



**Media Contact:**

Peter Cox  
peter@um-labs.com  
Phone: +44 20 3201 3200  
Cell +44 7785 333832

## UM Labs Ltd: New Call Fraud Controls for SIP Networks

London May 26<sup>th</sup> 2011, in a response to the growing problem of call fraud on SIP networks, UM Labs have added some innovative fraud controls to their SIP Security Controller.

The problem of VoIP call fraud, particularly on Networks running the Session Initiation Protocol (SIP) is growing. Call fraud occurs when attackers make use of IP connections to penetrate VoIP systems and to make free calls at the expense of the victim. Many attackers make use of *SIPVicious*, a package that is freely downloadable from the Internet, to identify vulnerable systems. Any phone system with an Internet connection will have already been targeted.

If that system is not adequately protected, the attacker will then proceed to make calls. Often the first the victim knows about the problem is when their phone bill arrives. To quantify the problem, UM Labs recently set up a honey pot system to determine how long it would take for the system to be found. Within 24 hours the system was discovered and multiple calls made to locations including mobiles in Mali and Haiti.

PBXs are vulnerable if they are not correctly configured. While a reputable SIP trunk provider will offer advice on correctly configuring the PBX, this can be a difficult task as the configuration needed to block fraudulent calls can conflict with the configuration needed to allow remote user access.

To solve this problem, UM Labs have added a number of sophisticated call fraud checks to their SIP Security Controller. The SIP Security Controller is an affordable Session Border Controller (SBC) designed for corporate use. In contrast to some other SBC products the UM Labs product includes comprehensive SIP security to protect against call fraud and other threats.

The new call fraud controls include automated filters to detect and block attack tools such as *SIPVicious* and to reinforce those filters with controls to detect suspicious call patterns. These filters are complimented by blacklists that block known attack sources and which can limit calls made via SIP trunks by country code or area code. The controls also include easily configurable call rate limits to prevent any user, malicious or otherwise from, making excessive calls.

Peter Cox, CEO of UM Labs commented, "The call fraud controls in the latest release of our SIP Security Controller are designed to simplify the task of securing a SIP based PBX and to allow a user gain full benefit of a SIP trunk while minimising the risk of call fraud."

These controls are implemented in V1.5 of the SIP security controller, which is currently shipping.

## *About UM Labs Ltd*

UM Labs is a pioneer and leader for security and connectivity products around internet telephony and other services based on the Session Initiation Protocol (SIP). The UM Labs core product is the SIP Security Controller that enables and protects customer systems making it easier to use Voice over IP (VoIP), SIP Trunks and other Unified Communications functions. Since the inception of UM Labs in 2007, SIP Security Controllers have enabled enterprises, government and communications service providers to successfully exploit the lower cost internet bandwidth for voice connections between sites and into SIP Trunks.

For more information, please visit our website, <http://www.um-labs.com/>