Overview of the report

Types of attacks

DoS

- Impairing Communication with Desynchronization
    - To desynchronize two targets, the attacker needs to send incompatible synchronization parameters that will result in a controllable offset.
    - The attacker has to win the AWDL election by transmitting max values for the equation

      $$c_A > c_B \vee (c_A = c_B \wedge m_A > m_B)$$

    - The attacker then 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
        - Discard Unicast AFs
            - While discarding unicast AFs does not prevent the attacker from winning elections, this makes it significantly more difficult
- Planting Malware via AirDrop

MitM

- Planting Malware via AirDrop
    - 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.
    - This is done by the attacker sending a TCP with the RST flag set to 1 for every request 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
    - Update UI to give stronger queues to unauthenticated users
    - Reset *Everyone* back to *Contacts only* after a timeout.
    - Secure airdrop for non-contacts.
    -

Sensitive Information Disclosure

- Identifying Devices and Users via AWDL Protocol Fields
    - Despite MAC randomization users may be trackable
    - Hostname may contain names: “Janes iphone”
    - The Real mac address that the phone uses to connect to APs
    - *Device Class* may differ between devices, macOS, iOS, tvOS
    - Protocol version can be used to infer OS version.
        - AWDL 2.0 -> 10.12
        - AWDL 3.0 -> 10.13
    - Mitigations
        - Disable Airdrop
        - Hide Real MAC Address When Not Connected to an AP.
        - Randomize Hostname for AWDL.
        -
- User Tracking
    -