



Media Contact:

Peter Cox

Email: peter@um-labs.com

Phone: +44 20 3201 3200

VoIP: sip@peter@um-labs.com

UM Labs Announce the first Gateway Implementation of Phil Zimmermann's ZRTP

London September 23rd, UM Labs Ltd announce the release of the first Gateway Implementation of Phil Zimmermann's ZRTP. ZRTP safeguards the security and integrity of VoIP calls by encrypting both the voice and video streams. ZRTP differs from other VoIP encryption schemes by providing a superior key exchange mechanism, eliminating the risk of unauthorised call monitoring and eavesdropping.

The UM Labs announcement means that ZRTP secured calls can be made from a growing number devices, including many of the newer cell phones, to any SIP based VoIP system including those from manufacturers such as Avaya, Cisco, Mitel, Nortel, Siemens and many others. The ability to provide this level of integration with targeted security is a key milestone on the path to effective Unified Communications.

As the use of VoIP services grows, the security and confidentiality of voice calls and video conference sessions routed over IP networks becomes a concern. One obvious technique to combat this problem is to encrypt the voice and video streams. A number of encryption techniques are available, but most suffer from the problem that the encryption keys are exchanged in the signalling channel. In layman's terms this means that encryption keys are sent along with the request to set up a call. As every call routing device between the caller and call recipient must obviously be able to see the call request, these devices are also able to see the encryption keys. This risks the confidentiality and integrity of the call because the keys can easily be recovered and used to decrypt a monitored call.

Phil Zimmermann designed ZRTP to overcome this problem by implementing the encryption key exchange in the voice channel where it remains invisible to intermediate call routing devices. ZRTP also includes features to detect and prevent *Man-in-the-Middle* attacks. With this technology caller can talk freely, confident in the knowledge that their conversation is secure.

UM Labs have added ZRTP support to both the branch office and enterprise versions of their SIP Security Controller product. Installing a UM Labs SIP Security Controller at a company's network perimeter means that home workers and remote users are now able to make secure calls into the corporate VoIP network and from there reach any other connected user or to call any PSTN number.

Peter Cox, CEO of UM Labs commented: "Support for the latest release of ZRTP is a key component in our latest product release. It comes at a time when ZRTP is available on a growing number of phones. The recent announcement from TiVi (www.tivi.com) for example, means that calls can be made from most cell phones. Simply by installing a UM Labs SIP Security Controller at their network perimeter, companies can enable secure inbound VoIP calls from any ZRTP capable device to any SIP based PBX."

Phil Zimmerman, creator of PGP and designer of ZRTP commented: “The fact that UM Labs have included ZRTP in the latest version of their SIP Gateway, significantly increases the number of destinations reachable from ZRTP phones. ZRTP users can now make calls to any user connected via any SIP PBX and be assured that the call is protected between the phone and the gateway”.

About UM Labs Ltd

UM Labs delivers a range of application level security gateways for VoIP and Unified Messaging. These gateways are designed to provide security controls targeted at the range of threats that affect VoIP and UM applications, exceeding the capabilities of standard Firewalls. UM Labs product range also provides a realistic and cost effective alternative to Session Border Controllers (SBC).

UM Labs founders include Peter Cox, formerly co-founder of Internet Security Specialist Borderware Technologies. While at Borderware, Peter contributed to the design of the Borderware Firewall Server, one of the first commercial Firewall products and to the company’s MXtreme product, an application level security gateway for email. Peter was also responsible for the project which gained a total of 3 Common Criteria EAL4+ certifications for Borderware’s products.

For the past two years, Peter has focused on researching VoIP security issues and has written a number of white papers including a survey of the threats facing VoIP applications and a discussion on the ability of standard firewalls to address each of these threats.

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

About Phil Zimmermann

Philip R. Zimmermann is the creator of Pretty Good Privacy, an email encryption software package. Originally designed as a human rights tool, PGP was published for free on the Internet in 1991. This made Zimmermann the target of a three-year criminal investigation, because the government held that US export restrictions for cryptographic software were violated when PGP spread worldwide. Despite the lack of funding, the lack of any paid staff, the lack of a company to stand behind it, and despite government persecution, PGP nonetheless became the most widely used email encryption software in the world. After the government dropped its case in early 1996, Zimmermann founded PGP Inc. That company was acquired by Network Associates Inc (NAI) in December 1997, where he stayed on for three years as Senior Fellow. In August 2002 PGP was acquired from NAI by a new company called PGP Corporation, where Zimmermann now serves as special advisor and consultant. Zimmermann currently is consulting for a number of companies and industry organizations on matters cryptographic, and is also a Fellow at the Stanford Law School's Center for Internet and Society. He was a principal designer of the cryptographic key agreement protocol for the Wireless USB standard. His latest project is Zfone, which provides secure telephony for the Internet.

For more information, please visit Phil’s web site, <http://philzimmermann.com/> or the Zfone project web site at <http://zfoneproject.com>