Student's name: Matheus Henrique Schaly

Professor's name: Carlisle Adams

Course: CSI 4139 Design of Secure Computer Systems

Due: 22th November, 2019

Assignment #2

First Part

Attack 1: A long-term device tracking attach which works in spite of MAC randomization and may reveal personal information such as the name of the device owner.

Implication 1: Sensitive information can be captured by attackers and used for malicious activities. Sensitive information includes 1) Name; 2) MAC address and AP (access point) that the device is connected to; 3) Device class; 4) OS version.

Mitigation 1:

1. Short-term solution: Disable AirDrop feature completely.
2. Mitigation 1: Hide real MAC address when not connected to an AP. That is, hide your real MAC address if you are not connected to a device that allows wireless devices to connect to the network.
3. Mitigation 2: Randomize hostname for AWDL (Apple Wireless Direct Link). As apple devices transmit their hostname in AWDL, if you a random hostname, the attacker would gather less information about you.

Attack 2: A DoS (Denial of Service) attack aiming at the election mechanism of AWDL (Apple Wireless Direct Link) to deliberately desynchronize the targets' channel sequences effectively preventing communication.

Implication 2: Significantly degrades communication between the targets by dropping communication packets.

Mitigation 2: Don’t accept unicast frames. By doing so, instead of addressing only a target, you would be addressing various different targets at once.

Attack 3: A MitM (man-in-the-middle) attack which intercepts and modifies files transmitted via AirDrop, effectively allowing for planting malicious files.

Implication 3: Allows the modification of files and insertion of malicious files.

Mitigation 3:

1. Provide stronger visual cues for authenticated receivers, as in HTTPS-protected websites that are augmented with a green (lock) symbol.
2. Regarding the process of receiving files: reset *everyone* to *contacts only* after a timeout. Or, if you are the user, avoid using the *everyone* option.
3. Introduce secure AirDrop mode for non-contacts. That is, simply put, deleting cookies after a transfer.

Attack 4: Two DoS attack on Apple’s AWDL implementations in the Wi-Fi driver. The attacks allow crashing Apple devices in proximity by injecting specially crafted frames. The attacks can be targeted to a single victim or affect all neighboring devices at the same time.

Implication 4: Disabling communication between among many different targets in a specific area around the attack.

Mitigation 4: Again, avoid accepting unicast frames.

Second Part

Vulnerabilities:

- **Protocol vulnerabilities:**
    1. AWDL has sensitive fields in the AFs (action frames) which devices broadcast *in the clear* multiple times per second when AWDL interface is active.
    2. AWDL *does not employ any security mechanisms*. Instead, Apple decided to leave security mechanisms to the upper layers. Thus, while end-to-end confidentiality and integrity can be achieved using a secure transport protocol as TLS, AWDL frame are vulnerable to forgery which render any upper layer using AWDL susceptible to attacks on availability.
    3. AirDrop service allows iOS and macOS devices to *exchange files directly via AWDL*. AirDrop has poor UI design choices that enables attackers to masquerade as a valid receiver.
- **Bug vulnerability:**
    1. DoS: *Kernel panic and system crash*. These flaws can be exploited by sending corrupt AFs. In particular; they can trigger kernel panics by setting invalid values in the synconization parameters (affecting macOS 10.12) and the channel sequence (affecting macOS 10.14, iOS 12, watchOS 12, and tvOS 5), respectively.
    2. Outlook: *Remove Code Execution*. While not critical by themselves, the mere existence of these vulnerabilities creates a new class of threats to Wi-Fi devices as an attacker can exploit them without any authentication towards the target, i.e., they do not have to be on the same network.

Third Part

Responsible disclosure:

- **Why is it important:** This paper identified, among other things, vulnerabilities and bugs regarding the AWDL protocol. Without a responsible disclosure, the authors would not have given enough time for Apple to act on those problems. Therefore, attackers would be able to have access to this paper, learn from it, and exploit the vulnerabilities before they have been fixed. Consequently, the responsible disclosure helped Apple to address the problems before they were made public.
- **How does it typically works:** The authors share their finding with the company. Furthermore, the authors may help the company to address the problems found. Nonetheless, the authors can still publish their work.
- **Have the authors done it correctly?** Yes, the authors shared their findings in December, 2018. As their paper was published in August, 2019, they have probably submitted their paper within a few months after sharing their findings. Moreover, they have reported the two implementation vulnerabilities on August 2018. Therefore, Apple had enough time to fix what they wanted to fix, and that didn't cause any problems with the authors' paper, that is, they still could publish their work.

Reference

M. Stute, *et al.*, A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link, *Proceedings of the 28th Usenix Security Symposium*, Santa Clara, CA, USA, August 14-16, 2019, pp. 37 – 54 (available at https://www.usenix.org/system/files/sec19-stute.pdf)