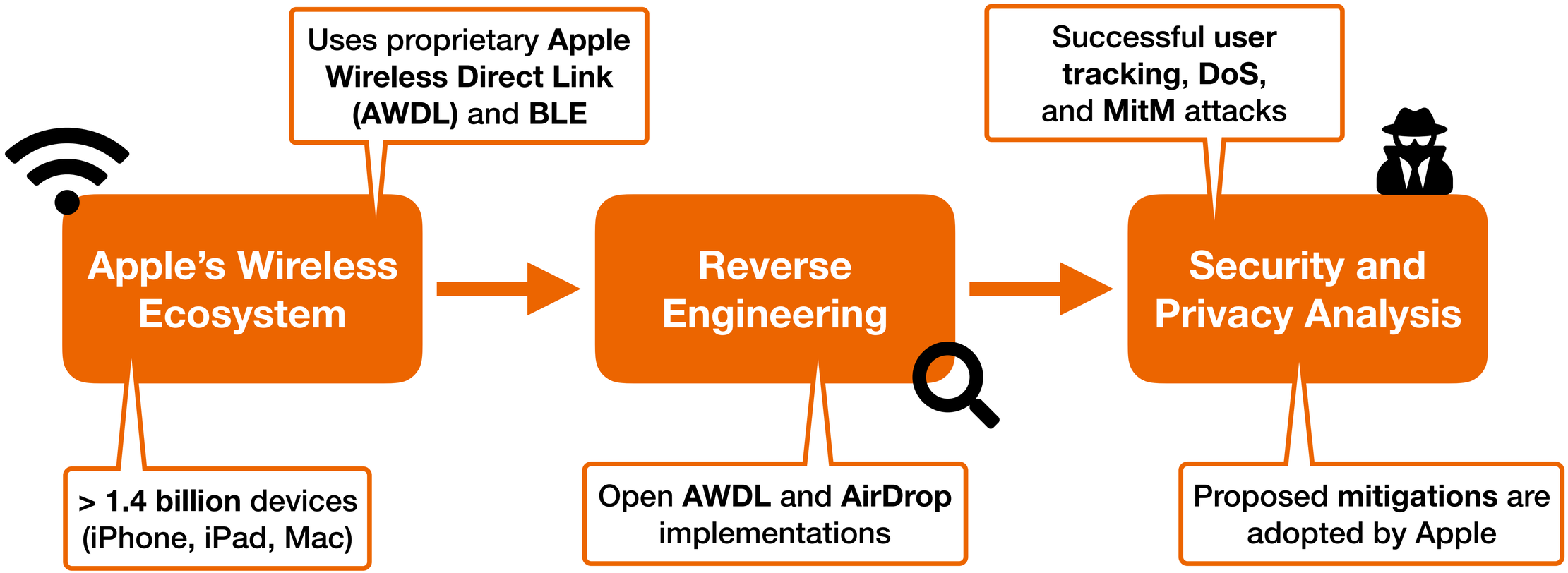
A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link

Milan Stute, Sashank Narain, Alex Mariotto, Alexander Heinrich,
David Kreitschmann, Guevara Noubir, and Matthias Hollick

TECHNISCHE UNIVERSITÄT DARMSTADT

SEEMOO SECURE MOBILE NETWORKING

Opening Up Apple's Wireless Ecosystem



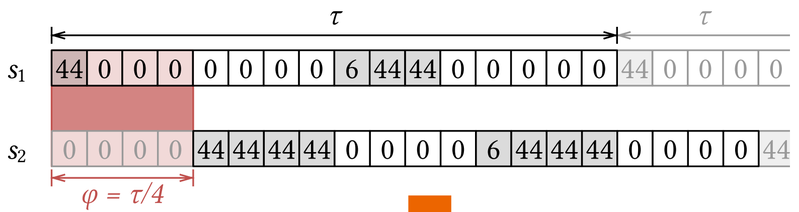
Vulnerabilities and Attacks

Remote activation
Brute force attack on
Bluetooth LE discovery
fixed in iOS 12.2

User Tracking
Revealing MAC address
and hostname
CVE-2019-8567
CVE-2019-8620

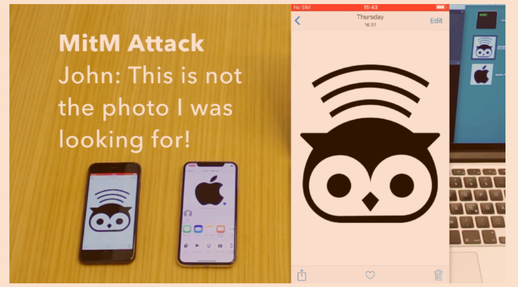
```
▼ Tag: Arpa
    Tag Number: Arpa (16)
    Tag Length: 16
    Flags: 0x03
  ▶ Arpa: Noahs-Iphone.local
```

Denial-of-Service
Breaking communication
via desynchronization
CVE-2019-8612



(Selective) Blackout
Crashing devices wirelessly
through corrupt frames
CVE-2018-4368

Man-in-the-Middle
Intercepting files
transmitted via AirDrop
fixed in iOS 13 beta

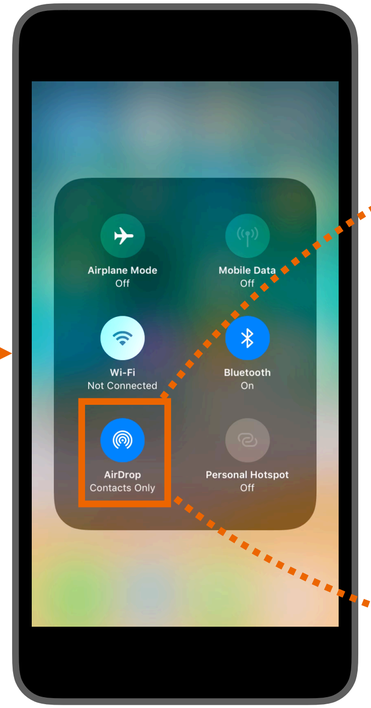



AirDrop

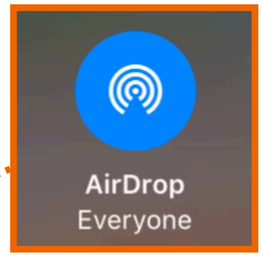
Discovery: Bluetooth

Jane

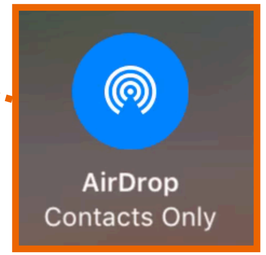
BLE advertisements including $H_{1..4}[0:1]$



John



turn on AWDL immediately



only if any $H_{1..4}[0:1]$ in address book

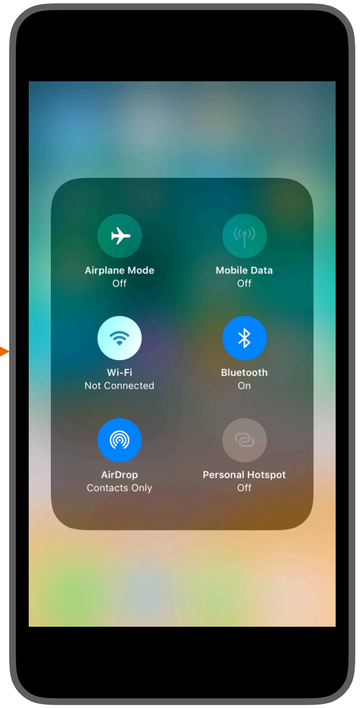
$H_1 = \text{SHA256}(...@\text{icloud.com})$ (your Apple ID)

H_n include associated phone numbers and other email addresses

Discovery: AWDL

Jane

Synchronize via
Apple Wireless Direct Link*
(provides Wi-Fi link layer)

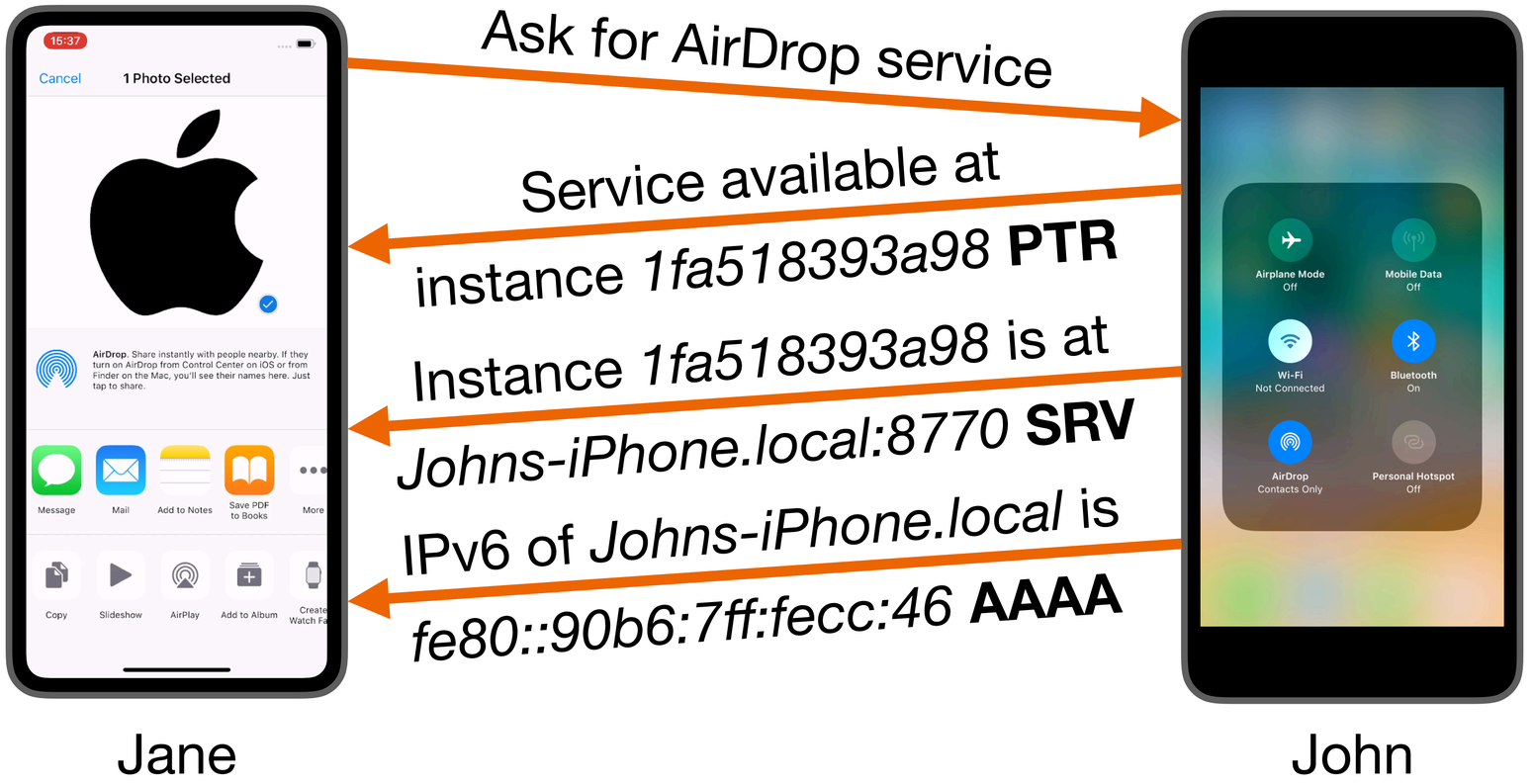


John

* Stute et al. *One Billion Apples' Secret Sauce: Recipe for the Apple Wireless Direct Link Ad hoc Protocol*. ACM MobiCom '18.


One Billion Apples' Secret Sauce: Recipe for the Apple Wireless Direct Link Ad hoc Protocol

Discovery: Bonjour



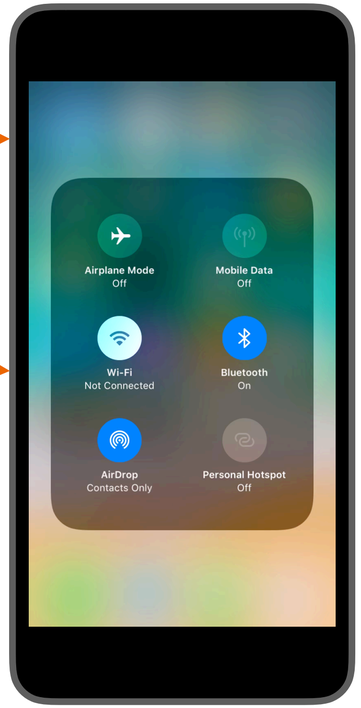
Authentication: HTTPS

Find out whether we are **mutual contacts**

Jane

TLS connection with client and server certificates*

HTTP POST **/Discover** with sender's record data**



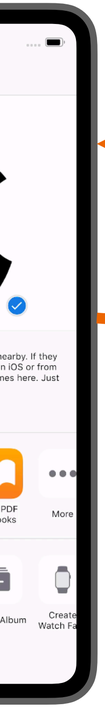
John

* Common name: com.apple.idms.appleid.prd.$UUID$

** $RD = UUID, H_1, \ldots, H_n$

$RD_\sigma = RD, \text{sign}(\sigma_{Apple}, RD)$

Authentication: HTTPS

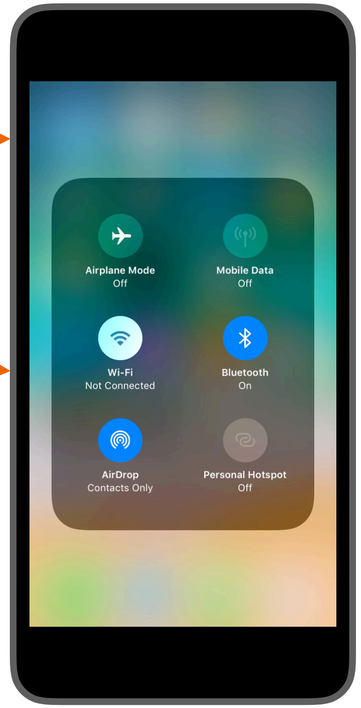


TLS connection with

client and server certificates*

HTTP POST **/Discover**

with sender's record data**



John

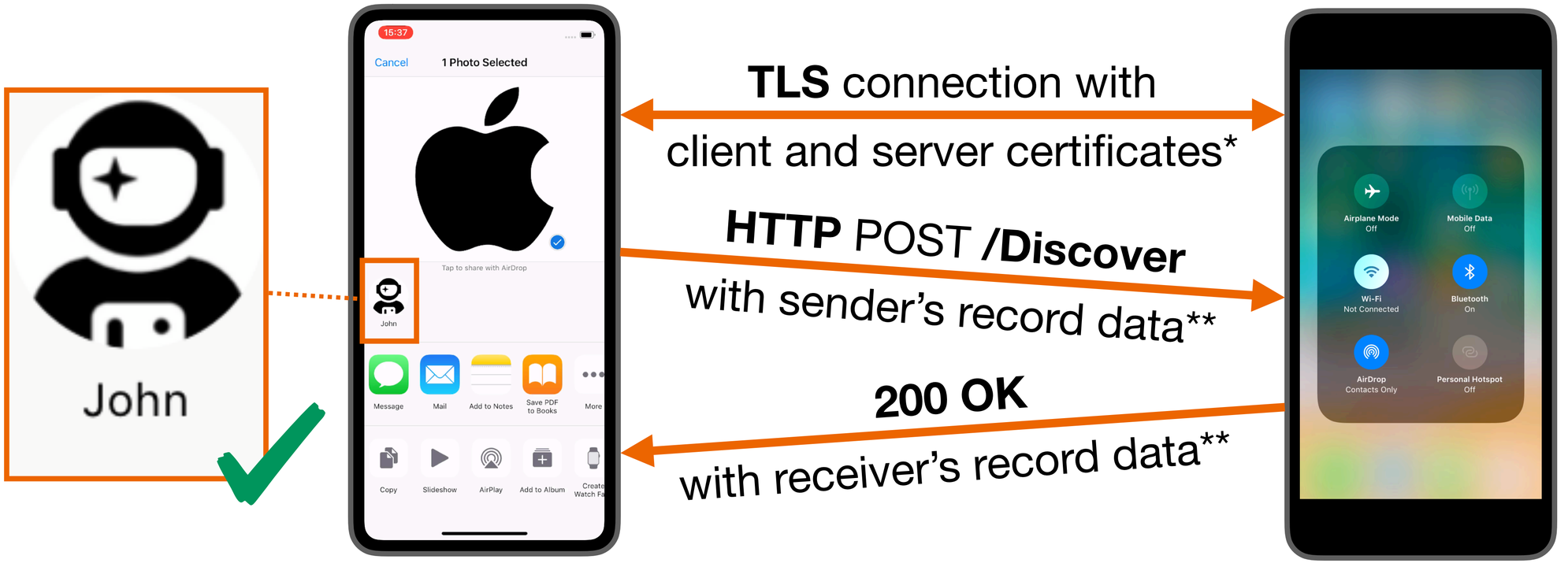
1. Verify signature of RD_σ
2. $UUID \in RD \leftrightarrow \sigma_{UUID}$
3. $\exists H_i \in RD : H_i \in$ address book

* Common name: com.apple.idms.appleid.prd.$UUID$

** $RD = UUID, H_1, \ldots, H_n$

$RD_\sigma = RD, \text{sign}(\sigma_{Apple}, RD)$

Authentication: HTTPS



TLS connection with client and server certificates*

HTTP POST **/Discover** with sender's record data**

200 OK with receiver's record data**

Jane

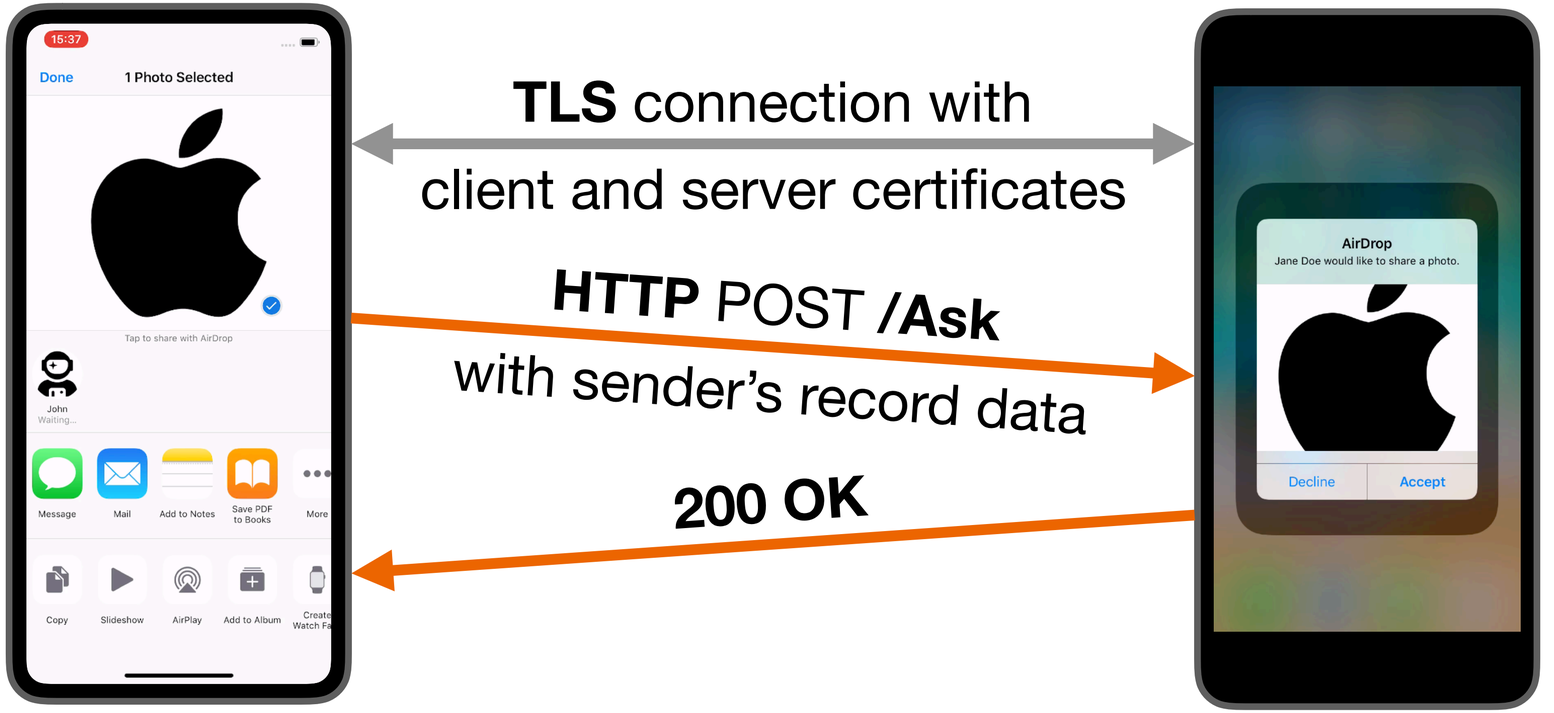
John

* Common name: com.apple.idms.appleid.prd.$UUID$

** $RD = UUID, H_1, \ldots, H_n$

$RD_\sigma = RD, \text{sign}(\sigma_{Apple}, RD)$

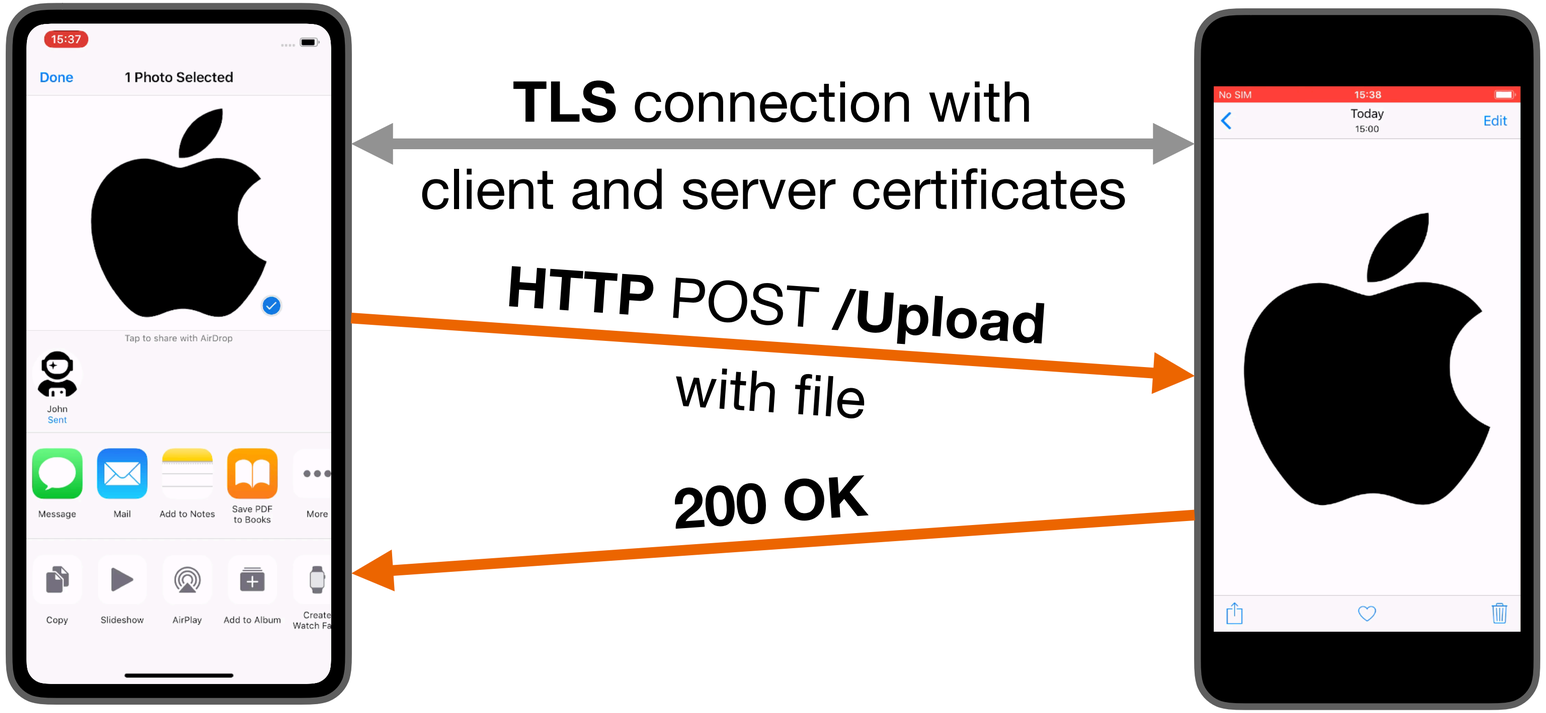
Data Transfer: HTTPS



User decides to **accept** or to **decline**

Data Transfer: HTTPS

Send the actual **file**



Jane

John

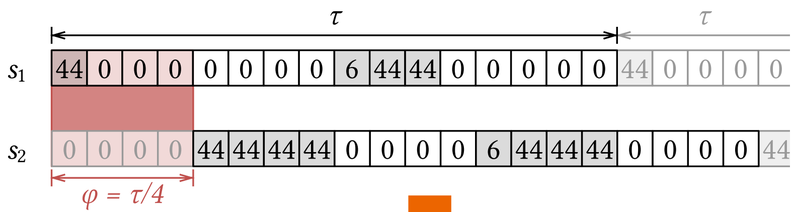
Vulnerabilities and Attacks

Remote activation
Brute force attack on
Bluetooth LE discovery
fixed in iOS 12.2

User Tracking
Revealing MAC address
and hostname
CVE-2019-8567
CVE-2019-8620

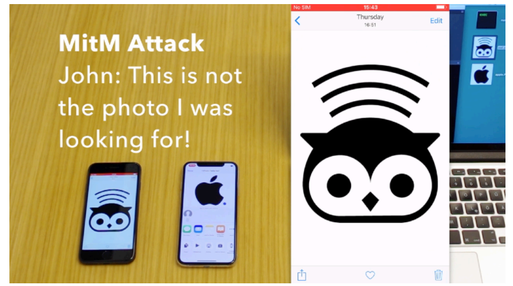
```
▼ Tag: Arpa
    Tag Number: Arpa (16)
    Tag Length: 16
    Flags: 0x03
  ▶ Arpa: Noahs-Iphone.local
```

Denial-of-Service
Breaking communication
via desynchronization
CVE-2019-8612



(Selective) Blackout
Crashing devices wirelessly
through corrupt frames
CVE-2018-4368

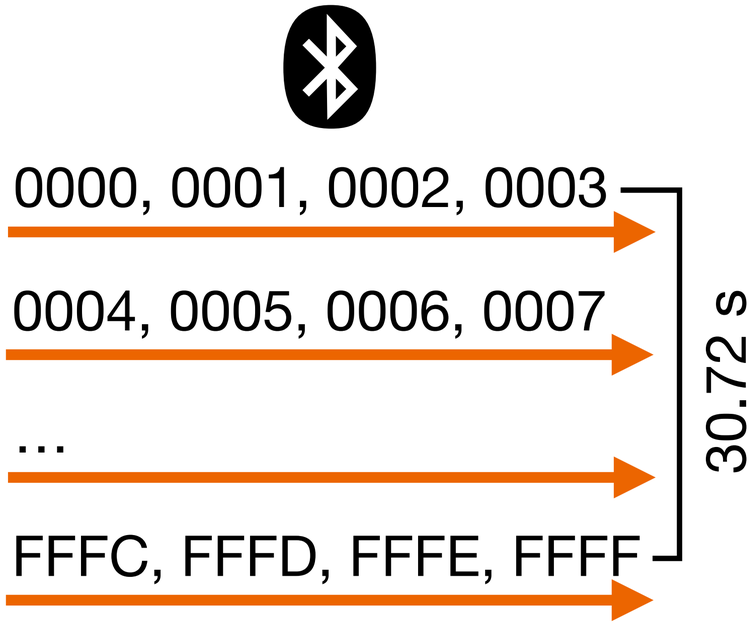
Man-in-the-Middle
Intercepting files
transmitted via AirDrop
fixed in iOS 13 beta



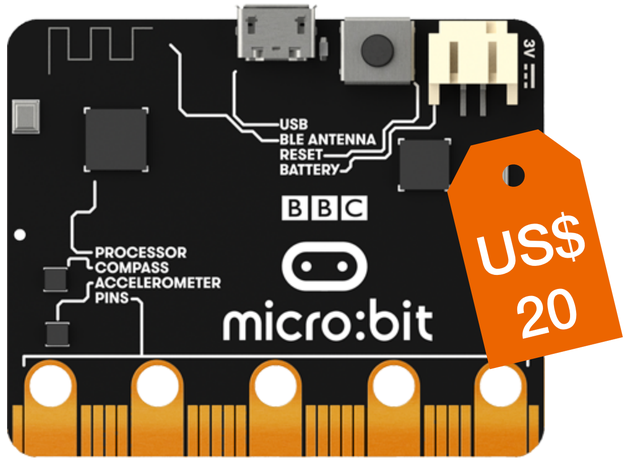
Tracking: Vulnerability Analysis

```
▼ Apple Wireless Direct Link action frame, Subtype: MIF
  ▶ Fixed parameters
  ▼ Tagged parameters (476 bytes)
    ▶ Tag: Synchronization Parameters
    ▶ Tag: Election Parameters
    ▶ Tag: Channel Sequence
    ▶ Tag: Election Parameters v2
    ▼ Tag: Data Path State
        Tag Number: Data Path State (12)
        Tag Length: 47
      ▶ Flags: 0x9f23, Infrastructure BSSID and Channel, Infrastructure Address
        Country Code: US
      ▶ Social Channel Map: 0x0007, Channel 6, Channel 44, Channel 149
        Infrastructure BSSID: ArubaAHe_[redacted] (70:3a:0e:[redacted])
        Infrastructure Channel: 104
        Infrastructure Address: [redacted]:00:a2:60 ([redacted]:00:a2:60)
    ▼ Tag: Arpa
        Tag Number: Arpa (16)
        Tag Length: 16
        Flags: 0x03
      ▶ Arpa: Noahs-Iphone.local
    ▶ Tag: Version
```

Tracking: Remote Activation



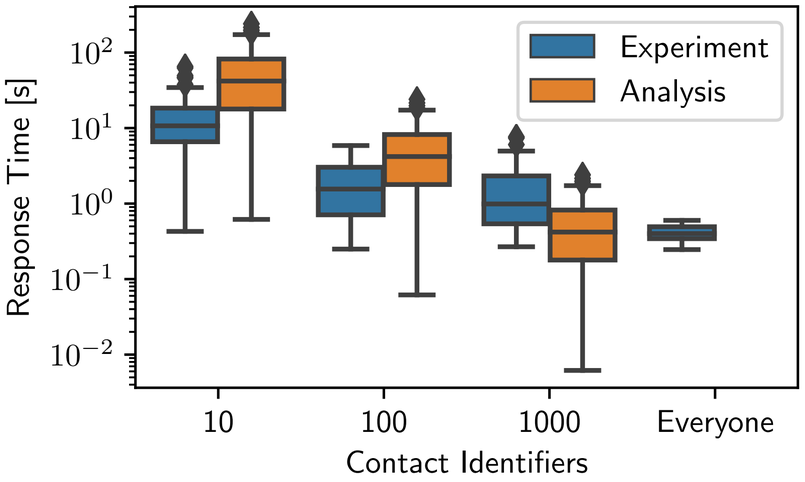
Brute Force Analysis



Source: microbit.org

Implementation

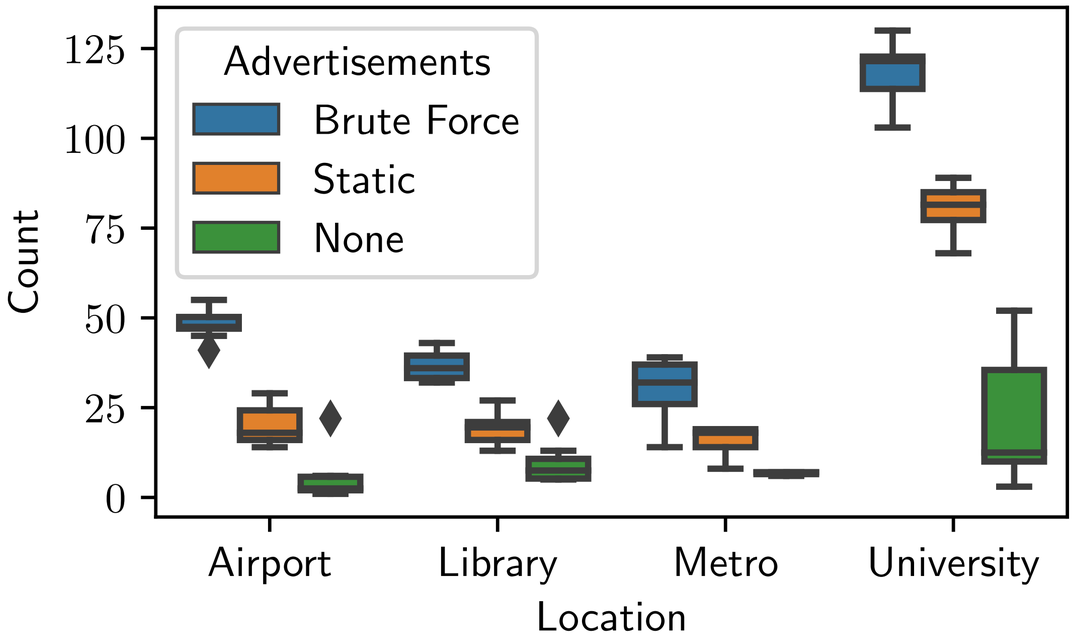
136 contacts on average



Experimental Evaluation

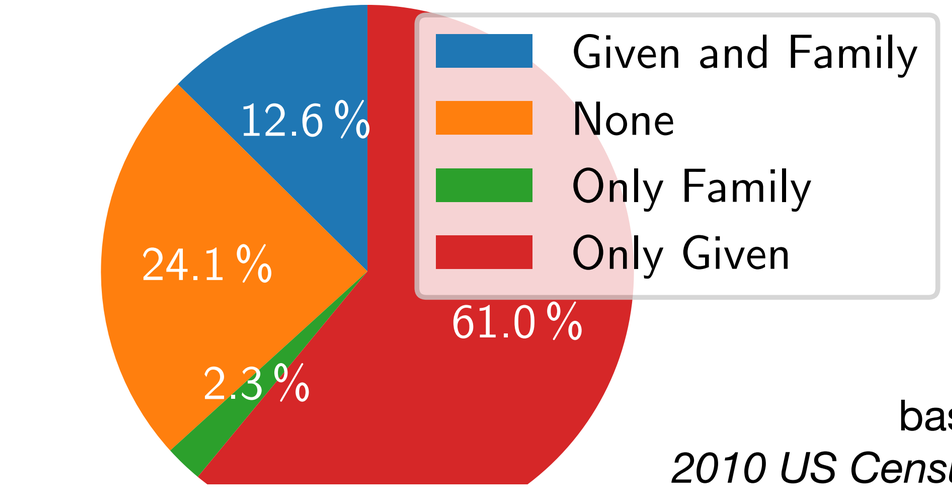
Tracking: Experimental Results

devices discovered in 1 min

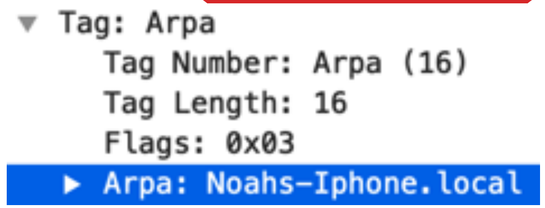


~2x devices discovered

persons' names in hostnames

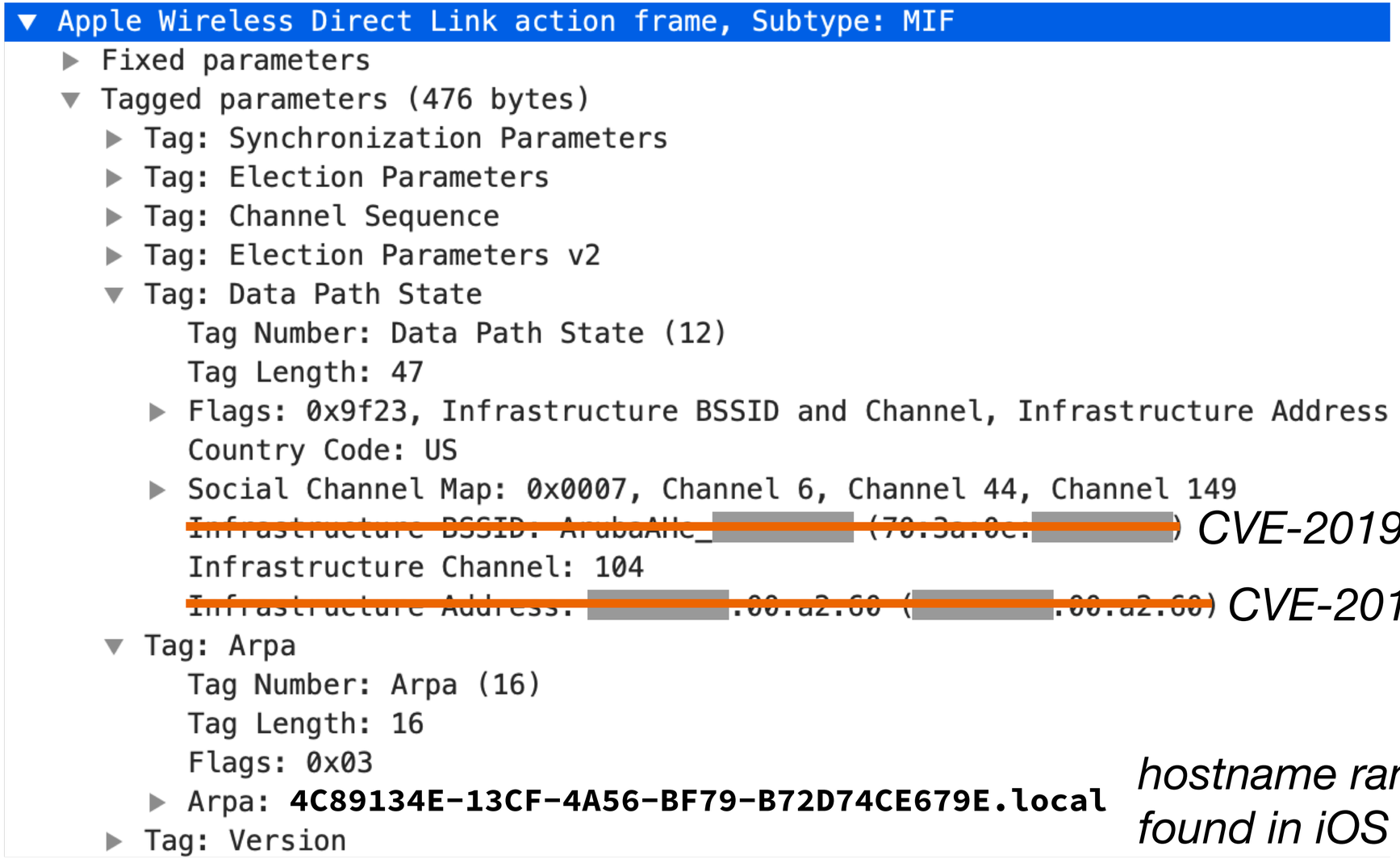


based on
2010 US Census and
1918–2017 US baby names



75% include person's name
(68% include the actual name)

Tracking: Mitigation



CVE-2019-8620

CVE-2019-8567

hostname randomization found in iOS 13 beta

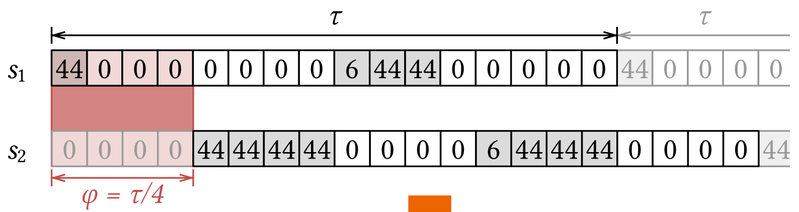
Vulnerabilities and Attacks

Remote activation
Brute force attack on Bluetooth LE discovery
fixed in iOS 12.2

User Tracking
Revealing MAC address and hostname
CVE-2019-8567
CVE-2019-8620

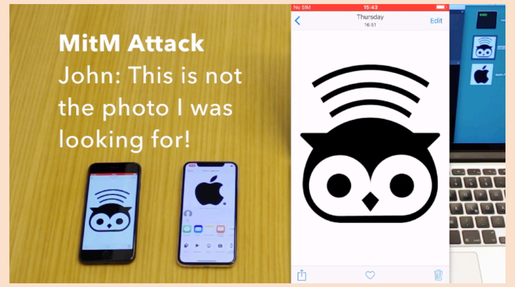
```
▼ Tag: Arpa
    Tag Number: Arpa (16)
    Tag Length: 16
    Flags: 0x03
  ▶ Arpa: Noahs-Iphone.local
```

Denial-of-Service
Breaking communication via desynchronization
CVE-2019-8612

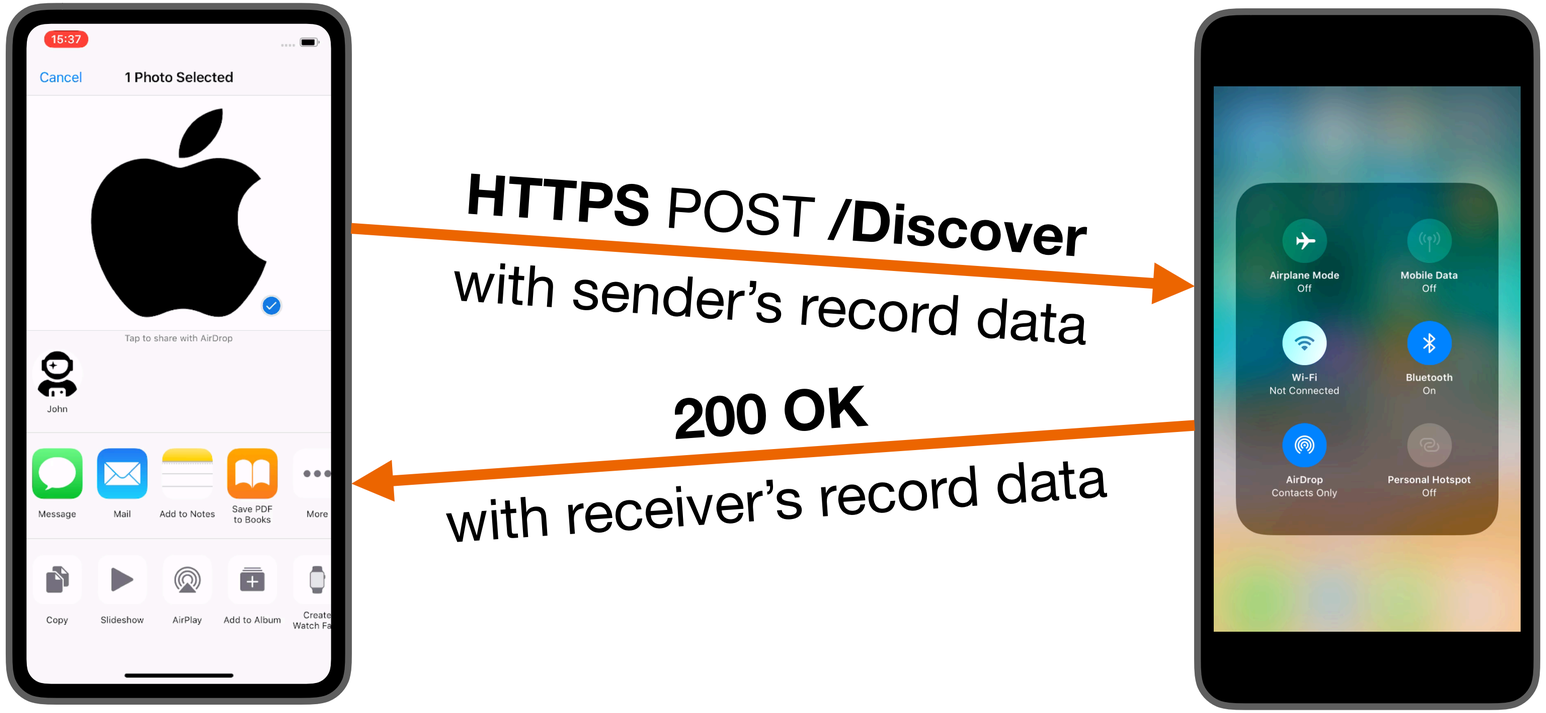


(Selective) Blackout
Crashing devices wirelessly through corrupt frames
CVE-2018-4368

Man-in-the-Middle
Intercepting files transmitted via AirDrop
fixed in iOS 13 beta



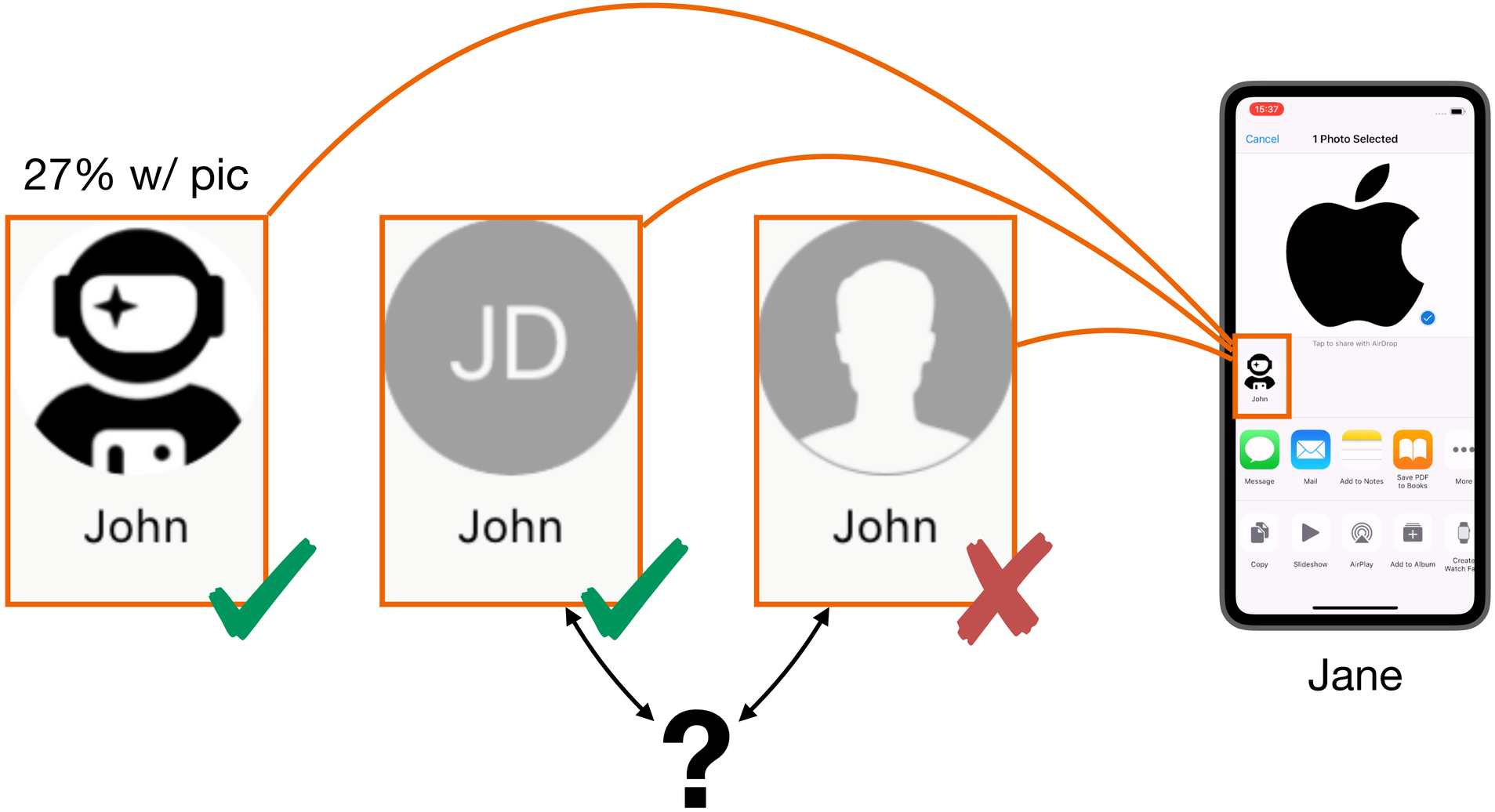
MitM: Recall AirDrop Authentication



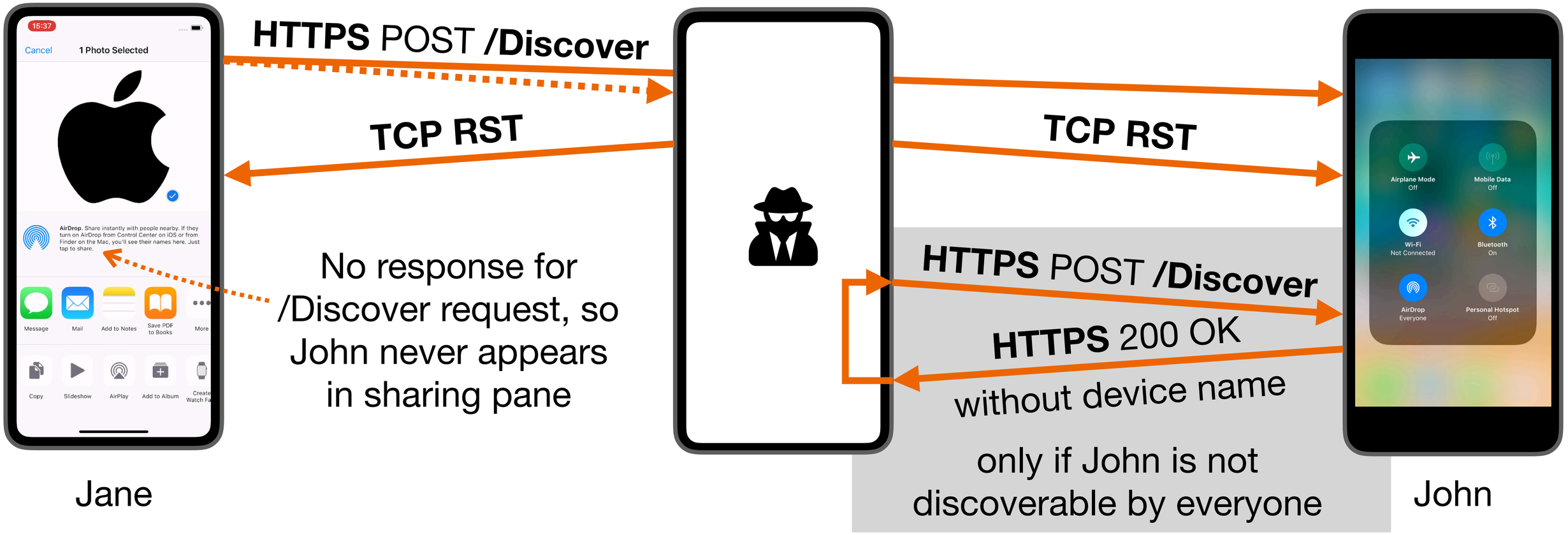
Jane

John

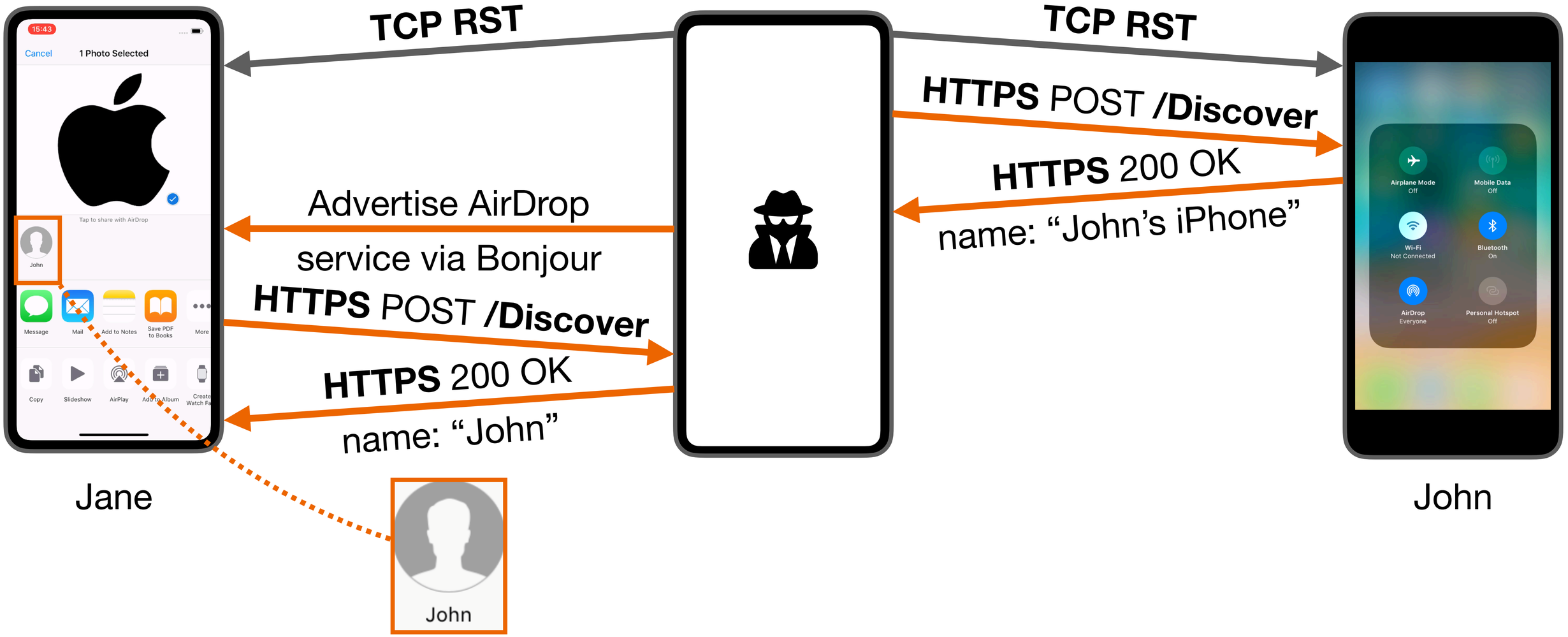
MitM: Ambiguous Receiver Authentication State



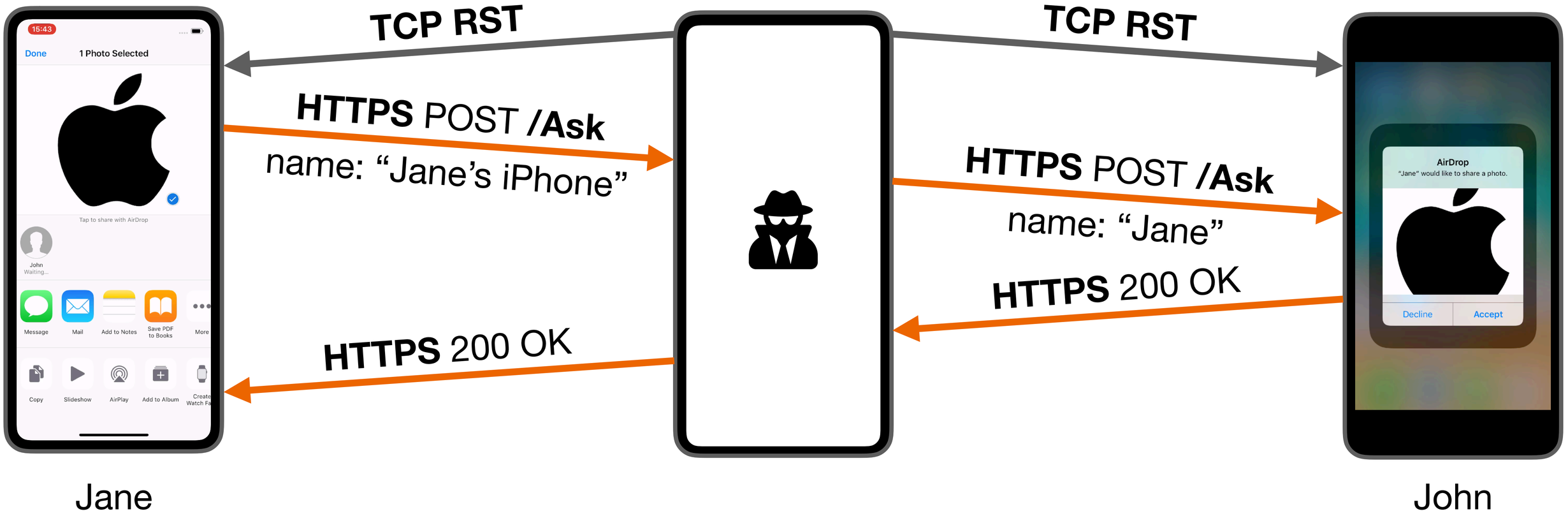
MitM: Breaking Authentication via DoS



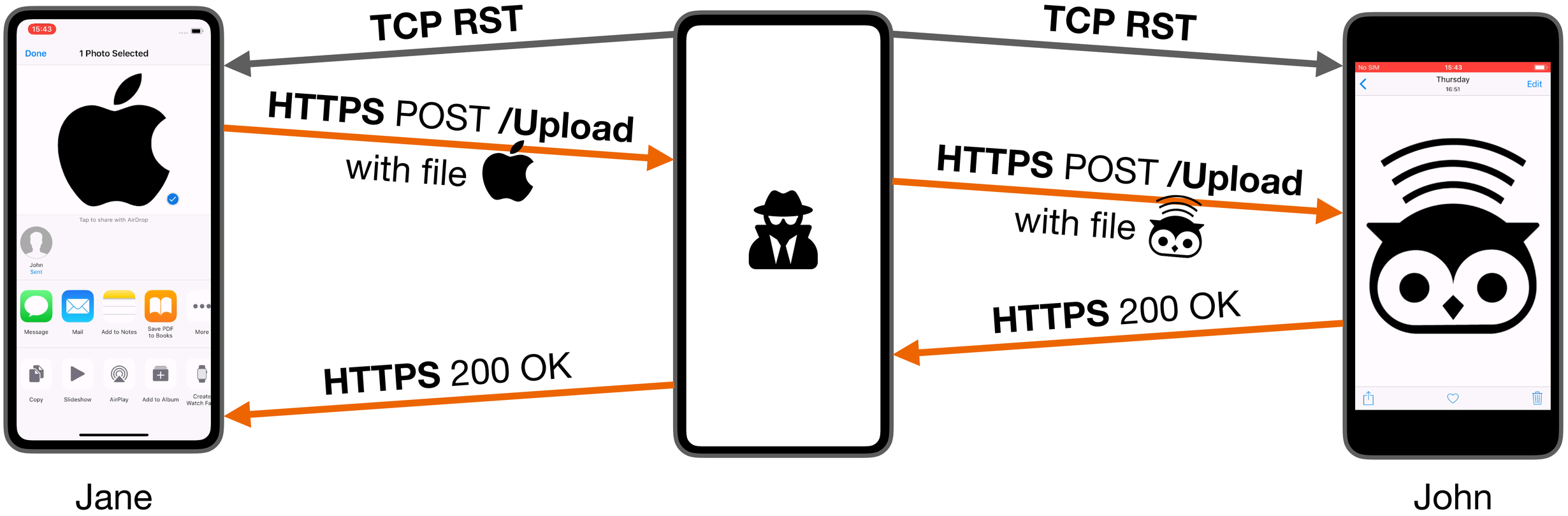
MitM: Identity Spoofing



MitM: Relaying Thumbnail



MitM: Replacing File

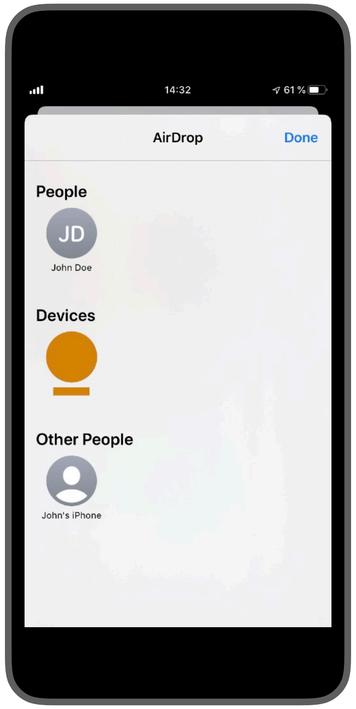


MitM: Mitigation

Contacts ✓

Own devices ✓

Others ✗



New sharing pane
in iOS 13 beta

Software

OpenDrop
AirDrop implementation written in Python

OWL
AWDL implementation written in C

… and more at https://owlink.org

Jerry Gamblin @JGamblin

Running an airdrop honeypot in Las Vegas has been more hilarious than I ever imagined.

```
Announcing service: host shrug, address fe80::d413:67ff:fe67:c417, port 8771
Starting HTTPS server
Receiving file(s) ...
File(s) received (size 0.31 MB, speed 7.40 MB/s)
```

CVE

CVE-2018-4368
CVE-2019-8567
CVE-2019-8620
CVE-2019-8612

possibly more to come in iOS 13 and macOS 10.15

Outlook

More services in Apple's wireless ecosystem (Handoff, Auto Unlock, …)

AWDL's successor **Neighbor Awareness Network (NAN)** is likely coming soon to xOS