Combating Denial of Service Attacks for VoIP and Unified Communications

Technical Summary
October 2014

The impact of Denial of Service Attacks has lead the network security industry to develop techniques to limit the impact of these attacks. These techniques are targeted at protecting data services. The growth of VoIP and UC Services and their reliance on IP networks exposes those services to DoS attacks. The design of the protocols used for VoIP and UC means that the defences developed for data services cannot offer full protection. The UM Labs SIP Security Platform provides comprehensive protection against DoS attacks for VoIP and UC services.

Denial of Service Attacks

The Computer Emergency Response Team (CERT) at Carnegie Mellon University defines a Denial of Service (DoS) attack as:

> *an explicit attempt by attackers to prevent legitimate users of a service from using that service*

DoS attacks are nothing new. Internet connected systems and data applications have been targeted for at least the last 20 years. Most of these DoS attacks relied on swamping systems with high traffic volumes so that they are unable to respond to legitimate service requests. The type of traffic sent to a target system will depend on the type of attack. An attacker may choose to flood a web server with multiple requests, he may send large numbers of login requests (using bogus user names) to a system's login page or he may target the system at much lower level sending malformed network packets. The effect of a DoS attack is magnified by sending more requests. These easiest way to this is to send from multiple sources, these attacks are known as Distributed DoS (DDos) attacks.

DDos attacks are a growing problem for data centres. A recent study by the Ponemon Institute showed that in 2013, 18% of outages were triggered by DDoS attacks. This was a significant increase on the 2012 figure of 2%.

Impact of Attacks

A successful DoS attack can be costly. Taking an on-line shopping service off-line means loss of revenue. An attack on an on-line banking system damages customer confidence and the bank's reputation. Disrupting a company's phone service can bring business to a halt. To protect against these risks, most good data firewalls include DoS protection. The nature of these attacks means that the security defences used concentrate on looking for known data patterns that could indicate an attack and implementing rate limits to reduce the impact of an attack. The Ponemon study quantifies this. In 2013 the mean cost of an unplanned outage was close to $8,000 per minute. This figure covers directly quantifiable cost, when intangible costs such as damage to reputation and loss of customer confidence are included, the real figure is likely to be higher.

VoIP Attacks

Voice over IP (VoIP) and Unified Communication (UC) applications run on IP networks. This means that these real-time communication applications are exposed to the same DoS attacks as data applications. However the complexity of the protocols used to run these applications means that VoIP and UC services are also exposed to an entirely new set of DoS attacks. Rather than swamping systems, these attacks rely on sending requests at a volume that cannot be distinguished from normal traffic. The request content is also very similar to a legitimate request so attacks are difficult to detect by content scanning. These two factors mean that traditional DoS protection measures are ineffective against many of the VoIP and UC specific DoS attacks.

VoIP and UC attacks that fall into this hard-to-block category include:

- Call disruption attacks, terminating active calls
- Call hijacking, taking over an active call
- Call re-direction, re-routing calls to an unauthorised destination
- De-registration, preventing a phone from receiving any calls
- Media injection, replacing or masking the audio or video stream in an active call

VoIP and UC systems are also targets for flooding attacks, but the threshold for a successful DoS attack is much lower than for a data application. A flooding attack on a web server must generate so many bogus requests that legitimate requests are not processed. This means thousands of requests per second. A call flooding attack that makes a phone ring or sends a text message will be effective at a rate of 2 or 3 per minute as the user will leave the phone off the hook or turn off the Instant Message app.

VoIP and UC systems present more targets for DoS attacks than data applications. A DoS attack against a data application typically targets the server. A DoS attack against a VoIP system has 3 targets, the caller's phone, the call recipient's phone and the server. The phones are often less protected that the servers.

These factors mean that defending against DoS attacks against VoIP and UC applications is more difficult than for data applications. Effective DoS protection should include the defences developed for data applications but must also protect against the VoIP and UC specific threats.

Defending Against DoS Attacks

The UM Labs SIP Security Platform solves this problem by implementing multi-level security controls. These controls combine IP level security with application level controls. The IP security controls protect against generic DoS and DDoS attacks while the application level controls handle VoIP and UC specific attacks, including those that do not generate detectable traffic floods.

The UM Labs technology employs a number of sophisticated techniques to defend against VoIP DoS attacks at the application level. When an attack is detected, information on the source of the attack is passed to the lower level security controls. These enables further attacks to be detected and discarded as quickly as possible. This mechanism, which is only possible in a product which is designed specifically for VoIP and UC security provides a very efficient and effective mechanism to protecting against both DoS and DDos attacks. Other products, which lack this ability, are not able to provide the same level of protection against these attacks.