Design of Secure Systems
CSI4139

University of Ottawa
Fall 2019

Assignment #2
Brennan McDonald - 8195614
Nov. 22

Overview

the paper *"A Billion Open Interfaces for Eve and Mallory"* highlights vulnerabilities with the Apple Wireless Direct Link and the AirDrop (AWDL) Protocol. Due to the fact that these vulnerabilities effect the protocol itself, it leaves a large percent of Apple products open to potential attacks such as iPhones, MacBooks, and Apple TVs. These vulnerabilities range from low severity with sensitive information and user tracking, to higher severity attacks such as Man in the Middle attacks with malware injection.

A denial of service or DoS attack is any attack that prevents a person from being able to do what they want to do. This could mean attack a website so that it does not load, or preventing a person from a phone from being able to use specific functions on that phone. The attack that is proposed in this paper is a DoS attack that takes two phones and prevents them from talking with each other by telling them to talk and listen at the wrong time.

A man in the middle attack or MiTM is an attack that allows an attacker to listen in between two other phones, computers, or devices and change the message that is being sent. This can be anything from changing a message to a virus or taking sensitive information such as credit card info or personal info from the message. In this paper, the authors have managed to place themselves between two iPhones and listen in to any photos that have been sent by the AirDrop service, this attack also alows the attacker to change the image to whatever they want.

The third attack mentioned in this paper is an attack that allows sensitive information about an Apple device to be stolen by an attacker. Due to the fact that iPhones share information about themselves with other devices around it, information like the iPhone version and user's name can be stolen. This allows an attacker to track an individual iPhone as it travels from location A to B. Possibly allowing an attacker to physically follow a specific device (and therefore user).

DoS via Desynchronization

The first attack mentioned in this paper is an attack that desynchronizes two AWDL devices by interrupting the communication between the two and sending incorrect offset parameters so the two devices can not relay information correctly. The first step in this is for the attacker to win the "AWDL election" which determines which phone will determine the communication parameters for the two devices. This is done by transmitting maximum values that are used in an equation to determine who will win the election.

The attacker sends individual unicast packets to each target, while ensuring that the two individual targets don't notice they are both being spoofed.This is done by unicasting to each device's unique address family. From here the attacker sends controlled offset parameters to each target to ensure they do not synchronize.

Mitigation

This paper proposes one solution to this DoS attack by discarding all unicast packets as there are not used in normal operation. While discarding unicast AFs does not prevent the attacker from winning elections, this makes it significantly more difficult.

AirDrop Man in the Middle

The paper puts forward an attack done on the AirDrop service enabling messages and files to be intercepted and modified by a malicious attacker.

This attack consists of three entities, the legitimate sender and receiver, and the attacker. The first and most important step in this attack is for the attacker to prevent legitimate receiver from appearing in the sender's UI. This is done by a targeted DoS attack to the sender. While this could be done via the Desynchronization attack, it's easier to use a TCP RST flood. A TCP RST flood is when the attacker send TCP packets with the RST flag set to 1 for every device that isn't itself, this will cause the sender to drop all connections that aren't with the attacker.

After the DoS attack has started, the attacker must authenticate to the receiver. If the receiver is in *everyone* mode, or will accept files from any person, this is trivial because we do not need to spoof a known contact. However, it the receiver is in *contact only* mode, this is a little more difficult as we much use the ongoing DoS attack to convince the receiver to switch to everyone mode. After we have authenticated to the receiver, we send a request using mDNS and wait until the sender sends their handshake request. We simply forward this on to the receiver and wait for their response. Proxying requests between the two, including sending the thumbnail of the legitimate file to the receiver. After the receiver has accepted, we can pick if we want to send the legitimate file or send a modified payload that contains malware.

Mitigation

This paper offers multiple ways to mitigate a potential MiTM attack on the AirDrop service. First they recommend a UI change to provide the user with a stronger indication that a receiver is unauthorized. This would prevent the victim from sending a file to an attacker who they believe is a legitimate user. Secondly they recommend resetting all users back to *contacts only* after a timeout. This would prevent the phones from staying in the dangerous *everyone* mode. Finally they suggest to add secure transmission airdrop for all non-contacts.

Sensitive Information Disclosure

By using device metedata, a device can be tracked and have sensitive information disclosed to attackers. When connecting to networks and broadcasting their status, iPhones randomize their mac address, while this is a good preventative measure to prevent tracking, it is not entirely effective. Data that is publicly disclosed such as an iPhone's hostname often contains the owner's first name in it. Phones also expose their real MAC address while trying to connect to WiFi access point, this can be used by an attacker to gain real information on the device. Protocol version and device class may also allow a user to be persistently tracked, being able to differ between protocol versions allows an attacker to gain insight into what iOS version a victim is running.

Mitigation

In order to mitigate these attacks, the paper recommends users disable AirDrop until Apple releases a fix that solves these vulnerabilities. The fixes that Apple could implement are to randomize and spoof hostnames so that a user's first name is not disclosed. In order to prevent attackers from discovering their real MAC address, phones should not broadcast their MAC address while not connected to an AP.

Responsible disclosure

According to Microsoft, responsible disclosure is "The issue is reported privately to the vendor and no one else until the vendor issues a patch." This definition is also supported by OWASP who uses it as a quote on their *Vulnerability Disclosure Cheat Sheet.* According to the paper, the researchers that put the report together notified Apple, allowed them to push fixes for the issues they were going to fix, and after waiting a year they published their work. I would state that this matches the industry definition of responsible disclosure in very sense.