

UM Labs offer Workshops, Seminars, Consultancy and Live Demonstrations to educate and advise a range of audiences. We can present at industry conferences or perform detailed audits and consultancy for corporates and public organisations.

The agenda below is for the one-day VoIP Security Workshop – which is usually held at the UM Labs training facility near Heathrow airport. The number of delegates is usually between 8 and 12 to allow specific areas to be discussed and demonstrated in more detail. This workshop can be tailored for other venues and for individual organisations.

Workshop Objective and Approach: to explain and explore the Security challenges that face VoIP networks today and in the future and review the security technologies that are available to protect against security risks. The agenda is flexible to allow certain topics or vendor-specific issues to be covered in more detail.

Audience: we find that a wide range of business managers are now involved in VoIP and Unified Communications. We cater for Network Managers, IT Planners, Security Officers, Facilities Managers etc. The delegates are often concerned with:

- Understanding the scope and impact of VoIP Security threats such as call flooding, call monitoring, caller ID spoofing and call disruption
- Utilising secure Data networks for Voice – without compromising security
- Including all their users on a VoIP network – utilising insecure public internet connections
- Trying to get PBX systems inter-connected and working with to SIP trunks

Agenda: this runs from 0930 through to 1630, with a couple of breaks and 1 hour for lunch; there is time for further discussion at the end.

Welcome and Introduction: Structure of the Day; Special Topics to be covered; Ask Questions.

Voice over Internet – VoIP: survey of VoIP protocols; industry standards based; proprietary.

VoIP, SIP, Unified Communications applications: voice; video; instant messaging; presence.

Security Threats: categories of Network Level; Application; Content and Media.

SIP Trunk: Vulnerability and interoperability issues.

Cellphone, Softphone and WiFi: the latest vulnerabilities.

Demonstrations of the Threats:

- call disruption,
- call eavesdropping
- denial of service

Assessing the Threat Impact:

Review of Security Technologies: strengths and limitations.

Defining an effective Security model:

VoIP vulnerability Assessment.

Conclusion and Further Questions, Answers, Discussions.