Improving Security in Jailbroken iOS Devices

Rohan Patel | rp4437@rit.edu
Department of Computer Science, Rochester Institute Of technology, Rochester, NY.
Advisor : Dr. Rajendra k Raj

MOTIVATION
• Increasing popularity of the jailbreaking devices. ~25-30 million jailbroken devices.
• Reverse engineering is easy on JB devices due to removal of OS restrictions imposed by Apple, hence making them a soft target for attackers.
• Lack of awareness in developer community leads to insecure app development. Hackers or criminals have numerous tools, reverse engineering methods available to attack the apps that developers are not aware of.

OBJECTIVE
• Inspect and exploit vulnerabilities (insecure data storage, lack of binary protections) in real-world applications using various penetration testing tools and learn to avoid them.
• Propose secure coding guidelines for developers to help them develop secure applications and avoid common security pitfalls.
• Develop a demo app that detects jailbroken device.

IMPLEMENTATION
• Runtime manipulation of the app using penetration testing tools Cycrupt, Hopper & Clutch.

Objective-C Runtime Manipulation: Runtime oriented language makes implementation decisions at runtime instead of compile & link time.
• Method Swizzling: Method swizzling is the process of changing the implementation of an existing selector. It’s a technique made possible by the fact that method invocations in Objective-C can be changed at runtime.

RESULTS

Cycrupt: A tool running on Javascript interpreter allows to write programs in Javascript & Objective-C. It is capable of hook into running process and allows modification of runtime behavior of application. ex: var a = [[NSString alloc]initWithString:@"12"];

Steps For Reverse Engineering An App :
1) Decrypt apps using command line tool Clutch.
2) Analyze code of decrypted app using Hopper.
3) Runtime manipulation, code injection using Cycrupt.

Jailbreak Detection Application: Finds installed Cydia app, runs sandbox integrity testing.

CONCLUSION & FUTURE WORK
• With plethora of tools available for attackers and developers are mostly unaware of any of these tools, reverse engineering mechanisms; companies shall invest equally in security not just UI/UX.
• Future scope of this project involves investigation of applications of various domains on larger scale (ex: target apps from various domains like banking, social networking, gaming) with latest jailbreak of iOS.

REFERENCES

ACKNOWLEDGEMENT
• Special thanks to Dr. Leon Reznik for feedback on project work.
• Parth Patel for providing his device for testing.