Mobile Phone Security: Side Channel Point of View

Roman Mostovoy, Pavel Borisenko, Alla Levina
Saint-Petersburg National Research Institute ITMO
Saint-Petersburg, Russia
ramostovoy@corp.ifmo.ru, borisenkopp@yandex.ru, alla_levina@mail.ru

***Abstract*—Mobile phones implement a lot of functions in addition to their original destination. You can control various area of your life through mobile phone. That gadget can accumulate, process and get access to extremely big amount of data including sensitive data. In the same time not many people really take care about security of their own devices assuming that the issue must be solved by default. Our purpose is to examine mobile phone security from the side-channel attacks point of view during different cryptographic computations using passive methods of signal detection.**

I. INTRODUCTION

The number of operations that a person can do with a mobile phone is growing rapidly. Especially now, when cloud services and methods of automation gaining growing in popularity, the mobile phone becomes the key not only to sensitive data of its owner, but also to the management of critical information flow or automated systems.

And that key is often left unattended, allowing an attacker to gain access to the device and, in particular, to register a spurious signal. Moreover, popular accessories, such as rechargeable high power battery or protective cases may carry additional malicious recorders of electromagnetic radiation or power consumption.

Using the shared medium for communication is the factor that makes the phone (and any other device with wireless communication) especially vulnerable. Sniffing of the traffic is an elementary task, and only a "cryptographic" barrier rests between the attacker and the data.

The first group of applications, an attacker potentially interesting in are various voice, text or video messaging services. In the case of the encryption apparatus performs a large number of computational operations of the same type (atomic in case of text messaging, or continuous in case of data streaming). Thus, at the disposal of the attacker may be a sufficient number of parasitic signal traces in order to determine the key. If that happens before the key is out of date, the entire flow of information will be disclosed to the attacker.

Secondly, the applications that provide shared access to data may be vulnerable. Some cloud storage work with the so-called user-controlled cryptography (when the encryption of data transmitted to the host is made on the device). It allows host system to implement more weak methods of stored data protection (and remove responsibility for the content). However, it creates a vulnerability to side-channel attack. Otherwise, even if host system is completely responsible to the security of the stored data, the protected connection channel and the authorization data (for example, which stored in an encrypted vault on the device) can still be the target of an attacker [5]. However, the task in this case, from side-channel attacks point of view, is more complex.

The third risk group is applications designed to integrate the phone into the Internet of Things (IoT) and a variety of services world, that are associated with the management of a variety of material and not material objects, processing of the status messages, making certain decisions. It also may include, for example, banking and other payment applications. In this case, of course, the main goal for the attacker will be the authorization data, but in addition to privacy of the data [4], an important role is played here by their integrity and availability, so that the task of ensuring the security of these applications is even more difficult and complex, and in addition of cryptographic protection in such applications should be implemented communication high-quality protocols, precluding, for example, a control command transmission to any device without proper authorization.

But we can't ignore the fact that there are many different power consumers excluding processor in the mobile phone: screen and various communication modules (GSM-module, Bluetooth, WiFi, NFC). For obvious reasons, these consumers usually work at the same time with the applications described above. It creates additional difficulties in the registration of traces, as all of these energy consumers can also make a noise in the side channels, but this noise is little informative, for example, in terms of the search of the encryption key. As we will show further, attacker is forced to take it into account.

The rest parts of the paper is organized the following way: in the second part we will observe our objects of research and methods of trace recording, in the third part some obtained results will be presented and, in conclusion, further purposes and probable applications of this research will be viewed in the fourth chapter.

ISSN 2305-7254

II. Object of research

In scope of this research we decided to concentrate on attacker's model with low-level opportunities regarding equipment. It also has defined requirement to software which was examined. It was important to perform restricted well-controlled computation operations. We are analyzing two mobile applications for Android operating system and several models of mobile devices.

The first application is more approximate to the production mobile chat with support of PKI based on the presence of a trusted central server. It allows you to simulate a real attack conditions on the mobile device, which at the same time have a number of negative features:

1) Any application seeks to interact with the user in many ways and the most basic one is graphic user interface (GUI). Working with GUI elements leads to active power consumption from the phone screen, making it difficult to identify parasitic signal directly related to cryptographic operations.
2) Users often become distracted by the actions that do not lead to the implementation of cryptographic operations on the device. Their attention is distracted by other applications, external stimuli, etc. It leads to noisy parasitic signal and a lot of data which the attacker is not interesting in.
3) Even if the user is fully concentrated on the actions that lead to qualitative parasitic signal (for example, sending messages to other users via a secure channel), he/she makes them slow, and hence, with a limited period of time you are able to get a very small volume of required data.

Due to the large number of constraints imposed on side-channel attacks by production applications, another special application has been developed, which is a "sandbox" of cryptographic primitives. Its concept is to minimize GUI, which is not used at all during the cryptographic operations, easily extensible set of cryptographic primitives and controllable set of secret encryption keys used. In addition, the application allows you to perform the necessary cryptographic operations at a high frequency for the rapid accumulation of sufficient data to carry out your attacks.

The full list of features is the following:

1) 3DES, AES, RSA and DES encryption are supported;
2) The list of secret keys is controllable;
3) Time-stamps and detailed logging are supported because it is very important to keep synchronization between the data and attacking tool;
4) High frequency of cryptographic operations with controllable delay. The same functionality was implemented for production application to facilitate data gathering.

Based on the fact that the attacker does not use expensive equipment to carry out attacks only two easily accessible tools were used for traces recording - external sound card and jack-jack cable:

Fig. 1. Test installation

III. Data analysis

First of all we would like to notice that registered signals strongly depend on a user's behavior and cryptographic computations which were performed in “silent” mode have much more clear traces:

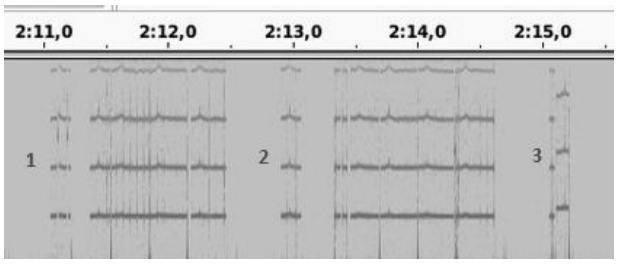

Fig. 2. Clear trace for Alcatel POP3: each time of message sending is numbered and clearly visible

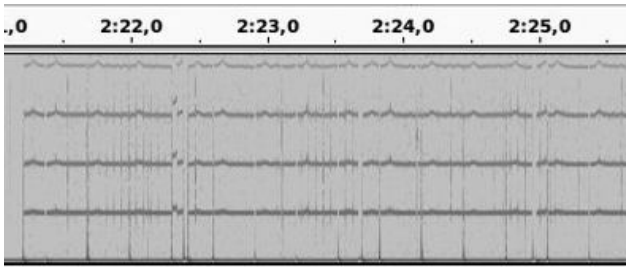

Fig. 3. Noisy trace for Alcatel POP3 during user interaction

It is worth noting that in addition to user behavior and implementation of applications on his phone, there is an equally important factor - installed hardware - which could equally be a problem for attackers and a useful tool. For example, we did a comparison of the acoustic parasitic signal from two phones: Sony Xperia M2 and Alcatel POP3. And there is a dramatic difference in the definition of the data. We got the distinct peaks in the moments of cryptographic operations (see Fig. 4) performing for the second device, but totally undiagnosed flow noise - for the first one.

This shows that different mobile devices are susceptible to side-channel attacks in different rate and, most importantly, manufacturers are able to influence the rate by changing the hardware architecture.

Side-channel attack can be based on various sources of data. But, whatever the source, it often has the need for crude parasitic signal pre-processing and depends on its quality. Furthermore, various attacks are based on different approaches

of data processing in terms of mathematics – the main influence is the encryption algorithm used for devices.

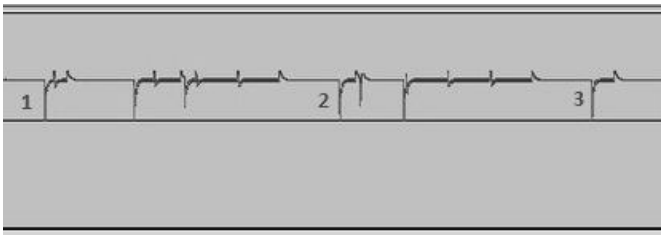

Fig. 4. Times of cryptographic operations on Alcatel POP3

We planned to use the most versatile approach for the analysis of parasitic signal based on artificial neural networks as possible in independence of cryptographic primitives used in the mobile device. It should be noted that this approach does not imply an absolute identification of a secret device key, but allows you to determine the most probable state for each of its bits.

On the first stage of trace analysis it's necessary to check if obtained traces are key- and plaintext-dependent. We've used multilayer perceptron for this purpose. In this paper we limit ourselves with this task. Further, in case of such dependence exists it is possible to teach multilayer perceptron to distinguish two keys which differ by only one particular bit.

In next stage we are going to use convolutional neural network (CNN) with convolution matrices configured using weights from networks prepared on the previous stage. It will allow make so called feature maps to distinguish each bit of the key.

There are a number of reasons for choosing convolutional neural network as a main analyzer for the key derivation task. First of all, particular bits of the key impacts to only particular trace parts. And it can be taken into account by CNN. Hence, there is a less amount of configurable links in such network than in multilayer perceptron.

Furthermore, convolution computations can be performed using many streams easier than most of networks with other topology. Finally, deep machine learning can examine much more complexity correlations [3].

The disadvantage of neural networks as a tool for analysis, is their low efficiency for a data containing a large number of features. In the case of parasitic signal the attacker is not able to independently distinguish important features of each trace. To solve this "curse of dimensionality" problem, we use normalized inter-class variance (NICV) method [1], which allows distinguish the most vulnerable features of traces, based on the data classification and detection of anomalous dispersion deviations.

IV. Conclusion

Mobile phones and wearable devices are very important part of today's information infrastructure. Therefore, the issue of their safety is becoming more critical every day. At the moment, in combination with other researchers [2], we can say that there are opportunities for attacks on these devices without the use of expensive equipment and, more important, in a passive way, without the threat of exposure for attackers.

Thus, this study aimed to determine the vulnerability of the test devices to the passive side-channel attacks, and its results can serve as a basis for certification testing.

Acknowledgment

We would like to thank Aleksandr Ometov and Sergey Andreev from Tampere University of Technology for what they interested us in the topic of side-channel attacks in the field of Internet of Things.

References

[1] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, Zakaria Najm, "NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage", vol. 3, p. 5, 2013.

[2] Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer, Yuval Yarom, "ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels", vol. 3, pp. 3-4, 2016.

[3] Lukasz Romaszko, Demian Battaglia, Isabelle Guyon, Vincent Lemaire, Jordi Soriano, "Signal Correlation Prediction Using Convolutional Neural Networks", *JMLR: Workshop and Conference Proceedings*, pp. 45–56, 2015.

[4] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, Klaus Wehrle, "Privacy in the Internet of Things: threats and challenges Security and Communication Networks", 2014.

[5] Garrett S.Rose, Dhireesha Kudithipudi, Ganesh Khedkar, Nathan McDonald, Bryant Wysocki, Lok-Kwong Yan, *Nanoelectronics and Hardware Security Springer Advances in Information Security*. Springer New York, pp. 105-123, 2013.