SECURITY MECHANISMS OF VOIP-TELEPHONY

Bilash D.A., Tkachov V.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The security of transferring data has a significant impact on the popularity of services of any type of telephony. Therefore, theoretical research of the increase of the degree of security is the important topic of the development of transferring data on the Internet [1]. While most of the technical hurdles appear to have been overcome, security still constitutes a major concern.

The purpose of this work is to analyze methods of increasing the security of IP-telephony. The most popular methods are using IP-security (IPsec) and secure real-time transport protocol (SRTP). IPsec is a framework for securing IP communications by encrypting and authentication each packet. There are two types of working. In the first mode, only payload packets are encrypted. That is a reason why this mode is suited for host-to-host over LAN. In the second mode, the entire IP packet is encrypted. Also, every IP packet needs to be encapsulated in a new packet for routing these packets. This method can be used for network-to-network, network-to-host and host-to-host over the Internet. SRTP provides the ability to encrypt transmitted messages, authenticate them, verify their integrity and prevent the possibility of playback attacks. Playback attacks carried out with interception and key substitution). But there is an important point in the work of SRTP it is the need to support encryption on both sides between which data transfers.

There is another well-known security mechanism that has well-served data networks is the use of NATs. When it secures a connection via this mechanism it needs to access the NAT. But there are DoS attacks which can cause lost this access. Authentication and identification can be used to prevent these attacks [2-3].

Thus, the development of VoIP- telephony provides a wide area of research on the topic of securing data that is transferring via the local area networks and over the Internet. Future researching will focus on increasing the errors tolerance and decreasing the delays in encrypting transferred data.

References

1. Кучук Г.А. Многошкальное вейвлет-моделирование трафика мультисервисных сетей / Г.А. Кучук, О.О Можаєв, А.А. Коваленко // Радіоелектронні і комп'ютерні системи. – 2009. – № 6(40). – С. 231-239.

2. Tkachov V.M. Automated Controllers Functioning Criteria in Content Distribution Systems / V.M. Tkachov, V.E. Savanevych // Scholars Journal of Engineering and Technology. – Volume-2: Issue-3A. – Apr-May; 2014. – Pp. 491-497.

3. Ткачёв В.Н. Анализ показателей качества передачи речевых фрагментов через пакетные IP-сети. Вероятность их идентификации / 14-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке», 18-20 марта 2010 г.: Сб. материалов форума. Ч.1. Конференция «Телекоммуникации» – Харьков: ХНУРЭ, 2010. – С.177.