Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

ANALYSIS OF WINDOWS PHONE 8 APPLICATIONS

Alexander Marsalek – alexander.marsalek@a-sit.at
Version 1.0, June 2015

Abstract:
This document provides an overview of current possibilities regarding application analysis on the Windows Phone 8 and 8.1 platform. For this, it lists possibly application sources, explains the different Windows Phone unlocking stages and finally it describes possible analysis methods. The document is meant to be a short study on these two aspects, reference to further, more comprehensive work is made. It concludes that the Windows platform and its applications offer great possibilities regarding application analysis.

Contents

Version	Date	Changes made	Modified by
1.0	19.06.2015	Initial document	Alexander Marsalek

© A-SIT, Partner für Sicherheitsfragen

1. Introduction

A-SIT gained knowledge about the Android and iOS platform and the analysis of its applications through research and past projects. While Android and iOS are still dominating the market [1], the Windows Phone platform is the fastest growing phone OS in terms of market share [2].
The goal of this project is to determine the possibilities on the Windows Phone platform regarding application analysis. The most relevant questions are:

1. Is it possible to obtain the binary application file?
2. Are the binary application files encrypted?
3. Can the application binaries be decompiled or disassembled?
4. Are there any analysis tools available?

2. Obtaining Windows Phone Application Binaries

Windows Phone 7 and 8 applications have the extension “XAP”. Starting with Windows Phone 8.1, the application format was changed to “APPX” to unify the application-development platforms of Windows Phone and Windows Store applications. The apps are called universal apps.
Initially, XAP files were ZIP archives and could be opened with standard ZIP extractors, similar to Android’s APK application files. In August 2012, Microsoft started to automatically encrypt XAP applications submitted to the Windows Phone Dev Center [3] to prevent piracy [4]. The applications are encrypted using the PlayReady DRM technology[1]. During the installation phase, the operating system automatically decrypts the applications files [5]. The distinction between encrypted and decrypted XAP files is easily possible with a simple text editor. Encrypted XAP files start with “PRE” while unencrypted XAP files start with “PK”.
Universal apps have the file extension “.appx”. Interestingly, APPX files are not encrypted. These files can be downloaded unencrypted from the official Windows Phone Store as “appxbundle”. This bundle contains the APPX file among other files. The following sections introduce different application sources.

2.1. Windows Phone Store

Like Google and Apple, Microsoft provides an official store[2] for its Windows Phone platform, which can be accessed using a preinstalled application from the devices or using a web browser. In contrast to the other two platforms, the Windows Phone store allows to directly download the application binaries for manual installation [6]. In contrast to XAP application files, downloaded APPX application files are not encrypted. All Windows Phone store applications are digitally signed.

2.2. Binary from Developer

A simple way to get the unencrypted application binary or even the source code is to contact the author. This approach will especially work for projects where the customer wants a security audit of her self-developed (or commissioned) application. At least a developer unlocked phone is needed to install these applications.

2.3. Unofficial Stores

Besides the official Windows Phone store, a variety of unofficial stores exists [7]. Some of them seem to be legitimate, but others promote cracked applications. Typically, these applications have no valid signature and can therefore not be installed on an unmodified Windows Phone.

2.4. Extraction from Device

Another way to obtain unencrypted applications is to extract them from the Windows Phone device. Currently, there are two known ways to extract the applications directly from the device. Either use a rooted Windows Phone or to directly dump the contents of

[1] http://www.microsoft.com/playready/
[2] https://www.windowsphone.com/de-de/store

the flash memory and extract the application from this image. The memory image can be created e.g. using a RIFF Box[3], which allows directly reading or writing memory. The gained image is only usable if the file system encryption of the device is not activated.

3. Unlocking Windows Phone 8

Windows Phone 8 has many security features that protect the integrity of the operating system and ensure that only trusted applications can be installed. The Windows Phone 8 and 8.1 platform uses UEFI Secure Boot to verify that the boot loader is trusted and utilizes Trusted Boot to ensure that the rest of the start-up process is protected. Trusted Boot verifies that all Windows boot components are unmodified and can be trusted. After the start-up process, the Windows Phone verifies that all system components and applications are properly signed before it loads and starts them. If an application or system component has been tampered it will not be loaded and started. Unsigned applications will not be executed, they have either to be signed by the Windows Phone Store or with an organisation's enterprise development certificate. Besides these security features, Windows Phones use address space layout randomization (ASLR) and data execution prevention (DEP) to reduce the likelihood that discovered vulnerabilities result in a successful exploit. Furthermore, the Windows Phone architecture isolates one application from another and from the operating system. This sandbox is called AppContainer. Even large portions of the operating system run inside this sandbox. Every AppContainer has a security policy that defines the capabilities to which the processes have access to. Device resources such as camera, network or sensors are called capabilities. By default, only a limited set of permissions is granted to all AppContainers.
These platform features make it very hard to gain higher privileges and to keep them. Yet there are ways to circumvent some of these security features.

3.1. Developer Unlock

A developer unlock allows to install and execute a limited number of unsigned applications. To developer unlock any Windows Phone it has to be registered for development purposes at Microsoft [8] [9]. If these capabilities are no longer needed the device can be unregistered again. This kind of unlock is not only used by developers for testing purposes, but also by users to install cracked applications [10].

3.2. Interop Unlock

The interop unlock softens the application sandbox. Normally only OEMs are allowed to use a specific set of high-privilege capabilities, which can be used to change the operating system. These capabilities can also be used by third-party apps on an Interop Unlocked phone [11]. Currently, the Interop Unlock works only on a limited number of Windows Phone devices. The Samsung ATIV S was the first Windows Phone 8 device that got interop unlocked [12]. Later an interop unlock was found for the Lumia 800 [13]. Using the "JTAG" method it seems to be possible to interop unlock a variety of Lumia Windows phones [14].

3.3. Custom ROM

On a few Windows Phones, it is possible to flash Custom-ROMs that are not signed by Microsoft. This allows building and flashing fully unlocked ROMs with full root access. The Huawei Ascend W1 is an example for such a device [15].

[3] http://www.riffbox.org/category/riff-jtag-features/

4. Analysing Windows Phone 8 Applications

Several analysis methods can be used to analyse Windows Phone applications. The simplest method, is to capture the incoming and outgoing network traffic and analyse it. Source code based analysis is also feasible as long as the unencrypted application binary is available. Furthermore, automated tools exist for the analysis of Windows Phone applications.

4.1. Network

The recording and analysis of network traffic works on Windows Phone similar as on other mobile platforms. The easiest way seems to be using a tool like Fiddler or Burp Suite to record the traffic. Both tools can be registered as proxy on Wi-Fi connections. Additionally a fake root CA can be installed on the phone to enable the capturing of unencrypted HTTPS traffic.

4.2. Source Code Analysis

Several decompilers for Windows Phone application binaries exist. To decompile an application, the unencrypted application binary is needed. After extracting the binary application file, its DLLs can be decompiled with a variety of decompilers. The following decompilers seem to be the most popular ones:

- ILSpy[4]
- .NET Reflector[5]
- Jetbrains dotPeek[6]
- JustDecompile[7]
- .NET Decompiler[8]

4.3. Analysis Tools

Tangerine[9] is one example for an automated Windows Phone application inspection tool. It support Windows Phone 7 and Windows Phone 8 applications. Currently Windows Phone 8.1 is not supported. Tangerine supports static and dynamic analysis techniques. No source code is required; the (unencrypted) application binary is enough. For more details on the Tangerine tool, refer to [16].

5. Conclusion

The Windows Phone 8 and 8.1 platforms offers several possibilities regarding application analysis. Application binaries can easily be download form the official store. Currently Windows 8.1 applications are unencrypted. This circumstance may change in the future, when Microsoft starts encrypting them, as it did with XAP files.
Even with an unmodified Windows Phone it is easy to capture the network traffic. Furthermore, the static analysis of an application's source code is possible for Windows Phone 8.1 applications, as a variety of decompilers exist. For more advanced analyses, an interop unlocked phone or a phone with a custom ROM is needed.

---

[4] http://ilspy.net/
[5] http://www.red-gate.com/products/dotnet-development/reflector/
[6] http://www.jetbrains.com/decompiler/index.html?topDP
[7] http://www.telerik.com/products/decompiler.aspx
[8] https://www.elance.com/samples/net-decompiler/70593007/
[9] https://github.com/andreycha/tangerine

6. References

[1] IDC, „Smartphone OS Market Share, Q1 2015,“ [Online]. Available: http://www.idc.com/prodserv/smartphone-os-market-share.jsp. [Zugriff am 15 06 2015].

[2] Ron, WinBeta, “WPC14: Windows Phone is the fastest growing mobile OS, sees more shipments than iPhone,” [Online]. Available: http://www.winbeta.org/news/wpc14-windows-phone-fastest-growing-mobile-os-sees-more-shipments-iphone. [Accessed 15 06 2015].

[3] Todd Brix, Microsoft, „Answering your top 10 Windows Phone Dev Center questions,“ [Online]. Available: https://blogs.windows.com/buildingapps/2012/08/10/answering-your-top-10-windows-phone-dev-center-questions/. [Zugriff am 16 06 2015].

[4] R. Edmonds, „Windows Phone Dev Center now automatically encrypts all apps to prevent piracy,“ [Online]. Available: http://www.windowscentral.com/windows-phone-dev-center-automatically-encrypts-all-apps. [Zugriff am 16 06 2015].

[5] L. D. Fulgentis, „The Windows Phone Freakshow,“ Hack in The Box Conference, Amsterdam, 2015.

[6] Microsoft, „How do I install apps from an SD card?,“ [Online]. Available: https://www.windowsphone.com/en-US/How-to/wp8/apps/how-do-i-install-apps-from-an-sd-card. [Zugriff am 17 06 2015].

[7] Dominic@androidios.com, „Alternative Store for Android, iOS And Windows Phone,“ [Online]. Available: http://www.androidios.com/alternative-store-for-android-ios-and-windows-phone/. [Zugriff am 17 06 2015].

[8] Microsoft, „How to register your phone for development for Windows Phone 8,“ [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/apps/ff769508%28v=vs.105%29.aspx. [Zugriff am 18 06 2015].

[9] N. Singh, „How to: Developer Unlock a Windows Phone for Free,“ [Online]. Available: https://www.techmesto.com/developer-unlock-windows-phone/. [Zugriff am 18 06 2015].

[10] N. Singh, „How to: Install Cracked/Patched XAP on Windows Phone,“ [Online]. Available: https://www.techmesto.com/how-to-deploy-xap-to-windows-phone-device/. [Zugriff am 18 06 2015].

[11] GoodDayToDie@xda-developers, „[XAP][GUIDE] Interop Unlock for WP8 + all Capabilities,“ [Online]. Available: http://forum.xda-developers.com/showthread.php?t=2435697. [Zugriff am 18 06 2015].

[12] D. Rubino, „Let the hacking begin: Samsung ATIV S gets interop-unlocked, making it a first for Windows Phone 8,“ [Online]. Available: http://www.windowscentral.com/hacking-samsung-ativ-s-gets-interop-unlocked. [Zugriff am 18 06 2015].

[13] R. Edmonds, „Interop unlock found for the Lumia 800, intervened by Nokia,“ [Online]. Available: http://www.windowscentral.com/interop-unlock-found-lumia-800-intervened-nokia. [Zugriff am 18 06 2015].

[14] lordmaxey@xda-developers, „[SUCCESS] Interop-Unlocking LUMIA - with JTAG,“ [Online]. Available: http://forum.xda-developers.com/showthread.php?t=2713098. [Zugriff am 18 06 2015].

[15] xda-developers, „Huawei W1 JailBreak note. 2014/3/09 updated,“ [Online]. Available: http://forum.xda-developers.com/showthread.php?t=2321642&page=7/. [Zugriff am 18 06 2015].

[16] D. Evdokimov und A. Chasovskikh, „Inspection of Windows Phone applications,“ Blackhat, Abu Dhabi, 2012.

[17] S. Sabri, „Samsung ATIV Odyssey has been interop unlocked, time to hack away,“ [Online]. Available: http://www.windowscentral.com/samsung-ativ-odyssey-gets-interop-unlock-time-hack-away. [Zugriff am 18 06 2015].