

1200 - Jailbreaking Apple Watch

Thursday at 12:00 in 101 Track 2

45 minutes | Demo

Max Bazaliy*Security Researcher, Lookout*

On April 24, 2015, Apple launched themselves into the wearables category with the introduction of Apple Watch. This June, at Apple's Worldwide Developer Conference, Apple announced that their watch is not only the #1 selling smartwatch worldwide by far, but also announced the introduction of new capabilities that will come with the release of watchOS 4. Like other devices, Apple Watch contains highly sensitive user data such as email and text messages, contacts, GPS and more, and like other devices and operating systems, has become a target for malicious activity.

This talk will provide an overview of Apple Watch and watchOS security mechanisms including codesign enforcement, sandboxing, memory protections and more. We will cover vulnerabilities and exploitation details and dive into the techniques used in creating an Apple Watch jailbreak. This will ultimately lead to a demonstration and explanation of jailbreaking an Apple Watch, showcasing how it can access important user data and applications.

Max Bazaliy

Max is a Security Researcher at Lookout with more than ten years of experience in areas as reverse engineering, software security, vulnerability research and advanced exploitation. Currently focusing on iOS exploitation, reverse engineering advanced mobile malware and hardware attacks. Max was a lead security researcher at Pegasus iOS malware investigation.

In the past few years, Max was a speaker on various security conferences, including BlackHat, CCC, DEF CON , Ruxcon, RSA and BSides.

Max holds a Masters degree in Computer Science and currently is PhD student at the National Technical University of Ukraine "Kyiv Polytechnic Institute" where he's working on dissertation in code obfuscation and privacy area.

@mbazaliy

[#defcon25/by_track/101-Track2/Thursday](#)

[#defcon25/By_Day/_thursday](#)