered by a secure supervisory host server to the current state-of-the-art firewall technology.

If the IP phone detects a DoS attack pattern, the suspected packets can be dropped and the event logged for further analysis. This offline analysis of blocked packets can trigger stronger defense mechanisms against the types of attack that have been identified. For example, if an IP phone's DoS protection identifies that a certain IP address is consistently the source of threatening packets, all traffic originating from that IP address could be blocked until such time that the packets coming from this IP address can be trusted.



Denial of Service Attacks

	DoS Attack	OSI Layer	Description
1	ICMP flood	2	High incoming rate of ICMP packets
2	ARP spoof	2	ARP reply received for no ARP request, leads to overwriting of valid ARP entry
3	Land	3	Source and destination IP address of packet is same
4	Fragment overrun	3	Fragmented IP packet whose fragment payload exceeds maximum IP total length
5	Jolt2	3	Actual length received is less than total length stated in IP packet
6	Tiny fragment	3	Fragment packet having extremely less data
7	Illegal IP options	3	Malformed IP option(s) exceeding IP header space
8	Fragmented ICMP packet	3	Fragmented ICMP packet
9	Illegal fragment offset	3	Fragment packet having offset as all "1"s
10	Short ICMP packet	3	Packet having IP total length less than ICMP header
11	Ss ping	3	Fragmented ICMP packet, having fragment offset overlapping
12	Bonk	3	UDP fragmented packets at high rate having offset overlapping at different byte boundaries
13	Illegal TCP options	4	TCP options are malformed or exceed the TCP length space
14	SYN flood	4	High rate of TCP SYN packets
15	Null scan	4	TCP packet with no flag set
16	Short TCP packet	4	Packet having IP total length less than TCP header
17	FIN ACK	4	TCP packet with Finish and Ack flags set
18	SYN fragment	4	Fragmented TCP SYN packet
19	Urgent offset	4	TCP urgent offset pointing data out of current payload
20	Short UDP header	4	Packet having IP total length less than UDP header
21	TCP SYN FIN	4	TCP packet with SYN and Finish flags set
22	Xmas scan	4	TCP packet bearing sequence number as zero with finish and urgent flags set

Conclusion

It is essential to safeguard IP phones from DoS attacks to ensure reliable and seamless voice connections, with a high level of voice quality. For most homes and businesses, telephone voice communications is the single most indispensable form of communications available to residents and employees. In the case of residential subscribers, human safety sometimes depends on the reliability of the home's telephones. For businesses, a lapse in telephone service, no matter how temporary it may be, is capable of placing the success of the enterprise in jeopardy.

Previously limited to web sites and computers on the Internet, DoS attacks can now target a particular IP phone or a group of IP phones because these devices rely on the Internet for connectivity just as computers, servers and websites do. As a result, it is critically important that users and service providers draw a line of defense around their IP phones so they can fend off any DoS attack in the future. The most effective way of erecting this defense is to begin at the IP phone itself. Router-based and other sorts of DoS defense mechanisms that are external to the IP phone are costly and ultimately, not as effective as instrument-based defenses. Given the advanced technology and processing capabilities now being built into IP phones, it is completely feasible that IP phones can be equipped with adaptive defense mechanisms that would be able to counter new DoS attack strategies while ensuring high quality voice service.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DSP	dsp.ti.com	Broadband	www.ti.com/broadband
Interface	interface.ti.com	Digital Control	www.ti.com/digitalcontrol
Logic	logic.ti.com	Military	www.ti.com/military
Power Mgmt	power.ti.com	Optical Networking	www.ti.com/opticalnetwork
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
Low Power Wireless	www.ti.com/lpw	Telephony	www.ti.com/telephony
		Video & Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments
Post Office Box 655303 Dallas, Texas 75265