Security guide for H.323

This guide discusses the potential security threats to an Internet Protocol (IP)-based videoconferencing system and the measures that can be taken to help combat those threats. The guide is aimed at sites deploying such H.323 videoconferencing systems in the UK Higher and Further Education communities, but may be equally applicable elsewhere.

This document assumes the reader has experience of ISDN (Integrated Service Digital Network) and/or IP-based videoconferencing systems. It addresses concerns about IP videoconferencing security, both in the implementation of an IP videoconferencing solution and in the use of IP videoconferencing. The Video Technology Advisory Service (VTAS) [VTAS] has already produced an introductory guide to H.323 videoconferencing [H323-INTRO], which readers not familiar with H.323 are strongly advised to read first.

Other useful reading includes the results of the UKERNA Video over IP Demonstrator project and the report of the subsequent H.323 Architecture Group [H323-ARCH], both of which covered many issues, including security. Documentation on the JANET Videoconferencing Service is also available online [JVCS-IP].