ZIMPERIUM®

10 formas de blindar y proteger las aplicaciones

La protección interna de la aplicación modifica la misma para hacerla más resistente a la ingeniería inversa, manipulación y control.

A continuación se encuentran nuestras 10 técnicas más recomendadas, desde la ofuscación más simple hasta la dotación a su aplicación de detección y respuesta a ataques de forma autónoma.

1 Modificar los nombres

Modifique los nombres de las variables y métodos reconocibles por cadenas de caracteres sin sentido alguno, para que resulten más confusas para un pirata informático. Existen varias herramientas de ofuscación gratuitas que permiten renombrar las clases, campos y métodos.

2 Insertar código ficticio

Incluya código adicional, no funcional, en la aplicación, para dificultar la ingeniería inversa sobre el mismo. Muchos de los ofuscadores gratuitos introducen adicionalmente código ficticio.

3 Eliminar el código y los metadatos en desuso

Elimine el código sin uso, la información de depuración y cualquier metadato que no sea imprescindible de las aplicaciones para reducir la información al alcance de un posible atacante.

4 Ofuscar las llamadas de Objective-C

Las llamadas a mensajes en Objective-C se realizan en tiempo de ejecución, lo que implica que se almacenan dentro del código en un formato plano que permite su manipulación. Proteja el código de Objective-C mediante la ofuscación de las llamadas a mensajes en texto plano para que su lectura y modificación no resulten sencillas.

5 Utilizar empaquetado binario

Empaquete su código para protegerlo del análisis estático. Los empaquetadores cifran y comprimen el código, añadiendo un "stub" que permite desempaquetarlo en tiempo de ejecución. Esto dificulta la ingeniería inversa para los piratas informáticos, ya que no podrán ejecutar el código mediante un desensamblador o decompilador.

6 Protegerse contra los depuradores

Los piratas informáticos hacen uso de depuradores de código para entender cómo funciona una aplicación y realizar ingeniería inversa del código.

Para evitar una depuración de forma sencilla, introduzca llamadas a una API para consultar información acerca del proceso y del sistema, y comprobar la presencia de un depurador. Para una mayor protección del depurador, utilice alguna herramienta que detecte los puntos de interrupción introducidos por el depurador y ejecute de forma automática las acciones de protección.

7 Diversifique su software

Cree diversas instancias de software, funcionalmente idénticas, pero en las que el código sea excepcionalmente diferente en forma y estructura. Esto obliga a los piratas informáticos a tener que descifrar cada copia de la aplicación por separado, en lugar de utilizar un único ataque para todas las instancias de la aplicación.

8 Ofuscar el flujo de control

Modifique la estructura básica de las llamadas a las subrutinas para que el código resulte indescifrable. Por ejemplo, las funciones en línea, sustituyen las llamadas a subrutinas por saltos calculados y simplifican el flujo de control, convirtiendo las estructuras condicionales en forma de árbol en sentencias "switch" planas

9 Proteger contra la manipulación

Implemente medidas de protección en la aplicación que prevengan los intentos de modificación y secuestro del código de la aplicación: introduzca sumas de comprobación superpuestas para comprobar¬ la integridad del código, añada la detección de "jailbreak" en iOS y de "rooting" en Android, utilice la comprobación cruzada de bibliotecas compartidas, la verificación de llamadas a funciones y otras medidas de protección contra la manipulación.

10 Haga que su aplicación se autodefienda

Al identificar un intento de manipulación, su aplicación debería generar la correspondiente respuesta a modo de protección. Si es posible, incluya acciones automáticas de protección en tiempo real, en lugar de generar alertas a reparar de forma manual. Entre las acciones defensivas más comunes se encuentran el bloqueo del acceso a la cuenta, la detención de la ejecución de comandos, la eliminación de datos sensibles y el cierre total de la aplicación. Para evitar futuros intentos de ataque, corrompa algunos elementos de la aplicación para que un pirata informático crea haber tenido éxito, pero en realidad, tenga únicamente un acceso reducido.

Zimperium ayuda a las organizaciones a desarrollar aplicaciones móviles seguras y acordes a la normativa. Es la única solución que combina la protección integral dentro de la aplicación con una visibilidad de las amenazas centralizada. Haga clic aquí para obtener más información.

ZIMPERIUM®

4055 Valley View Dallas, TX 75244
844.601.6760
info@zimperium.com