CONSTANTINE
THE PHILOSOPHER
UNIVERSITY
IN NITRA

Mobile device security

Department of Informatics
FPV UKF in Nitra

Introduction

Smart devices such as mobile phones and tablets every day are increasingly more widely used in the current communication in organizations of various types. The number of these devices is growing rapidly and with it the threat generated by different ways interfere with their functioning.

In our work we monitor the behavior of the mobile device with factory settings. Our purpose is to find out if these devices already at its first connection to the network threaten the privacy of the user.

Device security

Mobile devices often contain or have access to sensitive information that should be protected. Using smartphones brings new security risks that every user should consider before working with information that is somewhat private [1].

Kudakwashe [2] states that over time, mobile devices have become the target of all types of attacks that exist for traditional computers. Therefore, mobile devices should be protected by a wider set of security techniques than traditional desktops or laptops.

Reasons endangering safety

The most common problem is that users do not have a physically secure phone. Some users also forget to lock sensitive apps [3].

Another problem is that wireless WiFi connections are not always encrypted. There are many applications that do not implement encryption of data that are transmitted and received over the network [4].

Many users ignore the notification that a new platform update is released. With an unaddressed platform, apps are also not being updated many times, resulting in no security patches being installed [5].

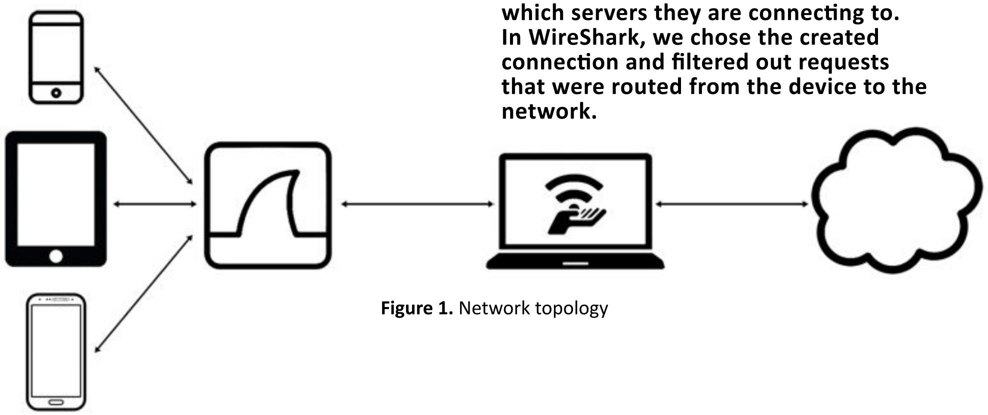


Figure 1. Network topology

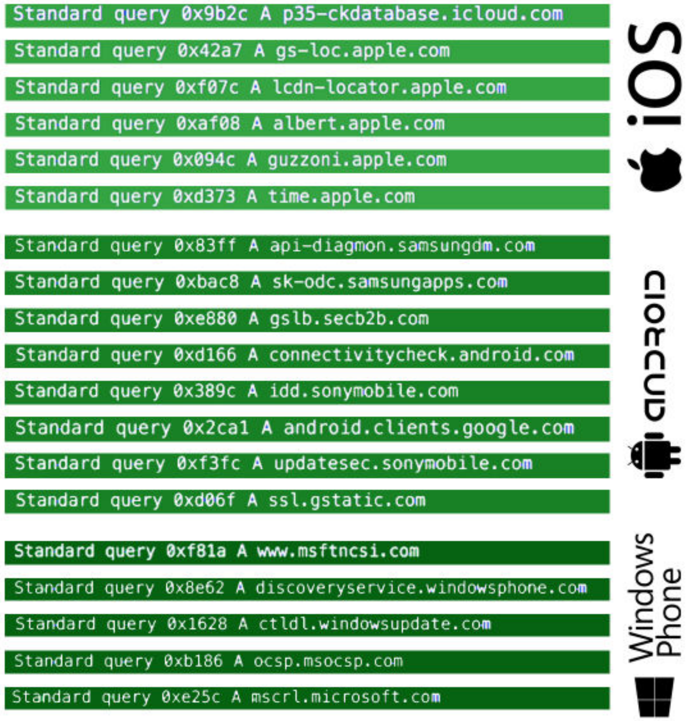
Security testing process

At first we determined which mobile devices will be tested. In the next step, we used a tool to create an access point that we then connected to each device.

Figure 1 shows the involvement of individual components - mobile devices, network connectivity devices, and a tool that provides capture and analysis of communications.

Once the access point was created, we connected the devices to the wireless network that we created and tracked their behavior. We used WireShark (Fig. 2) to capture and analyze data.

We've set all tested devices in the factory settings so that we can determine exactly which packets are sent to the servers and which servers they are connecting to. In WireShark, we chose the created connection and filtered out requests that were routed from the device to the network.



```
Standard query 0x9b2c A p35-ckdatabase.icloud.com
Standard query 0x42a7 A gs-loc.apple.com
Standard query 0xf07c A lcdn-locator.apple.com
Standard query 0xaf08 A albert.apple.com
Standard query 0x094c A guzzoni.apple.com
Standard query 0xd373 A time.apple.com

Standard query 0x83ff A api-diagmon.samsungdm.com
Standard query 0xbac8 A sk-odc.samsungapps.com
Standard query 0xe880 A gslb.secb2b.com
Standard query 0xd166 A connectivitycheck.android.com
Standard query 0x389c A idd.sonymobile.com
Standard query 0x2ca1 A android.clients.google.com
Standard query 0xf3fc A updatesec.sonymobile.com
Standard query 0xd06f A ssl.gstatic.com

Standard query 0xf81a A www.msftncsi.com
Standard query 0x8e62 A discoveryservice.windowsphone.com
Standard query 0x1628 A ctldl.windowsupdate.com
Standard query 0xb186 A ocsp.msocsp.com
Standard query 0xe25c A mscrl.microsoft.com
```

Figure 2. Captured DNS packets with WireShark

Results

We've found that Windows Phone devices are the safest in terms of networking, so users should also consider this platform when they buy the device.

The most commonly used Android and iOS platforms have shown a certain degree of threat, as they automatically, without the user's knowledge, send private data.

However, each device becomes the safest when accepting alerts and applying proposed safety methods and tools.

References

[1] Hevesi, P. 2016. Mobile Device Security: A Comparison of Platforms.Gartner. 2016. https://www.gartner.com/doc/ 3276422/mobile-device-security-comparison-platforms.

[2] Kudakwashe, M. a kol. 2015. Mobile Security Threats: A Survey of how Mobile Device Users are Protecting Themselves From new Forms of Cybercrimes. 10th International Conference on Cyber Warfare and Security. ACAD CONFERENCES LTD.

[3] Falconi, A. a kol. 2016. ECG Authentication for Mobile Devices. IEEE Transactions on Instrumentation and Measurement. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC.

[4] Bicakci, K. a kol. 2014. Mobile Authentication Secure Against Man-In-The-Middle Attacks . 9th International Conference on Future Networks and Communications. ELSEVIER SCIENCE BV.

[5] Dar, M., Parvez, J. 2014. Smartphone Operating Systems: Evaluation & Enhancements. International Conference on Control, Instrumentation, Communication and Computational Technologies. IEEE.

Jan Francisti
PaedDr. Peter Švec, Ph.D. (supervisor)