Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 123 (2018) 457–466

Procedia Computer Science

www.elsevier.com/locate/procedia

8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017

Text Messages Protection System

Andrey Starikovskiy, Arseniy Zhgilev, Nadezhda Shevchenko

National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute)
Kashirskoe highway 31, 115409, Moscow, Russian Federation
avstarikovskij@mephi.ru

Abstract

This paper deals with the development of text messages protection from unauthorized access and malicious software. The structure of an attacker model and main security threats are provided. The article tells about the requirements for protective systems of this kind, examines the main information security threats. The tools of system development such as protecting messages using the RSA algorithm, using ELGamal algorithm and using an algorithm based on elliptic curves are described. The performance results and effectiveness of the proposed ideas are provided. The implementation can be performed directly on mobile subscribers in the form of a software product, or as additional functional software of a virtual operator. The proposed protection system can significantly enhance security of mobile communication.

Keywords: protection of text messages, message encoding, key length, unauthorized access, security threats, intruder model

1 Introduction

Nowadays providing information security for mobile devices and processed in mobile networks data is an issue of great interest and importance. As mobile phones and tablet computers are provided with broader functions, the number of vulnerabilities is growing dramatically. Today an intruder can get an access to device, secretly make calls and eavesdrop them, send and steal texts, install malicious and spy software, get confidential data, get user location, steal money and even put the device out of order (Zhukov 2013, Mikhaylov 2013; Mikhaylov 2015a).

Many scientific papers discuss protection tools for mobile devices. For example, security software protecting from malware (Dube 2013, Mikhaylov 2014), data leakage (Sbirlea 2013, Taenam 2013) eavesdropping prevention mechanisms, algorithms for data analysis and detection of changes in the security level of data transmission in wireless networks (Mikhaylov 2014), etc.

One of the most popular ways of mobile communication is text messaging. Texts are quick, concise, and precise, stored in the phone memory, and can be reread at any time.

10.1016/j.procs.2018.01.070

However, they can contain confidential information as passwords or private intimate information, etc. Moreover, an intruder can send a malicious command on the phone via text infecting the device or even taking control under it.

This problem is topical as (Gojevic 2012) discusses a mobile network protection system against fraudulent and unwanted messaging traffic. Kashif, Mhair (2014) proposes a secure texting using encryption gateway and digital signature. However, the existing tools are not enough as new threats appear every day. They can take a lot of production capacity, memory, etc.

As text services are widespread today, this article will be devoted to the protection of transmitted messages from malicious attacks. The research presented in the paper can be used to improve existing mobile security means, eliminating the vulnerabilities and ensuring more effective information protection (Mikhaylov 2015b).

2 Text messages protection system

2.1 Intruder Model and Main Security Threats

In order to create tools protecting mobile devices from malicious software and unauthorized third parties access, it is necessary to formulate the requirements for these tools. In turn, the requirements are stated based on the model of the offender. (Mikhaylov 2015)

An intruder model should be structured as follows (Certificate FSC 2008):

— description of violators (subjects of attacks);

— assumption about information about the objects of attack available to the offender;

— assumption of existing intruder means of attack;

— description of the objects and purposes of the attack;

— description of the attack channel.

The main security threats for information transmitted over the communication channel of the cellular networks comprise:

— implementation of passive listening radio by the intruder;

— attack on the equipment of network subscribers (Mikhaylov 2014);

— interception of information through communication channels of network operators, change, distortion and redirecting of the transmitted information;

— overloading of operator's equipment, kill of the communication system;

— deliberate sale of confidential information to third parties by operators;

— deliberate provision of false information to the subscriber for the purpose of deception, misleading and sabotage;

— gathering data through third party applications installed by the user;

— use of vulnerabilities in operating systems of phone equipment;

— use of vulnerabilities of integrated systems;

— use of users' confidential data by companies developing software-hardware devices in exterior objectives. (Mikhaylov 2014)

There are two major threats to the text service: the threat to the confidentiality of information transmitted in the body of the message, as well as distortion of the texts in the part of the sender's address.

Texting allows sending 1120-bit of alphanumeric messages between mobile phones and external systems at a time. They are transmitted via the mobile network in plain text. Content is stored at the text system's operator and is available to employees. A5 algorithm is a stream cipher used for encoding data transmitted over the GSM standard and can be easily hacked (Dave 2006). Thus, it is necessary to add extra coding for transmitted messages.

The coding can be divided into two categories: symmetric and asymmetric. In symmetric coding the