RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -12

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- What is Obfuscation?
- Importance of Obfuscation
- Obfuscation Techniques
- Pros and Cons of Obfuscation
- Security program overview
- MCQ
- References

WHAT IS OBFUSCATION?

What is Obfuscation?

❑According to the Oxford dictionary, obfuscation denotes that the action of making something obscure, unclear, or unintelligible.

❑In software, the obfuscation of code is the process of modifying an executable so that it is no longer useful to unauthorized parties such as hackers but remains fully functional.

❑But almost all the code can be reverse-engineered with enough time and effort.

❑However, most of the platforms including Android, iOS, JAVA, and .NET have their decompilers, and it can be used to reverse-engineer source code from executable files and libraries without spending more time and effort.

❑This article is focused on obfuscation techniques and how to code obfuscate in Android applications.

Importance of Obfuscation

❑Anyone who has programming knowledge can be easily captured the whole picture of the source code when the executables (for instance in Android → APK) are decompiled.

❑Although, through the obfuscation process we can add additional security to the source code and make it hard for a human to understand the code especially hackers.

❑To protect trade secrets, processes, unauthorized access, vulnerability discovery and bypassing licensing or other controls can be done by using obfuscation.

❑Obfuscation is not like encryption.

❑The main purpose of the encryption is to transform data and information to keep it secret from the external parties.

❑The actual obfuscation is to make it difficult to understand for humans.

❑Encrypted code has to be decrypted before execution, but obfuscation is not required such de-obfuscation to execute them.

Obfuscation Techniques

Few techniques can be performed obfuscations in programming. Those are as follows.

1. Rename Obfuscation

The basic transformation is used by many obfuscators such as Android, iOS, and Java. It is done with the renaming variables and method names. It is used new strings, letters, numbers, unprintable characters and invisible characters for the transformation process.

2. String Encryption

All the strings are discoverable and readable in managed executables. Even though method and variables are renamed, strings can be used to navigate the critical code segments by looking for string references inside binary files. for instance, messages that are displayed to the user (error messages) can be made a significant impact on the user by attacking. Therefore, string encryption can be used to hide strings in the executable file. For instance, Caesor cipher algorithm[1] that can be used to perform string literal obfuscation as a basic obfuscation.

Obfuscation Techniques

3. Control Flow Obfuscation

It makes decompiled code look like more mixed logic which is very difficult for hackers to understand. in other words, Control flow obfuscation synthesizes conditional, branching and iterative construction that produce valid executable. These techniques may be applied for the runtime performance of a method

4. Instruction Pattern Transformation

Instruction patterns can be used to convert common instructions created by the compiler to others, less obvious constructs. These are sophisticated legal machine language instructions that may not map cleanly to high-level languages such as C# or Java.

5. Dummy Code Insertion

Inserting code segments into the executable that do not affect the logic of the main program. But it is getting harder to break by decompiling or reverse-engineering the code and difficult to analyze.

Obfuscation Techniques

6. Unused Code and Metadata Removal

Removing debug information including logs, non-essential metadata and used code segments from the applications are made smaller and reduce the information which is exposed to attackers. These approaches may affect the improvement of performance.

7. Binary Linking and Merging

In this technique that combines multiple input executables and libraries into one or more output binaries. Linking can be used to make the application smaller. it will help to simplify deployment scenarios and it may reduce information for hackers.

8. Opaque Predicate Insertion

This method is used to obfuscate by adding conditional branches that always evaluate to the known result that cannot be determined through the static analysis. This is the way of introducing potentially incorrect code that will never actually be executed but is confusing to attackers trying to understand the decompiled output.

Obfuscation Techniques

9. Anti-Tamper

An obfuscator can inject application self-protection into our code to verify our application has not been tampered with in any way. If tampering is detected, it can shut down the application, limit the functionality, invoke random crashes (to disguise the reason for the crash), or perform any other custom action. It might also send a message to a service to provide details about the tampering detected.

10. Anti-Debug

When a hacker is trying to pirate or counterfeit your app, steal your data, or alter the behavior of a critical piece of infrastructure software they will almost certainly begin with reverse engineering and stepping through your application with a debugger. An obfuscator can layer in application self-protection by injecting code to detect if your production application is executing within a debugger. If a debugger is used, it can corrupt sensitive data (protecting it from theft), invoke random crashes, or perform any other custom action. It might also send a message to a service to provide a warning signal.

Pros and Cons of Obfuscation

Security (Pros)

Maintainability (Cons)

Optimized Code (Pros)

Bugs (Cons)

Track Illegal Copies (Pros)

Obfuscation tools

There are a few tools related to Android Studio such as ProGuard and DexGuard. ProGuard is a free tool that is included in Android Studio, DexGuard which is a commercial version of ProGuard. It is available from https://www.guardsquare.com/en. When the ProGuard uses, it has been renamed variables, but we can still see the code structure. But DexGuard doesn't just rename variables, it performs much stronger control and preventative obfuscations.

.NET developers can use ArmDot commercial version. ArmDot uses several methods to obfuscate: obfuscate names, control flow obfuscation, and virtualization. Virtualization is a method that converts original code to instructions for some unique virtual machine, that is executed by the virtual machine, thus original code can't be restored or modified. some of the obfuscation tools as follows.

1. .NET: Dotfuscator, ILProtector, ArmDot
2. JavaScript: Javascript Obfuscator, Jscrambler
3. Android: ProGuard, DexGuard

MCQ

11. _____ is the illicit transmission of data from inside an organization or personal system to an external location or recipient.
    a) Database hacking
    b) Data leakage
    c) Data cracking
    d) Data revealing

2. Data leakage threats do not usually occur from which of the following?
    a) Web and email
    b) Mobile data storage
    c) USB drives and laptops
    d) Television

3. Data leakage is popularly known as _____
    a) data theft
    b) data crack
    c) low and slow data theft
    d) slow data theft

4. There are _____ major types of data leakage.
    a) 2
    b) 3
    c) 4
    d) 5

REFERENCES

- https://levelup.gitconnected.com/android-obfuscation-e608f79f0d09