iOS Security Research

Răzvan Deaconescu, Mihai Chiroiu, Costin Carabaș

https://github.com/malus-security/

iOS Security Challenges

closed source

multiple ACL-centric mechanisms: entitlements, file permissions, custom/hardcoded, sandboxing

areas of interest: sandboxing, jailbreaking, jekyll apps, IPC

XiOS

dynamic protection against jekyll apps

binary analysis/rewriting

based on previous work (PiOS, PSiOS)

ACS CCS 2015

Sandblaster

first complete reversing of iOS sandbox profiles

public/open-source

works for iOS 11 included

tech report on arXiv

Sandscout

automated flaw detection in iOS Sandbox profile

soon to be open-source

5 CVEs reported to Apple

ACM CCS 2016

iOracle

automated jailbreak helper + filesystem analysis

soon to be open-source

issues reported to Apple

AsiaCCS 2018

Sigil

iOS IPC automated analysis framework

focus on XPC + ACLs

analysis on latest iOS version; may not require jailbreak

under work, to be published at venue and open sourced

Team

Will Enck, NCSU

Luke Deshotels, NCSU

Răzvan Deaconescu, UPB

Mihai Chiroiu, UPB

Costin Carabaș, UPB

Ahmad Reza-Sadeghi, TUD

iOS Security Research

Sandblaster

Sandscout

iOracle

Sigil

iExtractor