THE APPLICATION OF STEGANOGRAPHIC ALGORITHMS ON UP-TO-DATE MOBILE PLATFORMS

VLADIMIR S. GALYAEV

ABSTRACT: *The article examines the applicability of steganographic techniques on up-to-date mobile platforms. It reviews the software using the steganographic algorithm and determines the characteristic features of these programs. The article gives the testing results of the author's own developments of mobile applications for steganography*

KEYWORD: *Ssteganography, mobile applications, information security*

Introduction

Over the past two years the focus on development of information technologies has fully shifted to mobile ones. Most of the researches, developments, large financial projects and attractive startups are concentrated in this sphere. Mobile applications penetrate into the various sectors of economy. Earlier mobile applications have covered mainly games industry and communications (instant messengers or social networks connection), but now they allow you to deploy a mobile office, conduct advertising campaigns, track traffic, etc. Though in 2015 the Russian mobile market showed the lowest growth for the first time since 2009, it definitely impresses. According to the report of J'son & Partners Consulting the aggregate sales in Russia were 25.3 million smartphones and more than 14.2 million tablets in 2015. The same report predicts by 2020 smartphones fully oust ordinary mobiles from the market. Besides even today they become a necessity for many people and in spite of the difficult economic situation users continue to buy smartphones. Another feature of 2015 was the rapid spread of add-on devices that can be integrated with the smartphones.

If the mobile phone market showed some slowdown, the mobile apps and services market via mobile devices gave a steady increase about 170-180% per annum. More and more people are using mobile devices for the Internet access. According to Russian telecom operators from 82 million network users 50 million people use the mobile Internet. For example, about 11.8 million users – more than 10% of the population – go online only from mobiles. For November 2015 54% of traffic was mobile one. The mobile advertising expenses increased by 2.2 compared to 2014. At least 20% of profit organizations have either their own mobile app or site. In 2015 mobile apps sector grew fast for public and municipal institutions: tracking the public transport, making appointments with the government agencies, etc.

Moreover people began actively use personal mobile devices to perform their job functions within the organization. Besides it becomes available for users to connect to the local network and to have access to key information resources. More than half of executives support the ideology of BYOD (bring your own device) believing that it helps cost savings and increases the employee's efficiency.

Thus, we have the following: mobile devices are used for personal purposes as well as for working needs, at the same time they allow users to gain access to critical data among a wide variety of applications and various files formats.

1. Problem statement

An access to corporate resources leads employees into temptation to transfer these data to competitors. However a direct transfer can be monitored by the IT department or the Security Service. Besides the encrypted data transmission cannot help the insider, as only the fact of the

transmission is important. Moreover the transfer of the encrypted data to a potential competitor is more suspicion. In this case an interesting solution is a hidden transfer with the use of steganography techniques. Data transmission in the form of built-in innocent images or sound files are often not tracked or blocked by standard means.

It is possible to transfer not only hidden data containing a commercial secret, but hidden transmission of executable code. In April 2016 Check Point company has published exposure of fraudulent scheme against payment platform Alipay owned by Alibaba Group. The hackers have turned to an employee of one company (the company name is not disclosed in the interests of the investigation) dealing with the game software for mobile platforms for putting the malicious code into one of their ongoing developments. As this company was in the white list the malware program was easily passed free anti-virus of Qihoo 360 – one of the largest Chinese market players of antivirus products. As the infected program is propagated through third-party software the full check isn't also carried out. The main purpose of attackers was the users of online sales system Taobao.com (analog Ebay in China). This system's characteristic feature is a specific purchasing products' scheme: in order to purchase a favorite item from the seller the buyer sends him a picture of the lot with the help of a special messenger AliWangwang. After that the seller approves the transaction and the payment is made via Alipay associated with this online sales system. The malware by means of steganography embedded a specially built malicious code in the sent pictures. This code installed a keylogger on the seller's mobile device as soon as he received pictures. The attackers had initiated the refund procedure to force the seller to enter their credentials in Alipay after infection. The credentials were intercepted and used for the further withdrawal of money from the payment system.

Thus, it becomes more and more important to study the application of steganography techniques for transmitting hidden messages within the mobile Internet, as well as finding ways to counteract this transmission.

2. Analysis of the software market

If we consider the platforms' division for mobile devices (smartphones and tablets) there is the following correlation in the Russian market at the moment:

- Android (4.4 version and above) – 71.1% (global level 61.54%);
- iOS (6 version and above) – 21.4% (global level 25.16%);
- Windows (including Mobile) – 5,2% (global level 1.92%);
- other systems – 2.3% (global level 11.38%).

For Windows family it is possible to use the software written for personal computers and laptops. This issue has already been studied [1, 2]. Therefore within the current study we decided to focus on the Android platform.

We could identify only one application in the course of studies of the official Google Play store. It is "PixelKnot: Hidden Messages" of The Guardian Project Company. At the end of April 2016 the application had 0.3.3 version, posted June 26, 2015 with more than 10 000 downloads. According to the submitted reviews it was identified some problems with starting and using the applications in a large number of devices, including the inability to extract the image on another device. The research team has installed this application to 8 different smartphones and 3 tablets' models. As a result the application couldn't be started in 3 smartphone models. Also it was impossible to extract hidden information which was installed and transferred via a cloud service Google Drive in 25% of experiments.

We searched for the steganographic programs for mobile platforms propagated through other software providers. So there were 5 different setting software packages (apk-files): two of them carried the malicious code detected by antivirus programs for mobile devices Eset Mobile

Security and Kaspersky Internet Security; the third program hid information by direct bonding files; and the last two ones had the same features as discussed above PixelKnot: Hidden Messages.

As a result it should be noted that the market of steganographic programs for mobile devices is absolutely undeveloped today.

3. Carrying out the experiment

A research team had developed their own application for Android mobile platform. It has not hosted on Google Play but propagated as apk-file. The application realized DCT LSB method working with JPEG-images.

The anti-virus programs referred above did not respond to this program; they consider it valid.

In the experiment this application was installed in 8 different smartphones and 3 tablets' models. The black-and-white picture was used as a latent image: 3% black and 97% white color (drawing). 6 different kinds of image quality were studied as packages: from black-and-white to full-color of high quality.

The average processing time of an image by the mobile program is 2.5 seconds. The image's volume changing was not revealed. Thus, the hiding information is not detected.

The images were transmitted in several ways:

- through cloud services: Google Drive and DropBox;
- through messengers: WhatsApp, Viber, Telegram;
- through social network's applications: VK, Facebook, Instagram.

In all cases the data transfer has been implemented with the opportunity to retrieve the hidden information in the package. So the information wasn't lost during data transmission.

Thus, we have proved the possibility of transferring steno messages using only the mobile platforms capabilities.

Conclusions

This study was devoted to the considering the possibility of using steganographic methods and a computer experiment on the implementation of steganography techniques for hiding images in pictures. The implementation is quite possible and isn't detected without special software. Furthermore, our plans are to develop some tools for banning the hidden data transmission and identification of steno messages within the study.

REFERENCES

1. **Galyaev V. S.** Transmission of steganographic messages using social networks // Fourth International Scientific Videoconference of Scientists and PhD, students or candidates "Trends and Innovations in E-business, Education and Security", Bratislava, November 19. 2014. P.17-22.
2. **Stanev S. S.,** Paraskevov Kh., Galyaev V.S. Meaningful comparisons of Bulgarian, Russian and English scientific terms for network steganography. Collected papers of the scientific-practical conference with international participation from the Naval Academy "Sea Days 2013", Varna, 07.2013.