**Project Description and Goals**

*Provide a description of your research proposal, written in terms easy to understand for someone outside your field. Include your project’s overall objectives as well as specific goals you plan to accomplish this semester.*

The Apple App Store is the only legitimate means for millions of people to install their favorite applications on their iOS devices. Users can download applications directly to their phones or use iTunes, a desktop application for syncing music, apps, and other information with iOS devices. Unlike competing mobile operating systems like Android, the iOS is considerably more locked down. While there are analyses of iOS applications, there is little research on the interaction between iTunes and iOS beyond the limited documentation offered by Apple. This project focuses on how iTunes handles downloaded applications prior to transferring them to the iOS device.

To install an application on iOS using desktop iTunes, the application is first downloaded to the computer from Apple servers. The application is downloaded in a format called IPA, which is a compressed archive containing code and resources such as pictures. iTunes then embeds some metadata, then transfers the IPA to the iOS device. It is possible to analyze this IPA immediately after download. The fundamental goal is to identify the extent to which the IPA can be modified and still recognized and transferred by iTunes. It is necessary to investigate whether pictures or other assets can be changed without triggering integrity protection. While Apple states that code is encrypted, we can analyze whether the encryption key is unique, meaning that each downloaded IPA is only valid for that specific user. Lastly, it is clear that a raw IPA without iTunes’ metadata invalid in iOS, but if this metadata could be replicated, there could be a possibility of installing our own albeit encrypted applications without iTunes.

**Project Significance**

*Explain in general terms why the information gained from this research project will be beneficial.*

Apple’s ecosystem is secure because it is locked down to the App Store as the only legitimate source of applications. By analyzing how iTunes treats IPA files, we could identify potential security holes, where a malicious attacker could modify his Apple-approved application to look like a bank application, install it on a device, and capture user credentials. The knowledge gained from this analysis could be used as the basis for further investigation into Apple’s application security.

**Methodology**

*Clearly state how you plan to accomplish the goals listed in your project description. Identify the specific steps necessary to perform your research.*

Using an open source tool called *mitmproxy*, we can analyze network traffic as iTunes sends a request to Apple servers to download an application IPA. Not only can the web request be examined, it is possible to intercept this IPA and dump it for analysis. This tool also allows for the substitution of the file iTunes requests with one specially prepared with iTunes not aware of any change. Using these techniques, we can start by modifying filenames in known IPAs to check how iTunes responds to changes. Depending on the former, we can make larger changes, such as substituting pictures and other resources continuing to check whether iTunes accepts the IPA.

By being able to intercept this IPA, we will compare a dumped IPA without any metadata to one that has been processed by iTunes to discover any differences to see what files iTunes added or modified inside the archive. To see the difference, we can take a unique MD5 hash of all files in both IPAs see what files have been modified. Depending on the results of the former, we will attempt to replicate iTunes’ processing step to create a final IPA that iOS successfully installs without the use of iTunes. Interception also means that we can analyze Apple’s code encryption. More specifically we would compare the same IPA that has been downloaded by two different users to see whether it is the same. We can do this by taking a unique MD5 hash of both IPAs and checking to see whether they are the same. Using these series of experiments, we can determine whether a security hole is present and whether further goals are needed.

**Time Line**

*Provide a detailed timeline of goals of your project. Be sure to include the goals listed above.*

First, we will try intercepting an IPA download as occurs, making small changes, and feeding our intercepted version back to iTunes. Depending on how iTunes reacts to these changes (ie states that downloaded IPA is corrupted), we can perform larger changes, such as replacing pictures. After experimenting with changing files inside IPAs, we will compare the files inside unprocessed and processed IPAs to identify the embedded metadata. We can then analyze the metadata and attempt to create our own, embedding it inside unprocessed IPAs and attempting to install the IPA on iOS. Lastly, we will analyze IPAs downloaded across different users and different times to identify how Apple encrypts their code.

**Background Experience**

*List any previous research experience, applicable course work, or other relevant experience you may have.*

In order to prepare myself for this research, I have taken EC440: Introduction to Operating Systems to gain insight into the inner workings of applications and the operating system. I have also taken EC327: Introduction to Software Engineering, where my knowledge of C/C++ was greatly expanded. In addition to my classes, I have done some programming projects of my own, such as *PE Section*, a library for creating and editing file headers in the (Windows) portable executable format. I have also done some work with reverse engineering eventually creating *.NET Obfuscator*, a tool for programmers to protect their software by making decompiling more difficult.

**Bibliography**

*List the sources you have consulted in preparation of this proposal, as well as any references you have cited within this application. If you need additional space, use the Appendix.*

<http://megele.io/crios.pdf>

http://seclab.nu/static/publications/ndss2011pios.pdf

https://www.cs.purdue.edu/homes/bsaltafo/pubs/CCS\_15\_iRiS.pdf