I/UCRC: CARFS
Center for Advanced Research in Forensic Science

Hardware-Based Exploitation and Forensics Evaluation of iOS Devices

PI: Dr. Todd McDonald

Computer Science/SoC

UNIVERSITY OF SOUTH ALABAMA

DFII: Digital Forensics Information Intelligence

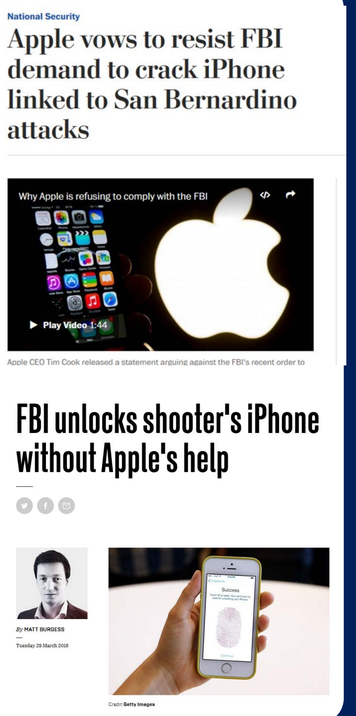
RELEVANCE / OBJECTIVES

Relevance

- iOS (iPhone Operating System) devices provide best privacy preserving features
- iOS devices used for nefarious purposes create problems for forensic analysis
- Unlock scenarios are of particular relevance for incident response in industry and government sectors

Objectives

- Develop library of exploitation techniques
- Demonstrate breadboard functionality
  - Data collection of iOS electromagnetic signals
  - Control of iOS functions using specific



APPROACH / TECHNIQUES

- Purchase iPhone devices
- Experimentally demonstrate known vulnerabilities and techniques for unlock
- Set up breadboard environment
- Understand and demonstrate control and manipulation of devices using standard known techniques
- Explore effects of low-cost electromagnetic manipulation and power glitching
- Catalogue and demonstrate unlock capabilities for known iOS versions and device families

Written instructions:

1. Reboot your iPhone ready to set it up as a new device.
2. Start the setup process and select your country and language
3. On the "Choose a Wi-Fi Network" screen press the "i" next to Wi-Fi symbol for the Wi-Fi network you want to connect to.
4. Scroll down to where it says "DNS" and type in one of the following
   - USA/North America: 104.154.51.7
   - Europe: 104.155.28.90
   - Asia: 104.155.220.58
   - In rest of the world: 78.109.17.60

MILESTONES / DELIVERABLES

Deliverables

- Report of exploitation techniques for iOS based on version families
- Demonstration framework for breadboard iPhone setup
- Data results for initial studies using low-cost EM-based probing of an iPhone device

Milestones

- 4 m: Research / acquire tools and techniques for iOS exploitation based on version families
- 8 m: Setup breadboard functionality for EM analysis and input control of iPhone
- 12 m: Gather relative data and build expertise for hardware-based exploit demonstration on iOS devices relative to unlock scenarios

INDUSTRY BENEFITS

Economics

- Considerable market in law enforcement, government, and industry to assist forensic examiners faced with locked iOS devices.
- Identifying, categorizing, and realizing a demonstration framework for techniques that provide solutions for this unique iOS problem would provide great opportunity in these sectors.

Potential Member Benefits

- Provide a list of potential iPhone vulnerabilities by iOS version family to IAB members
- Provide prototype demonstration capability for forensic data recovery from locked iPhone devices