INTRODUCTION INTO REVERSE ENGINEERING
&
 SECURITY

Cyril Cermak


09:18
Taycan
Details
75 %
286 km
Recommendations
Porsche Newsroom
News from the world of Porsche
Vehicle
Map
Discover
Account

MOTIVATION 💪

EXERCISES

- OBJC RUNTIME MANIPULATION, SWIZZLING, FULL JB BYPASS
- SWIFT RUNTIME MANIPULATION, PARTIAL JB BYPASS
- EXTRACT IN MEMORY SECRETS
- FACE ID BYPASS
- CRYPTO ALGORITHMS EXTRACTION
- KEYCHAIN DUMP
- SSL PINNING FULL BYPASS

DEMO TIME

QUICK RECAP-OBJC JAILBREAK

- BINARY DUMP
- HOOKING INTO RUNTIME - ASLR
- RETURNING FROM THREAD
- SWIZZLING OBJC FUNCTION
- FULL JAILBREAK BYPASS

QUICK RECAP - SWIFT JAILBREAK

- FINDING THE LIBRARY CALL
- HOOKING INTO RUNTIME - ASLR
- MODIFYING REGISTERS
- FISHHOOK - RE-BINDING SYMBOLS
- PARTIAL SWIFT’S JAILBREAK BYPASS
- FULL SOLUTIONS - BINARY PATCHING

QUICK RECAP - FACE ID BYPASS

- INJECTING OBJECTION INTO RUNTIME - SWIZZLING
- FULL BYPASS OF FACE ID
- EXPOSURE OF DATA PROTECTED BY FACE ID
- EXPOSURE OF IN-MEMORY SECRETS

QUICK RECAP - CRYPTO BYPASS

- FACE ID BYPASS - NOT POSSIBLE
- MONITORING OF CRYPTO OPERATIONS
- RE CRYPTO ALGORITHM
- USING THE ALGORITHM FOR OUR OWN OPERATIONS

QUICK RECAP - KEYCHAIN DUMP

- OBJECTION KEYCHAIN DUMP
- FACE ID NOT BYPASSABLE

QUICK RECAP - SSLPINNING

- SSL PINNING IMPLEMENTED WITH TRUSTKIT
- DYLD INJECTION
- FULL BYPASS WITH SSLKILLSWITCH

KEY TAKEAWAYS

- CLIENT-SIDE IS NOT SAFE
- ALWAYS TEST AND QUESTION YOUR APP'S SECURITY
- ENCRYPT SENSITIVE DATA, IT'S WORTH IT, 100%
- OBFUSCATE SECRETS, ALWAYS, NO EXCEPTIONS
- NO MATTER WHAT PREVENTIONS YOU IMPLEMENT, THEY WILL BYPASS IT
- DON'T BLINDLY IMPORT LIBRARIES

KEY TAKEAWAYS

- CLIENT-SIDE IS NOT SAFE
- ALWAYS TEST AND QUESTION YOUR APP'S SECURITY
- ENCRYPT SENSITIVE DATA, IT'S WORTH IT, 100%
- OBFUSCATE SECRETS, ALWAYS, NO EXCEPTIONS
- NO MATTER WHAT PREVENTIONS YOU IMPLEMENT, THEY WILL BYPASS IT
- DON'T BLINDLY IMPORT LIBRARIES

THANK YOU!

LINKED IN

MY WORKS

📱 ACHIEVEME

⛓️ EOSMATE / 💻 EOSMATE.IO

💻 APPSTOREREVIEWS.NET

📖 MODULAR ARCHITECTURE ON IOS

👨‍💻 RE TALKS/WORKSHOPS