

The UM Labs range of SIP Security Controllers is designed to protect against a wide range of security threats that affect VoIP systems running the Session Initiation Protocol (SIP). This application note describes these security threats.

Threat Classification - SIP-based VoIP applications and servers face three distinct categories of threats:

- **IP Network Level threats.** This category includes threats associated with the underlying Internet protocols which drive VoIP. These threats are common to all IP applications.
- **Protocol and Application threats.** This category includes threats that directly target the VoIP protocols and applications. These threats are specific to VoIP systems.
- **Content threats.** This category includes threats that affect the content delivered by a VoIP service, the audio or video stream. Most of these threats are specific to VoIP applications, but some may affect related services, for example streaming audio or video services.

Attack types - Each category includes a range of attacks, each with a unique primary aim and methodology:

- **Denial of Service/Distributed Denial of Service (DoS/DDoS).** The aim of a denial of service attack is to force the target into processing large numbers of network requests so that the service offered by the target is degraded or disrupted. DDoS attack is a coordinated DoS attack from several sources.
- **Penetration.** A penetration attack is designed to to gain unauthorized access to a system, to access data stored on that system, or to use a service provided by that system. A penetration attack aimed at a VoIP system may give an attacker access to call processing systems enabling calls to be re-routed or may enable an attacker to make unauthorized calls.
- **Remote Execution.** This attack enables an attacker to introduce malicious code onto a target and have that target execute that code. The gives an attacker complete control over the target.
- **Unauthorized Service Access.** The aim of this attack is to bypass any authentication or access controls and gain access to protected services. It differs from a penetration attack in that it uses standard service access mechanisms, relying on weak or poorly implemented access controls for its success.
- **Service Misuse.** These attacks make use of standard service requests to achieve their goal. For example, a SIP call hijack uses requests that are designed to provide features such as call hold and call transfer to take control of an established call.
- **Protocol Misuse.** This is a broad category covering a range of attacks that make use of the service protocols in a non standard way, with the aim of disrupting the target. Many of these attacks are also DoS attacks. For example many VoIP phones are vulnerable to attacks where valid VoIP protocol requests are sent in a non-standard order. In many cases these trigger a device reset.
- **Protocol Fuzzing.** This is a variant of protocol misuse where, rather than send valid protocol requests, the attacker sends malformed requests or even random data.
- **Eavesdropping.** This attack monitors a data stream and recovers the information transmitted. An eavesdropping attack on a VoIP system can capture and record calls.
- **Device Discovery.** Device discovery attacks are used to identify and enumerate potential targets for other attacks.

The UM Labs SIP Security Controller protects against all three of the defined threat categories and each of the defined threat types.

IP Network Level Threat Protection

UM Labs' range of SIP Security Controllers includes an IP Firewall module to protect against IP Network Level threats. This module is optimised for VoIP and is designed to conform to the US Government Protection Profile for Firewalls. The IP Network Level threats blocked by this module include:

Threat	Threat type	Potential Impact
Malformed packet flood	DoS/DDoS	Service Failure
Unauthorized Service Access	Penetration	System compromise
TCP Connection Flood	DoS/DDoS	Service Failure
Other TCP threats (e.g. Syn flood)	DoS/DDoS	Service Failure
UDP Flood	Dos/DDoS	Service Failure
Multiple ICMP threats	DoS/DDoS	Service Failure
Buffer Overflow threats	Remote Execution	System compromise

Protocol and Application Threats

The UM Labs SIP Security controller includes a SIP proxy that is both SIP Transaction and SIP Dialog stateful. This proxy protects against those threats that target SIP applications and which rely on specific features of the SIP protocols.

Threat	Threat type	Potential Impact
Malformed SIP packet flood	DoS/DDoS	Service Failure
Unauthorized Service Access	Penetration	System compromise
Toll Fraud	Unauthorized Service Access	Direct Financial loss
SIP Message Flood	DoS/DDoS	Service Failure
SIP De-Registration Attack	Dos	Loss of service to targeted device
Call termination attack	Dos	Loss of service to targeted device
SIP OPTIONS Scan	Device Discovery	Identifies targets for other attacks
Unauthenticated Service Requests	Unauthorized Service Access	System compromise
SIP Authentication Replay	Unauthorized Service Access	System compromise
Call Hijack Attack	Service Misuse	Compromise of targeted calls
Protocols fuzzing and misuse	Protocol Misuse	Service Failure.

Content Threats

The UM Labs SIP Security Controller processes all media streams through a secure RTP proxy. This proxy provides call encryption and protects against other content threats.

Threat	Threat type	Potential Impact
Unauthorized Call Monitoring	Eavesdropping	Loss or confidentiality
RTP Injection	DoS	Loss of service to targeted device
Protocols fuzzing and misuse	Protocol Misuse	Service Failure.

About UM Labs UM Labs Ltd. was founded in 2008 by security software pioneers dedicated to the promotion of secure global standards for unified communications. The company has an extensive support organization and partner network, with offices in the following locations:

United Kingdom

Heathrow Blvd 4
280 Bath Road
West Drayton
UB7 0DQ
UK
Phone: +44 20 3021 3200

USA

5586 Main St, Suite 206
Williamsville
NY 14221
USA
Phone: 716 568-4931

Canada

366 Adelaide St, Suite 301
Toronto, ON
M5V 1R9
Canada
Phone: 416 598-7537

Website: um-labs.com

Email: info@um-labs.com

VoIP: sip:info@um-labs.com