iOS DEVICE AND APP TRUST EVALUATION CONT

Lecture 18a

COMPSCI 702

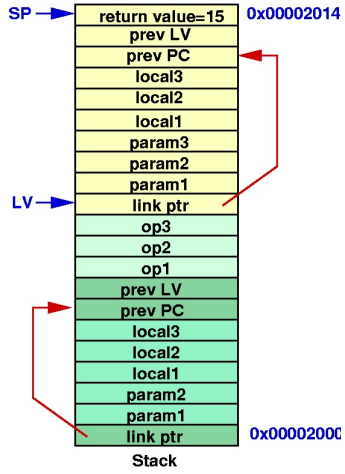
Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

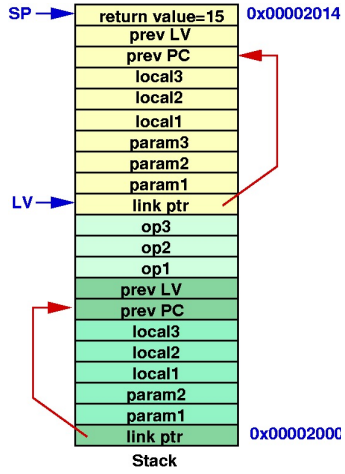
April 22, 2021

REGULAR DEP



- Protection against buffer overflow attacks
  - Only non-writable pages can be run
  - Stack is obviously writable
  - Data is also writable
  - So, exploits have to use Return Oriented Programming (ROP)

ROP



- Can execute only non-writable pages
  - Marked executable
- So attacks have to call existing code
  - Find chunks of code (gadgets) ending with ret instructions
  - Fill stack with addresses to return to
- Much more difficult than simple code injection

MACF

- The Mandatory Access Control Framework (MACF)
  - Originally from FreeBSD
  - Security labels can be tagged to system objects

SIDELOADING IN iOS

- Developers can release open-source apps outside of the App Store
- Interested users can use the open-source app
  - Open the app code in Xcode
  - Compile and run it on their own devices
  - This way, it is possible to completely bypass the App Store
- Somewhat similar to Android
  - Sideloading apps from unknown sources
  - A bit more complex because sideloading requires a physical connection and a Mac running Xcode
- Actually, its main purpose is for developers to test their own software on real hardware

SUMMARY

- Apps are signed by Apple
  - To a great extent, this limits malware
  - Stops apps being modified by exploits
- All executable pages are signed
  - CSE is much stricter than normal DEP
  - Any changes cause the app to be killed
  - The only exception is the JavaScript JIT in Mobile Safari

RESOURCES

- **iOS Hacker's Handbook**
  Charlie Miller, Dionysus Blazarkis, Dino Dai Zovi, Stefan Esser,Vincenzo Iozzo, Ralf-Philipp Weinmann
  John Wiley & Sons, Inc., 2012

- **Maintaining Your Signing Identities and Certificates**
  https://developer.apple.com/library/mac/documentation/IDEs/Conceptual/AppDistributionGuide/MaintainingCertificates/MaintainingCertificates.html

ACKNOWLEDGEMENT

- Some of the slides are based on the presentation shared by Robert Sheehan, thanks to him!

Questions?

Thanks for your attention!