APPLICATION OF IP-TELEPHONY AS A SECURE ALTERNATIVE FOR GSM COMMUNICATION

Uchaev N. A., Smirnova Z. D., Petrov S. N.
Scientific adviser: associate prof. Petrov S. N.
Belarusian State University of Informatics and Radioelectronics, Belarus
E-mail: petrov@bsuir.by

Abstract — The article deals with mechanisms of protection, ensure data transmission in GSM networks and methods of designing of security systems for voice transmission, using the IP-telephony.

1. Introduction

Mobile cellular networks are used everywhere. Unfortunately, to date, in connection with the development of industry, the authentication mechanisms used in data networks and encryption mechanisms are not allowed to confidence in the safety of the data transmitted.

The report describes the theoretical mechanisms of the protection of data used in the networks of the 2nd generation, methods of analysis of data transmitted in communication networks and techniques of organization networks secure voice-based IP-telephony.

2. Main part

Second generation mobile communications standard in many respects is complicated by a problem of unauthorized access to the transmitted data. Unfortunately, the second generation networks continue to be used and it will last for years to come. In the second generation networks, There are two vulnerable components: a base station authentication mechanism and encryption mechanisms.

The use of jammers to jam the frequencies legitimate base stations in places with unstable reception (underground parking, subways, warehouses) and project developments OsmocomBB (figure 1), for the organization of the cell, and subsequent attacks "man in the middle" will allow to capture the flow of voice data. Applicable stream encryption algorithm A5/2 allow in the presence of rainbow tables and GPU – to get the raw data in a very short period of time (a few seconds).

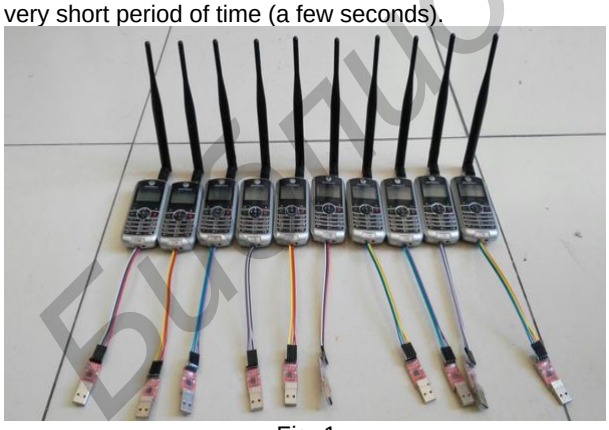

Fig. 1

In the case of mobile applications for interdepartmental transfer of information or as a means of business communication, this creates a real possibility of data leakage.

IP-telephony systems, in particular, using the SIP-protocol, have a number of possible scenarios that increase the security of data transmitted. For authentication, the central server can be used SSL-certificates, and for encryption of transmitted data - specialized solutions for SIP (SIP/TLS, ZRTP), and classic VPN tunnels, for example – L2TP and IPSEC.

This communication system can be deployed within the organization and used for internal negotiations, as well as to communicate with the partner companies that use similar solutions. Moreover, in contrast to the expensive and inconvenient scramblers, this solution does not require long-term financial investments. Software packages are free (Asterisk project [1]) functionality to the IP-telephony today is present in every modern smartphone. As the transport network can be any available Wi-Fi network, Ethernet-connection or the mobile Internet on the smartphone.

To ensure access to the public network can be used by GSM/PSTN VOIP gateways, attacks that will be much easier to track because of static placement of these devices.

3. Conclusion

Revealed the vulnerability of second-generation GSM networks to attacks, "man in the middle" and the weakness of the encryption algorithms.

The usage of IP-telephony system as secure voice network has been proposed.

4. References

[1] Welcome to the OsmocomBB project [Electronic resource] / OsmocomBB. — Access mode: http://bb.osmocom.org/trac.
[2] Ready To Get Started With Asterisk? [Electronic resource] / Asterisk. — Access mode: http://www.asterisk.org.

ПРИМЕНЕНИЕ СИСТЕМ IP-ТЕЛЕФОНИИ В КАЧЕСТВЕ БЕЗОПАСНОЙ АЛЬТЕРНАТИВЫ GSM СВЯЗИ

Учаев Н. А., Смирнова З. Д., Петров С. Н.
Научный руководитель:
канд. техн. наук, доц. Петров С. Н.
Белорусский государственный университет информатики и радиоэлектроники, Беларусь

Аннотация — В докладе приводятся теоретические данные о механизмах защиты, применяемых в сетях второго поколения, методики анализа передаваемых данных в сетях связи и методики организации сетей безопасной передачи голоса на базе IP-телефонии.