Abstract

Lawful interception of telephone calls is a monitoring tool used where the approaches of traditional inquiry are insufficient to produce legal evidence, once properly authorized by the courts. Whereas in traditional telephone technology interpretation can be carried out by just tapping the subscriber's line, in Voice over IP the question can become complex, by its inherent characteristics of mobility, security and the varying paths traversed by signaling and media traffic. Due to the growing use of the Voice over IP systems, laws and technical standards have been created to regulate the intercepted voice traffic by service providers, in consequence of court orders. Nevertheless, even if a specific infrastructure might provide the necessary conditions to identify and intercept the traffic in a reasonable time, in accordance with the regulations, there are still possible difficulties in the interpretation of this content itself, if the media is using mechanisms to guarantee privacy. In contrast to the plain old telephonic system, Voice over IP protocols provide cryptography as a standard feature, and its routine use will make lawful interception process impractical. This dissertation describes the initiatives to provide lawful interception and details of the SIP protocol, including its associated security protocols, pointing up the technical difficulties to proceed with wiretapping in this environment. It presents a new proposal to manage session keys used to protect media streams, as a way to permit the key recovery. Finally, comparisons of the proposal are made with other standards-based alternatives for key recovery, indicating the advantages and disadvantages in the application of the cases where a key escrow system is used.

Key-words: VoIP. Lawful Interception. SIP. Kerberos.