Denial of Service attacks against VoIP systems

A White Paper from Velona Systems

Tony Friar, Chief Technical Officer
Denial of Service attacks against VoIP systems

This paper describes the main types of Denial of Service (DoS) attacks that can be used against Voice over IP (VoIP) telephony systems, analyses the existing solutions, and discusses why they are not sufficient to deal with many of the present-day and imminent attacks.

The attacks described here are those against VoIP systems using Session Initiation Protocol (SIP), though the concepts covered here generally apply to most other VoIP signalling protocols. SIP is the main signalling protocol used by Voice over IP (VoIP) systems across the world. SIP is used by 4G and 5G mobile networks, IP PBXs, and hosted voice systems.

A Denial of Service (DoS) attack is aimed at causing VoIP telephony systems to stop functioning as normal. DoS attacks are launched for a number of reasons, such as:

- To extort money (if the company refuses to pay the attack continues)
- To damage the brand and reputation of the company being attacked (customers, business partners, investors, etc. are unable to contact the company being attacked.
- Service Providers suffering outages caused by a DoS attack can lose customers
- As a cover for other wider forms of cyber-attack (e.g. block or bring down a call centre's phones so that people cannot report financial crime, or block or bring down a business's phone lines so they cannot be contacted while their bank account is being emptied)
- For political, or state sponsored cyber terrorism, reasons
- Sometimes DoS attacks are launched just for fun

The types of DoS attacks against SIP based VoIP systems, covered in this paper are as follows:

- Call Flooding
- Message Flooding
- Incomplete Transactions
- Malformed Messages (Fuzzing)
- Rebooting of endpoints such as VoIP phones
- Disruptive Signalling
- Malware based attacks using 4G & 5G mobiles

A common feature of a lot of these attacks is that they arrive at their target from the Internet and are also usually generated by SIP attack kits which have unique SIP signatures.
Call Flooding (aka Telephony Denial of Service) Attacks

Call Flooding or Telephony Denial of Service (T-DoS), and even sometimes called Mass Calling, is a DoS attack that involves sending large numbers of calls towards a specific target or targets with the intention of preventing the normal operation of telephony services because the phones / softphones keep ringing and as soon as they are answered and cleared the phone often rings again either immediately or very soon afterwards.

T-DoS attacks prevent both incoming and outgoing calls or at the very least cause severe limitations. Such attacks are often launched for financial gain with the intention of extracting a payment to stop the attack or by acting as a cover while financial fraud takes place. The FBI issued a bulletin about this, as far back as 2010 [1], but the problem persists today.

Call Flooding DoS attacks can be used in a number of scenarios of which the following are some examples:

- Targeting the main switchboard number of a company or organisation
- Targeting a specific department in a company or organisation
- Target a call / contact centre
- Targeting emergency services
- Targeting individuals
- Targeting a Service Providers voice over DSL or voice over cable residential customers (depending on how this attack is carried out it can also be seen as a Nuisance Attack used, for example, to wake up customers in the middle of the night)

Call Flooding is almost always used against end businesses and organisations including government departments. There have also been incidents when emergency services numbers have been targeted and a bulletin issued by US law enforcement agencies as far back as 2013 warns of attacks against emergency services [2].

Call Flooding is not often used directly against Service Providers when the aim is an attack against the Service Provider itself (though a Call Flooding attack against a business or organisation may be passed on by a Service Provider) because of the large number of calls that would need to be generated to cause a problem for the Service Provider.

However, the authors of this paper believe that this is changing and 4G VoLTE mobile networks as well as 5G networks have and will come under Call Flooding DoS attacks via malware infected handsets.

Call Flooding attacks against VoIP systems may pass via the Service Provider that provides the telephony service to the end business or organisation; or may be sent directly to the customer or organisation via the Internet.
Although Call Flooding attacks can be used against any type of business, individual or organisation that uses telephony, they can be especially damaging when used against businesses that rely on predominantly telephony for their business or to function. Examples include call centres and banks.

**Note:** Call Flooding is often referred to as Telephony Denial of Service (T-DoS). Given that there are a number of DoS mechanisms that can be used against telephony systems it may seem strange that the term T-DoS is often used only in this limited sense. This limited definition is historical and is related to the pre-VoIP days when flooding a telephony system with calls was generally the only option open to most attackers looking to carry out a DoS attack.

Velona Systems takes the view that this definition needs to be updated and as such when we refer to a T-DoS attack we mean any DoS attack directed towards a telephony / Unified Communication system be it a Service Provider fixed line, mobile or Fixed Mobile Convergence (FMC) network or a small, medium, or large end Enterprise.

**Message Flooding Attacks**

A SIP Message Flooding attack involves sending more SIP messages to the target(s) under attack than the target(s) can deal with. If the target has insufficient memory or CPU to deal with the attack, then it will stop processing calls, either partially or fully, or other functions may be affected instead or as well (e.g. billing records may stop). An attack that uses SIP Message Flooding may also utilise Incomplete Transactions and / or Malformed SIP Messages.

**Incomplete Transaction Attacks**

A SIP Incomplete Transaction attack involves not responding to a SIP message that the target of the attack has sent. This results in the target of the attack having to keep track of a transaction for longer than would be expected and can lead to memory exhaustion problems. Incomplete Transaction attacks utilise large numbers of transactions to achieve their aim. An attack that uses SIP Incomplete Transactions may also utilise SIP Message Flooding and / or Malformed SIP Messages.

**Malformed Message Attacks**

A SIP Malformed Message Attack (also known as Fuzzing) involves sending a SIP message that is either not compliant to the relevant SIP specification(s) or which is compliant but which the SIP stack / SIP parser of the target is not able to process correctly (e.g. due to a software bug). The aim of a SIP Malformed Message attack is to cause the target of the attack to stop processing calls either partially or fully. This could be achieved because the target is sent into some form of loop by the attack or reloads or is affected in some other way related to the internals of the target software.
Rebooting of endpoints such as VoIP Phones

Many VoIP endpoints (e.g. IP Phones) can be rebooted by a single SIP message. The idea behind this is that the endpoint may need to be rebooted for maintenance purposes because of a problem or to apply a new configuration or software.

If configured correctly most VoIP endpoints can challenge the reboot message and ask for a response based on a shared password-based mechanism. If the endpoint does not support such a mechanism (rare these days) or the mechanism is not configured, then it can be possible to reboot the endpoint as frequently as the attacker requires therefore creating a DoS attack.

Disruptive Signalling

Disruptive Signalling attacks are arguably not strictly DoS attacks but more of a nuisance attacks. However, they have been included here as they can affect the productivity of users and their ability to carry out their work. Disruptive Signalling attacks include:

- Incorrect Voicemail Message Waiting notifications
- Incorrect Call Waiting Notifications
- Incorrect presence states
- These attacks are intended to cause confusion and inconvenience rather than a total or partial outage.

Malware based attacks using 4G & 5G mobiles

As mobile phone networks move to 4G VoLTE and then 5G, nearly five billion more devices will directly enter the VoIP population. Given the wide-ranging estate 5G will bring, it will only take a small number of Mobile Network Operators (MNOs) who fail to protect their equipment to jeopardize everyone.

Hacked and malware infected user mobile devices will be used to carry out Denial of Service (DoS) attacks and Toll Fraud attacks against both the core network and Enterprises being served by those Core Networks and these attacks are already being seen on 4G VoLTE networks.

In even small and medium sized 4G networks there can literally be millions of SIP messages over a very short period-of-time and finding the specific message without the appropriate tools to detect Malformed SIP Messages can be extremely difficult if not impossible within the time needed to prevent the next attack.

See Velona’s White Paper ‘SIP Based Malware & Ransomware Attacks against 4G VoLTE & 5G Networks’ for further details.
Limitations of existing Solutions

A large number of VoIP DoS attacks use SIP attack kits. Since most Firewalls do not provide Deep Packet Inspection on VoIP traffic, the main line of defence sits within the Session Border Controllers (SBCs) placed in the Core and Edge of the Network.

Core SBCs (simply called SBCs) are used to protect Service Provider VoIP networks while Enterprise Session Border Controllers (E-SBCs) are used to protect the end customer (who sits at the Edge of the Service Provider’s network).

Both these types of SBC do not currently identify SIP attacks kits beyond (sometimes) making a basic check on a specific field that contains the name of the attack kit, and even then, this requires specific configuration on the SBC. The attackers can easily change this field to spoof a legitimate SIP endpoint or network.

Both types of SBC are also very often unable to detect and block a large number of Malformed SIP message types, as well as SIP messages that may comply with standards, but which are unusual, and which can cause DoS attacks to devices and nodes behind the SBC, or even in some cases to the SBC itself.

The E-SBCs which do try to detect malformed messages often require specific configuration, which under load can result in processing issues.

There is growing trend to remove on-site E-SBCs and instead rely on private tunnels, VPNs, and end-to-end encryption. Up to a third of attacks come from Insiders, against whom encryption provides no protection. Furthermore, malware infected 4G & 5G devices will already be registered on the mobile networks and will be able to use the IPsec tunnels so are already ‘inside’.

DoS attacks against VoIP have started to become more sophisticated and there has been a noticeable increase in the use of Malformed Messages to cause outages to both end businesses and Service Providers.

The authors of this paper believe that such attacks will increase significantly and that 4G VoLTE and 5G voice networks are hugely at risk from malware infected handsets that can send Malformed SIP Messages as well as taking part in Mass Calling DoS attacks against the core 4G or 5G voice infrastructures (IMS).
Conclusion

Attacks against VoIP infrastructure by cyber criminals and state actors are a significant and growing problem. VoIP DoS attacks can be standalone attacks intended only to prevent a specific system or systems from functioning correctly, or they can be part of a broader cyber-attack as in [3] and [4].

At present the clear majority of DoS attacks against voice systems use Mass Calling / T-DoS and to an extent Targeted Nuisance Calling. However, more sophisticated attacks such as Malformed Message attacks and Incomplete Transaction attacks are rising.

A recent report from IBM's Security Intelligence website describes spikes of malformed SIP messages were mostly the result of specially crafted SIP messages that were terminated incorrectly. Persistent, invalid messages are known to cause vulnerable servers and equipment to fail. [5]

As VoIP systems replace traditional phone systems and as 4G VoLTE and 5G mobile networks that use end to end VoIP are deployed the potential for a greater number of attacks grows higher.

These attacks can lead to not only revenue loss and reputational damage, but in some severe cases to injury or loss of life. As cyber-attacks increase, it is vitally important that VoIP systems are tested for weaknesses on a regular basis, and continually monitored so that attacks are detected and stopped as soon as possible.

The ability to easily identify SIP attack kits and Malformed SIP Messages is now of vital importance and a key part of the armoury in the defence against VoIP infrastructure attacks.
Velona’s approach to protecting against VoIP DoS attacks

Velona provides a range of products and services for VoIP security that identify and detect SIP Denial of Service attacks.

** Threat Management for VoIP

1. **SIP Fingerprinting Library** (available as an OEM product for C and Java) allows the manufacturer, model and often software version of SIP packets to be identified, so that legitimate and non-legitimate signalling can be easily separated.

2. **SIP Malformed Message Detection Library** (also available as an OEM product for C and Java) allows the identification of not only SIP signalling that is not compliant with the relevant standards, but also the identification of SIP messages that are unusual and could indicate a DoS attack.

3. **WATCHER** is an off-the-shelf solution that includes SIP Fingerprinting, SIP Malformed Message Detection, Mass Calling Detection, Message Flooding Detection and Toll Fraud Detection.

4. **CRACKER** is a Cloud SaaS Verification and Testing platform to enable SPs and MNOs look for weaknesses in SIP security and affordably run Load Testing, and SIP parser / Torture testing so that they can fully verify they are deploying solutions which have the required Advanced Security robustness built in to their deployments.

**Advanced VoIP Security consultancy**

Velona provide Advanced VoIP Security consultancy to a range of clients within Telecommunications and Enterprise.

**References**


