

Voice Over IP (VoIP) Denial of Service (DoS)

By Mark Collier
Chief Technology Officer
SecureLogix Corporation
mark.collier@securelogix.com

Introduction

Denial of Service (DoS) is an issue for any IP network-based service, including electronic commerce, email, Domain Name Service (DNS), and Voice over IP (VoIP). DoS can take various forms, but generally involves an attack that prevents users from effectively using the targeted service. For example, there have been DoS attacks on well-known ecommerce web sites that prevented users from using the service. DoS can result in a complete loss of service or degradation to the point where users will not use the service. DoS is one of the most serious types of IP network-based attacks—and one of the most difficult to defend against. Because VoIP is another service on the IP network, it is just as susceptible to DoS as other IP network services. Plus, because VoIP is a real-time service, it is even more susceptible to DoS attacks that impact delivery of audio.

Types of DoS

There are many ways to create a service disruption on a VoIP network. These can be as simple as turning off power to a server, disabling a switch or router, disconnecting cables, turning off an IP phone, or logging in as an administrator and disabling services. These attacks can be addressed with a combination of good physical security and strong authentication for administrative access.

Enterprise VoIP, as with any network-based service, must communicate with other components on the Local Area Network (LAN) and possibly an untrusted network such as the Internet. For example, IP phones must be able to exchange signaling packets with an IP PBX in order to set up calls. IP phones must be able to exchange audio packets with other IP phones to allow calls to take place. Because legitimate users need to access these services over the network, it is also possible for attackers to target these same components for DoS attacks.

There are several different basic types of DoS that occur over the IP network:

- Implementation flaw DoS – occurs when an attacker sends a carefully crafted packet or sequence of packets that exploit an implementation flaw in a VoIP component, such as an IP PBX. The packet may be very long, syntactically incorrect, or otherwise malformed in a way that causes the target component to fail because it wasn't implemented robustly enough to handle unexpected packets. With the rush to implement new VoIP systems, features and standards, implementation flaws are common.
- Flood DoS – occurs when a large number of normal packets are sent to a target VoIP component. With this form of DoS, the target system is so busy processing packets from the attack, that it will not be able to process legitimate packets. Legitimate packets will either be ignored or processed so slowly that the VoIP service is unusable. One variant of this sort of attack is one where the flood packets cause the target system to allocate resources or consume processing power waiting or polling for a response that will never be sent. Another variant is a Distributed DoS (DDoS), where multiple systems are used to generate a massive flood of packets. See the following figure for an illustration of a flood DoS:

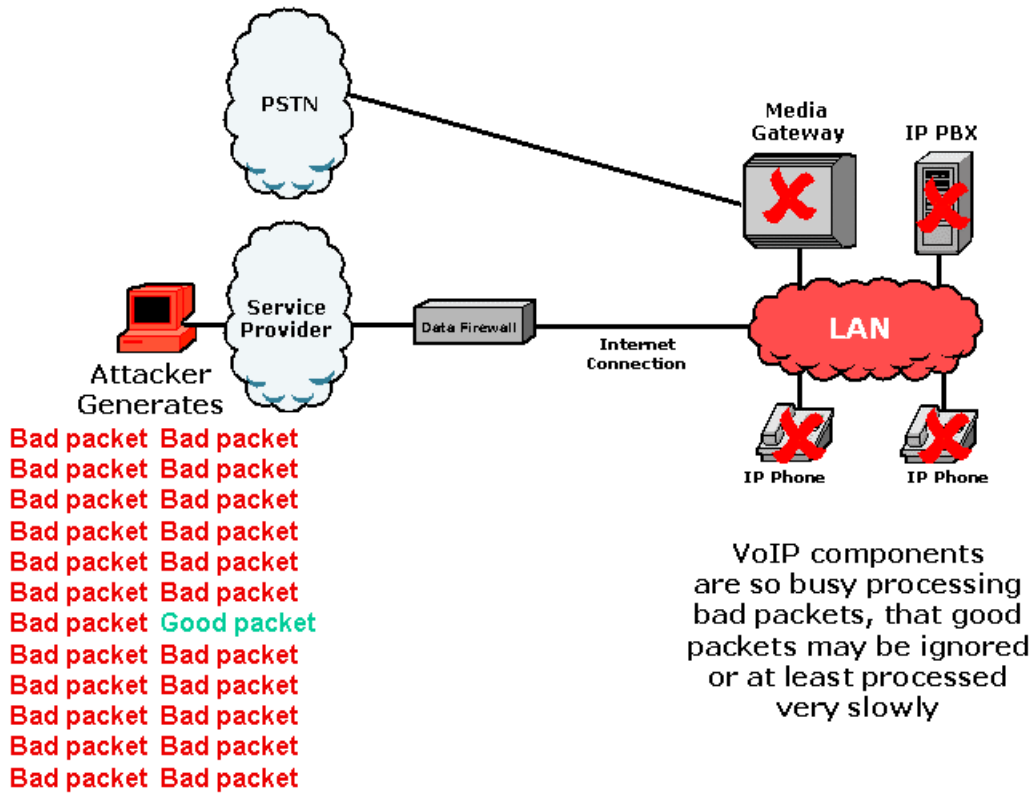


Figure 1 – Flood DoS

- Application-level DoS – occurs when a feature of the VoIP service is manipulated to cause DoS. For example, hijacking the registration for an IP phone can cause loss of any inbound calls to that phone.

Any component in a VoIP system can be a target for DoS. DoS can be especially damaging if your key voice resources are targeted (e.g., media gateways, AA, IVR, VM, and other systems). DoS can also be used to generate large numbers of toll, information (411), or emergency calls (911). Your network can also be used as a DoS launching point from which the generated calls are directed at another enterprise.

Platform DoS

An attacker can create DoS by targeting a critical underlying support service on an IP PBX or IP phone. For example, a TCP/IP SYN flood attack can be used to target an implementation of TCP/IP that is vulnerable to this attack. Another example would be to attack a known vulnerability in the underlying Windows operating system of an IP PBX. Some recent examples of platform attacks are listed below:

- Cisco Call Manager – the underlying Windows operating system and web server have been susceptible to attacks.
- 3COM NBX – a 3COM NBX configuration utility can be caused to crash by running a standard scan with the Nessus vulnerability scanner. This system can also be caused to crash by sending a specific response to the FTP server.
- Pingtel xpressa IP Phone – sending a specially crafted packet to the management interface can crash the operating system.

- Kphone Soft Phone – this application can be caused to crash by sending a specially crafted STUN packet.
- Cisco IP phones – some of the early Cisco IP phones could be crashed by using well-known DoS tools.

In addition to these DoS vulnerabilities, there are many more examples where a remote user can use the vulnerability to gain access to the system and/or execute arbitrary code, which could also be used to create a DoS. For more information on these and other vulnerabilities, use the following link and enter “VoIP” or “IP Telephony”:

- <http://search.securitytracker.com/cgi-bin/ts.pl>

Signaling and Media DoS

A VoIP system must exchange both signaling and media packets over the LAN, WAN, and possibly even an untrusted network such as the Internet. Virtually all VoIP system components must process both signaling and media. DoS is therefore possible by targeting the signaling and/or media processing software on VoIP components. The following figure lists example signaling, media, and platform attacks, as they correspond to software layers in a VoIP component such as an IP PBX:

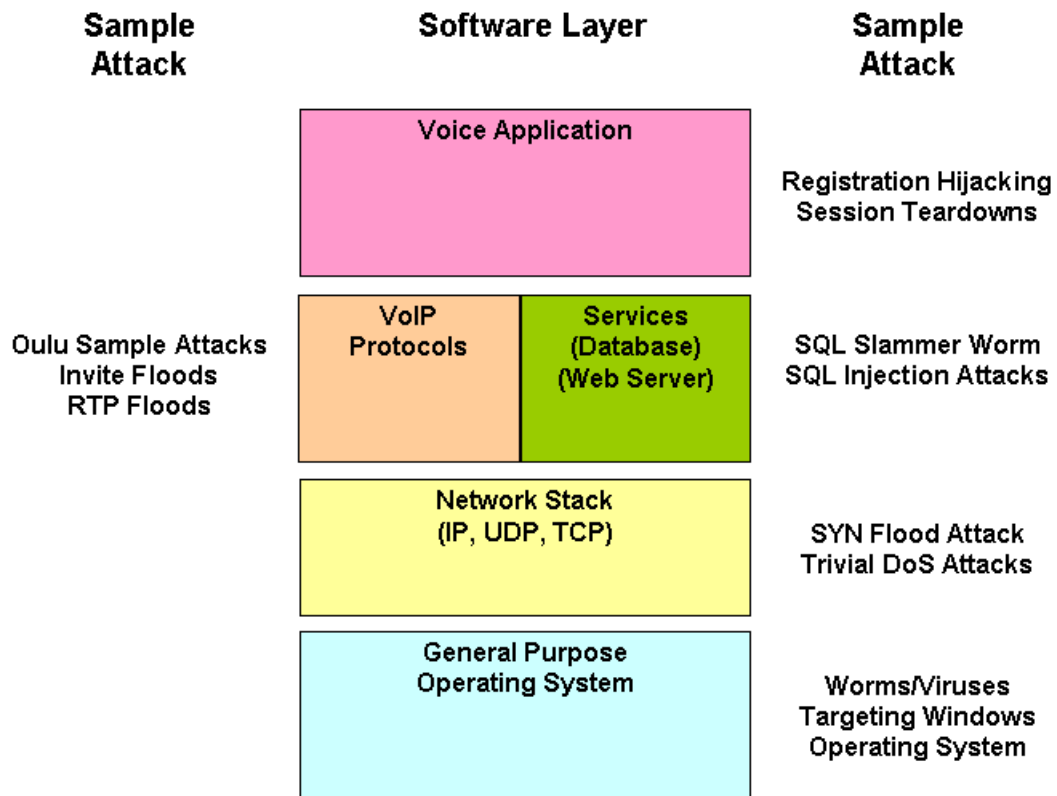


Figure 2 – Example DoS Attacks on Different Software Layers

The next two sections provide more information on signaling and media DoS attacks, including some additional examples.

Signaling DoS

Every component in a VoIP system, including the IP PBX, IP phones, media gateways, VoIP-aware firewalls, etc. must process signaling. DoS against the signaling interface is a major issue for the following reasons:

- Complex protocols – there are many VoIP protocols, including SIP, H.323, MGCP, SCCP, etc. Multiple protocols are generally in use in most VoIP environments. Complex software is needed to support these protocols. Where there is complex software, there will be implementation flaws.
- Weak authentication – very few VoIP components use strong authentication, so VoIP components can be easily tricked into processing spoofed packets from an attacker.
- Firewalls – most firewalls do not check for VoIP signaling attacks.

One indicator of how vulnerable VoIP components are to signaling DoS, is the results of research performed by the University of Oulu in Finland. Oulu has developed simple SIP and H.323 protocol test suites and run them against several implementations. In Oulu's words, the results were "alarming," indicating that virtually all of the tested components failed. As a result of this research, many vendors issued security advisories, including Nortel and Cisco. For more information on this research, see the following pages:

<http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/>

<http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/h225v4/>

Note that these protocol suites can be downloaded and used to test your SIP or H.323 system. There is also a draft RFC describing a "SIP Torture Test," which is another useful set of tests that vendors should follow to ensure their SIP implementations are robust.

Some recent examples of actual signaling DoS vulnerabilities are as follows:

- Cisco CallManager Express – can be forced to reload by sending a specially crafted SCCP packet.
- VocalTec gateway – can be crashed by sending a specially crafted H.323/H.225 packet several times (approximately 10).
- PWLib H.323/H.225 – this commonly used library can be exploited by sending a specially crafted packet. This flaw can result in a DoS, depending upon what application is using the library.
- sipd – can be crashed by sending a specially crafted SIP packet.

SecureLogix has developed various "flood" tools that send large numbers of INVITE requests to a variety of SIP proxies and phones. The components tested were unable to effectively process calls while the attack was active. The components did generally recover after the attack ceased.

In addition to implementation flaw and flood-based DoS, there are application-level attacks that are also possible. A few examples to consider are as follows:

- Registration hijacking – VoIP protocols used for handset communication use the concept of "registration," which involves an IP phone registering itself with an IP PBX/proxy to allow routing of inbound calls. If an attacker is able to hijack this registration, they can intercept inbound calls and prevent them from reaching to the IP phone, effectively creating a DoS.
- Session teardown – VoIP protocols, especially SIP, allow IP phones to send termination messages between the IP phones. It is possible for an attacker to craft a termination message and send it to the IP phones, tearing down the call and creating a DoS.

Media DoS

Virtually all VoIP systems use the Real Time Protocol (RTP) to transmit the media (audio) packets. RTP is a very simple protocol, especially when compared to any of the signaling protocols used by VoIP. Accordingly, there will be much fewer implementation attacks, since the software needed to implement

RTP is very simple. However, because RTP carries media, which must be delivered in real-time to be usable for an acceptable conversation, it is vulnerable to flood-based attacks. For example, an attacker can flood a media gateway, IP Phone, shared WAN link, or other media-processing VoIP component, interfering with the processing of normal packets. If this attack causes the target to drop or ignore legitimate RTP packets, then the audio quality may be unacceptable for conversations.

In tests with SIP, SecureLogix conducted RTP flooding against a number of IP phones. The floods were very effective, resulting in severe or total degradation of the audio. While these attacks did spoof packet values, such as MAC address, IP address, and RTP sequence numbers, it was observed that most IP Phones did not even check these values. It was also observed that when very large RTP packets (approximately 1500 bytes) were sent to ports on certain IP phones, they crashed and had to be manually rebooted.

Recommendations

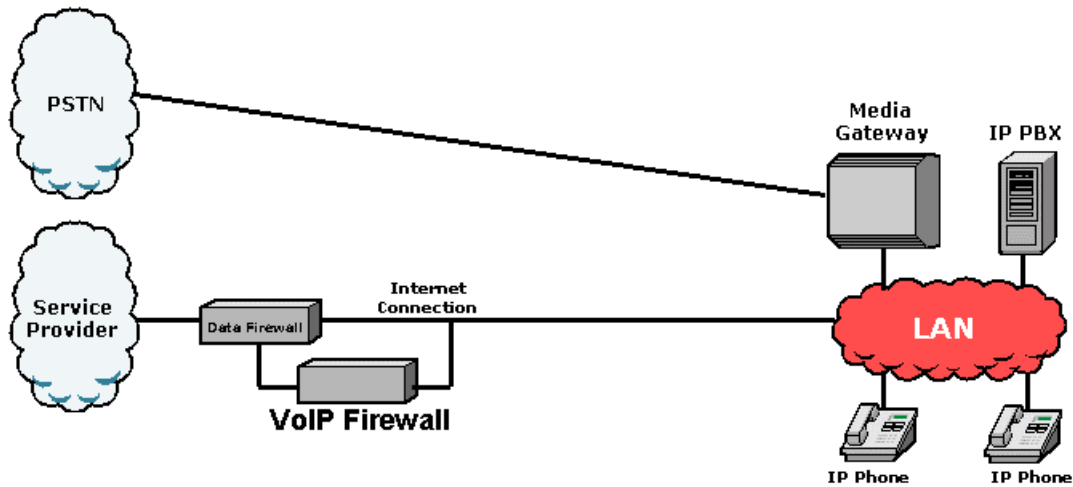
DoS is a very difficult threat to deal with. New implementation flaws are being identified at an increasing rate as more and more VoIP is deployed. Flood-based DoS will become a critical issue as VoIP is exchanged between enterprises over untrusted networks. DoS is best mitigated with the following steps:

- System hardening – involves disabling/removing unnecessary network services, locking down the operating system, and using internal host-based intrusion detection to mitigate certain classes of attacks. All VoIP components should be hardened.
- Strong authentication – allows VoIP components to be sure that they are communicating with legitimate components. Any packets from non-authenticated components can be more easily discarded. This model works well for internal VoIP deployments is helpful when VoIP is exchanged over an untrusted network.
- Traditional firewall – provides another layer of protection, focusing on mitigating platform-level attacks.

VoIP firewalls can provide additional security, especially on the enterprise perimeter when VoIP is exchanged over an untrusted network. A VoIP firewall can provide the following types of DoS mitigation:

- Implementation flaw DoS:
 - Monitor for known VoIP attack patterns and discard packets accordingly.
 - Monitor for new forms of attacks and discard packets accordingly.
- Flood DoS:
 - Perform signaling and media rate limiting.
 - When a flood DoS is detected, quickly discard obviously malicious packets.
 - Allow packets from known, authenticated sources.
 - Use enterprise calling patterns to determine action to be taken on questionable packets.
 - Maintain adequate bandwidth for known, good calls.
 - Monitor for and drop rogue RTP streams.
 - Monitor for and drop rogue RTP packets, which are targeting active RTP streams.
 - Monitor media packet size, port destination, and rate. Drop malicious packets and throttle streams as necessary.
 - Monitor for and drop illegitimate packets, which carry high QoS markings.
- Application-level DoS:
 - Monitor for and counter external attacks such as registration hijacking and illegal teardowns.

The following figure illustrates where in the network a VoIP firewall can be placed and summarizes the DoS attacks it should mitigate:



- Addresses implementation Attacks:**
 - Monitor for and drop malformed packets
- Addresses flood Attacks:**
 - Perform rate limiting
 - Discard obviously malicious packets
 - Allow packets from trusted sources
 - Prioritize known good calls
 - Monitor for rogue RTP
 - Monitor media packet size, rate, etc.
- Addresses application-level attacks:**
 - Address registration hijacking/session teardown

Figure 3 – VoIP Firewall Deployment and Examples of Mitigated DoS Attacks

Conclusions

DoS is one of VoIP's most challenging threats to address. DoS is an issue now, and will become a more significant issue going forward, as VoIP is more widely deployed and as enterprises start to interconnect their internal networks via untrusted networks. Research has shown that many VoIP components are vulnerable to DoS. The threat to these components will increase. Requiring well-designed VoIP components, use of strong authentication, and VoIP firewalls best mitigates this threat.