Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of Apple ZeroConf

(Xiaolong Bai, **Luyi Xing)** (co-first authors),

Nan Zhang , XiaoFeng Wang , Xiaojing Liao , Tongxin Li , Shi-Min Hu

TNList, Tsinghua University,

Indiana University Bloomington

Georgia Institute of Technology,

Peking University

Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of **Apple ZeroConf**

Zero Configuration Networking (ZeroConf)

ZeroConf

- Bonjour

ZeroConf

- Bonjour protocol
  - zero-configuration networking over IP that Apple has submitted to the IETF.

- Goals:
  - With little or no configuration
  - to add devices/services to a local network
  - Existing devices can automatically find and connect to those new devices/services

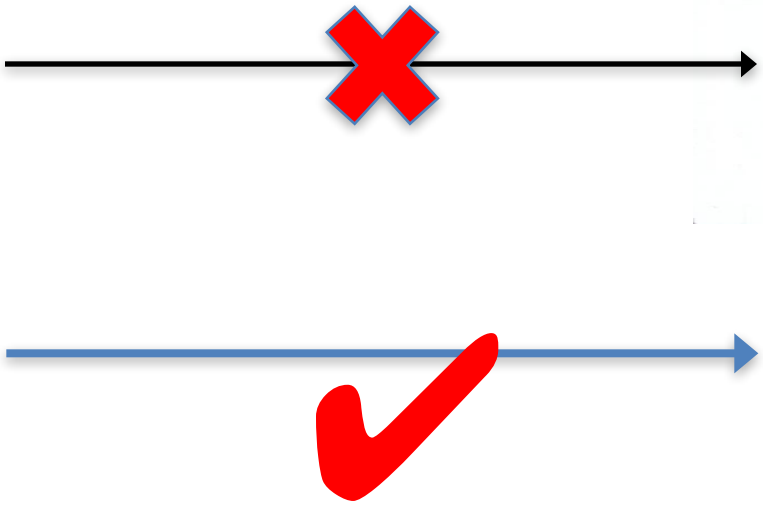
Bonjour

- Administrators
  - no need to assign IP, host names, service names to network services (e.g., printer)

- When first use a service, users simply
  - ask to see what network services are automatically available
  - and choose from the list.

How about traditional configured network?

Traditionally



Must Configure:

- IP
- Printer name,
  - e.g., lh135-soic.ads.iu.edu
- DNS server

Traditionally

Must Configure:

- IP
- Printer name,
  - e.g., lh135-soic.ads.iu.edu
- DNS server

Features of Bonjour

1. Service configures itself
   - IP, hostname, service instance name
2. Clients automatically discover available services
   - No pre-knowledge of the service's name, hostname or IP

1. ZeroConf Concept
2. So, how?

Add a new printer to a network

A printer configures itself

A printer configures itself

IP

fe80::abcd:1234

No?

Great, I'll take it.

A printer configures itself

IP

fe80::abcd:1234

Anybody using hostname

NPI9fe5.host.local?

A printer configures itself

IP

fe80::abcd:1234

Hostname

HP9FE5.host.local

No?

Wonderful, I'll take it.

A printer configures itself

IP

fe80::abcd:1234

Hostname

HP9FE5.host.local

Service Instance Name

HP-Service-9FE5

Anybody having a printing service named HP-Service-9FE5?

A printer finishes configuring itself

IP

fe80::abcd:1234

Hostname

HP9FE5.host.local

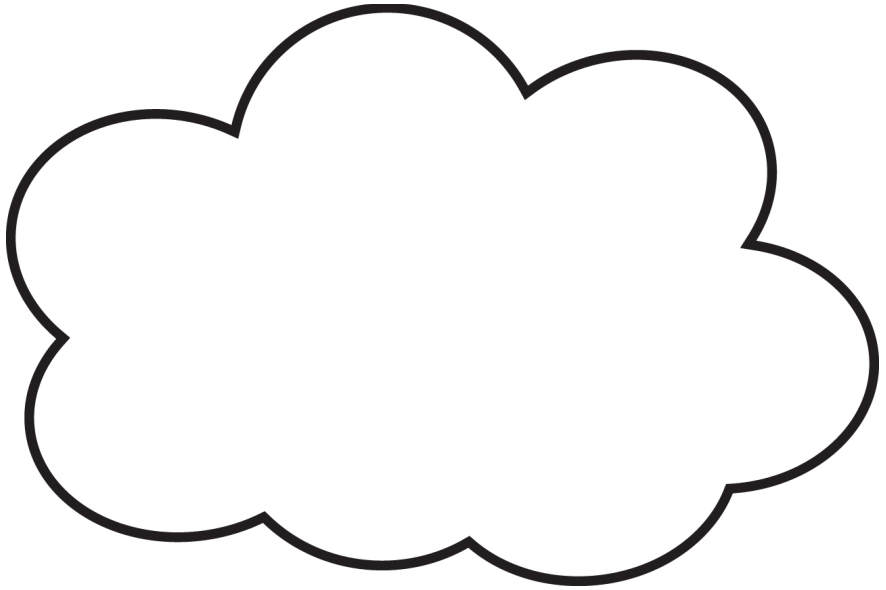
Service Instance Name

HP-Service-9FE5

Features of Bonjour

1. Service configures itself
   - IP, hostname, service instance name
2. Clients automatically discover available services
   - No pre-knowledge of the service's name, hostname or IP

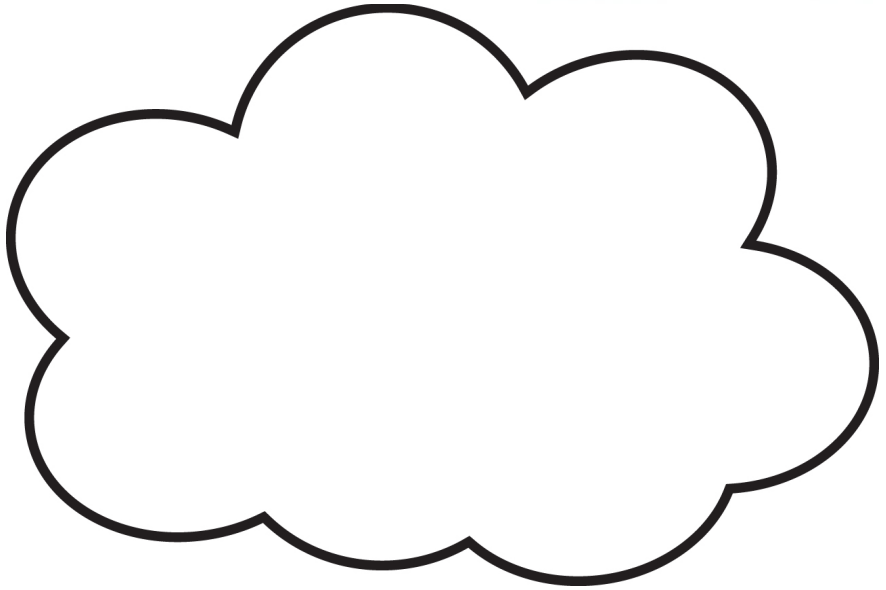
Automatically find the printer



Q1:
Anyone has a printer service?

A1:
I have HP-Service-9FE5

Automatically find the printer



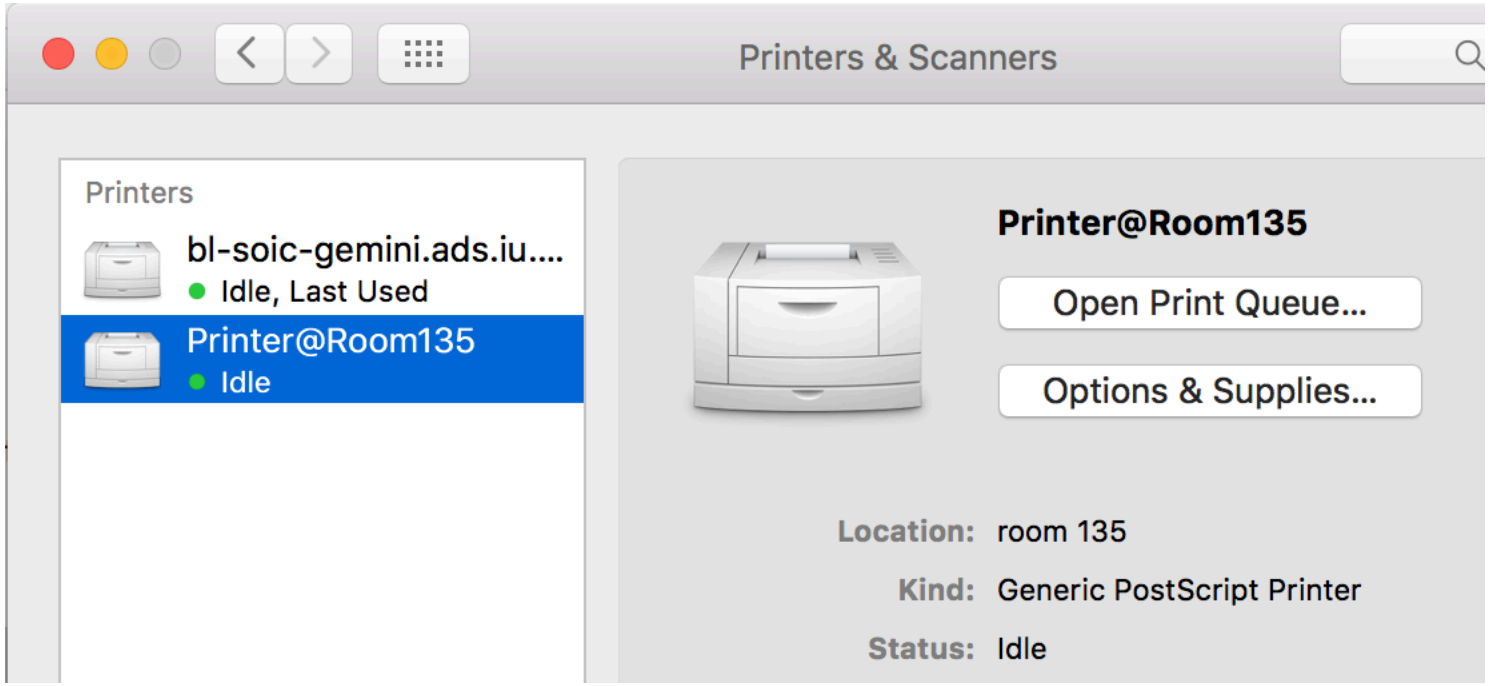
Q1:
Anyone has a printer service?

A1:
I have service instance
HP-Service-9FE5

Q2:
So on which host is this HP-Service-9FE5?

A2:
It's on host
NPI9fe5.host.local

Added/Saved the printer to your list



IP

fe80::abcd:1234

Hostname

HP9FE5.host.local

Service Instance Name

HP-Service-9FE5

Added/Saved the printer to your list

IP

fe80::abcd:1234

Hostname

HP9FE5.host.local

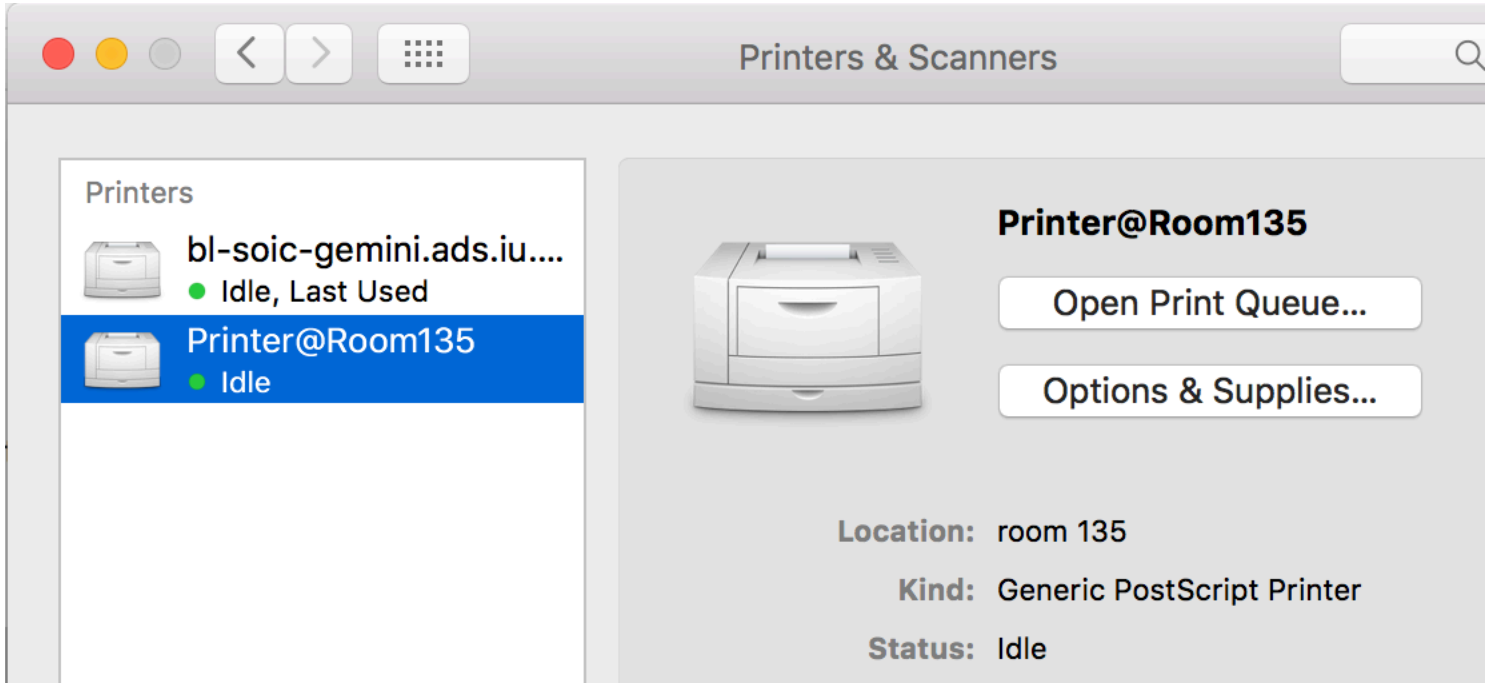
Service Instance Name

HP-Service-9FE5

Apple:

Applications store service instance names, so if the IP, port, or host name changed, the application can still connect.

Service instance name HP-Service-9FE5 is saved



~~IP~~
~~fe80::abcd:1234~~
~~Hostname~~
~~HP9FE5.host.local~~
Service Instance Name
HP-Service-9FE5

Saved printer =
A printer who owns service name HP-Service-9FE5

Adversary

- On a device (malware infected) in your local network
- Aims to intercept secrets/files transferred between uninfected devices

Adversary

- Your Mac/printer are un-infected
- Steal your printing documents?

1. ZeroConf Concept
2. ZeroConf How
3. ZeroConf Breaking

1. ZeroConf Concept
2. ZeroConf How
3. ZeroConf Breaking

Case 1: Printer

A device infected by malware

IP

Hostname

Service Instance Name

HP-Service-9FE5

A device infected by malware

IP

Hostname

Service Instance Name

HP-Service-9FE5

I have a printing service instance named

HP-Service-9FE5

Service Instance Name

HP-Service-9FE5

A device infected by malware

IP

Hostname

Service Instance Name

HP-Service-9FE5

I have a printing service instance named

HP-Service-9FE5

Service Instance Name

HP-Service-9FE5

Saved printer =
A printer who owns service name HP-Service-9FE5

New Service Name

HP-Service-9FE5 (2)

Service Instance Name

HP-Service-9FE5

Why it happens?

Three Changing Attributs:

- IP
- Hostname
- Service Instance Name

Apple:

Applications store service instance names, so if the IP, port, or host name changed, the application can still connect.

Lack of authentication

Three Changing Attributs:

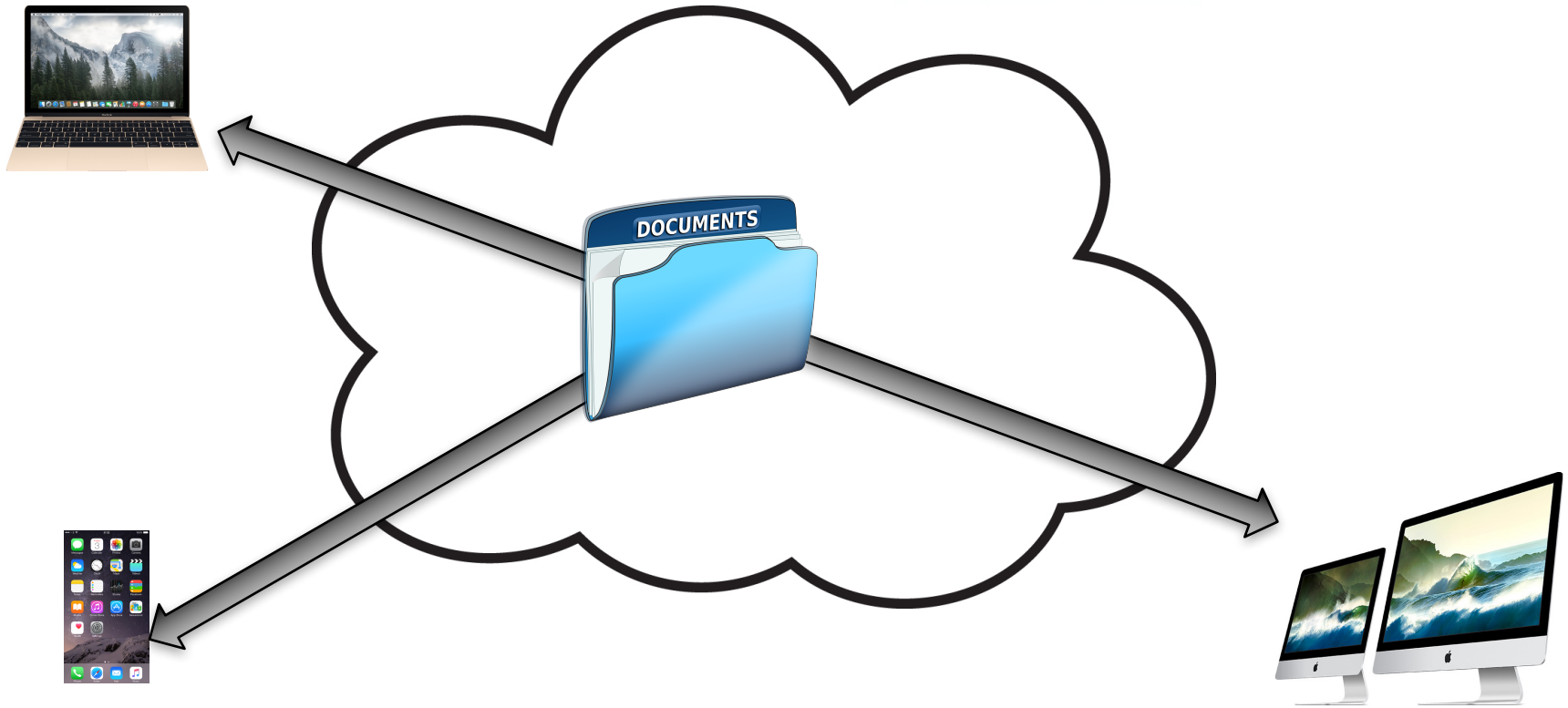
- IP
- Hostname
- Service Instance Name

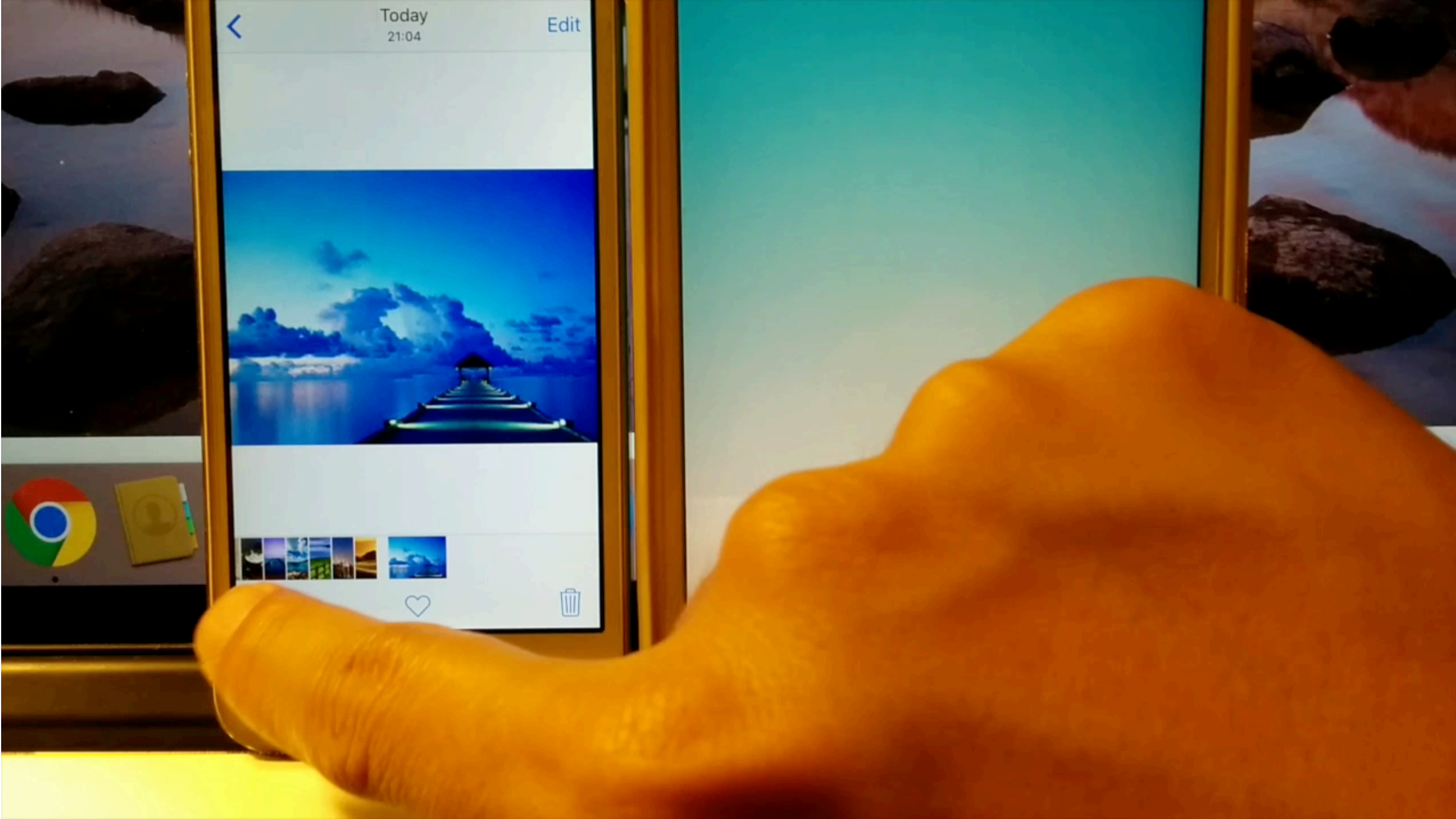
- Anyone can claim any value of the three attributes
- The protocol only guarantees no duplicates.

1. ZeroConf Concept
2. ZeroConf How
3. ZeroConf Breaking

Case 2: Airdrop

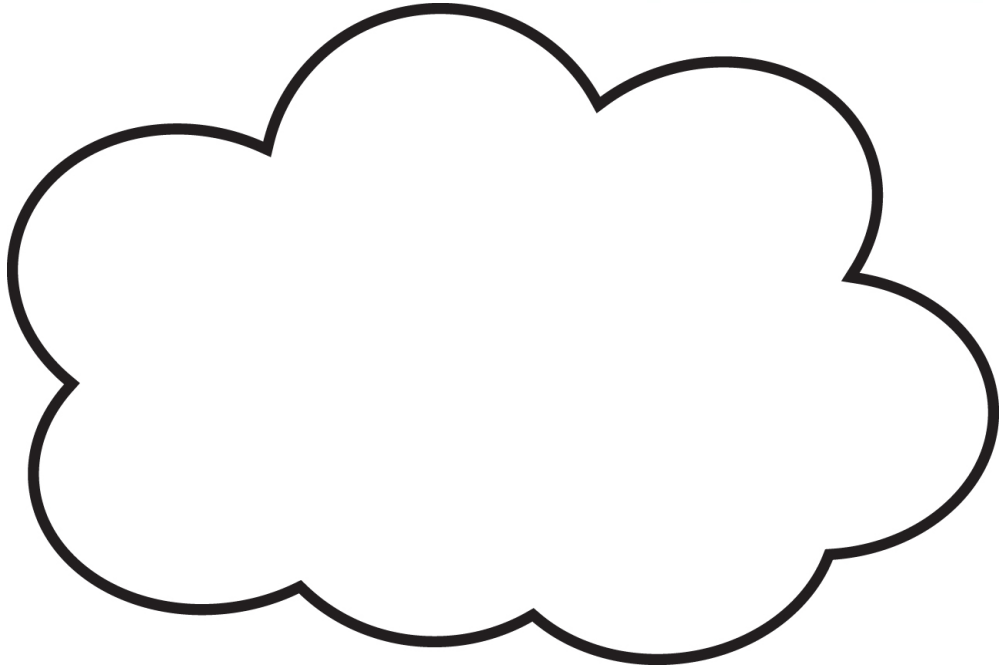
Airdrop between Apple devices




Today
21:04
Edit

Attack Airdrop

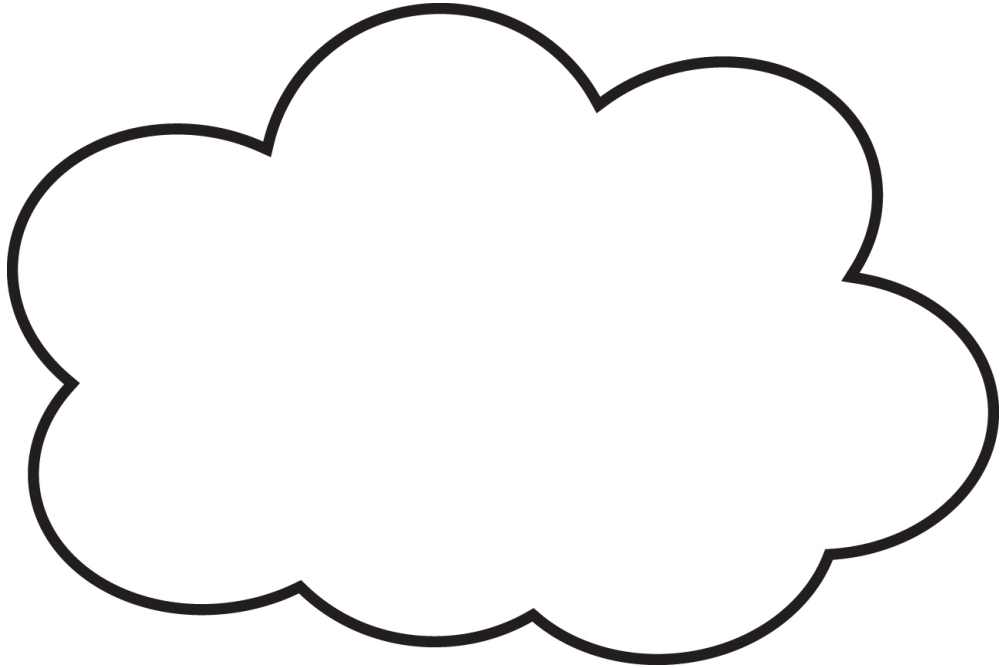
Jeff's Macbook:
Q1: Anyone has an airdrop service?



Alice's iPhone:
I have a service named abcd.airdrop.service

Attack Airdrop

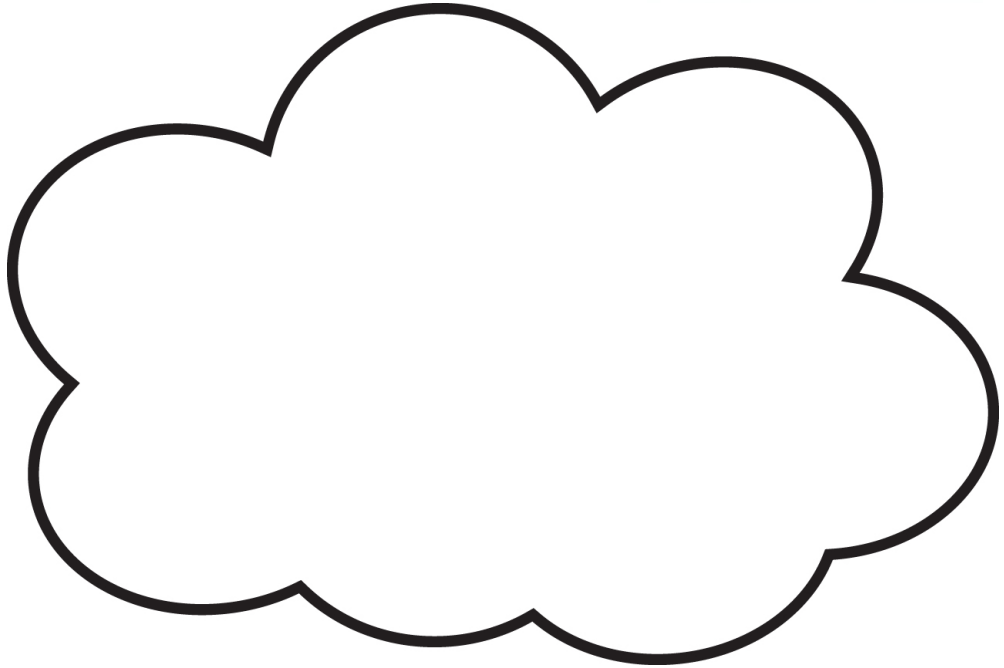
Jeff's Macbook:
Q2: So on which host is Alice's service?



Alice's iPhone:
I have a service named abcd.airdrop.service

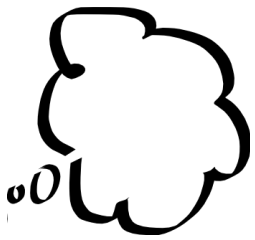
Attack Airdrop

Jeff's Macbook:
Q2: So on which host is Alice's service?



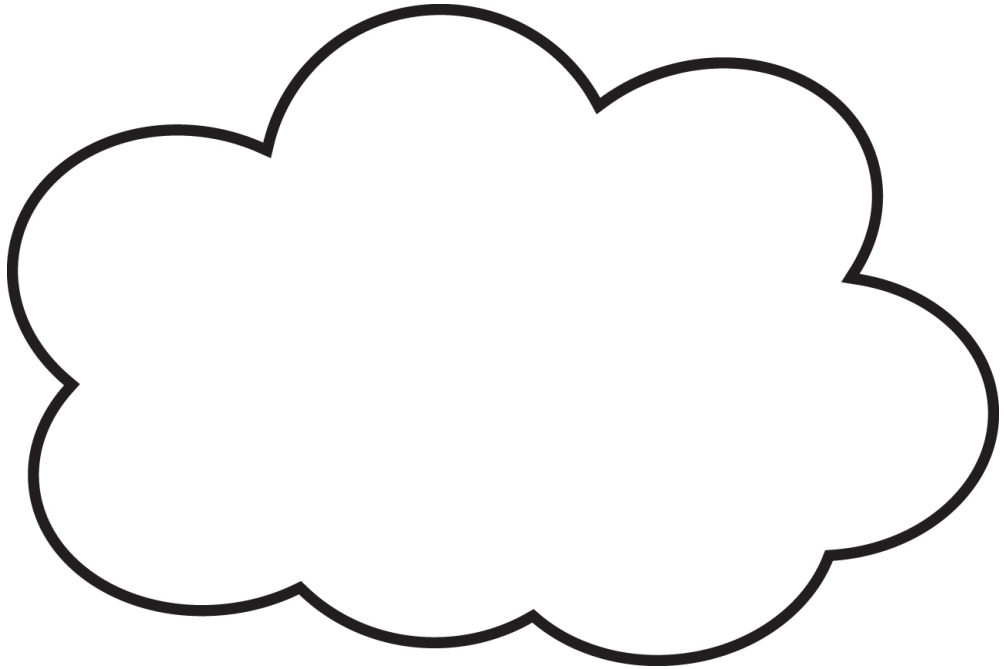
Bob's iMac:
A2: It's on host Bobs.imac.local

Alice's iPhone:
A2: It's on host Alices.iphone.local



Alice's iPhone has service named abcd.airdrop.tcp, which is on host Bobs.imac.local

Jeff's Macbook:
Q2: So on which host is Alice's service?

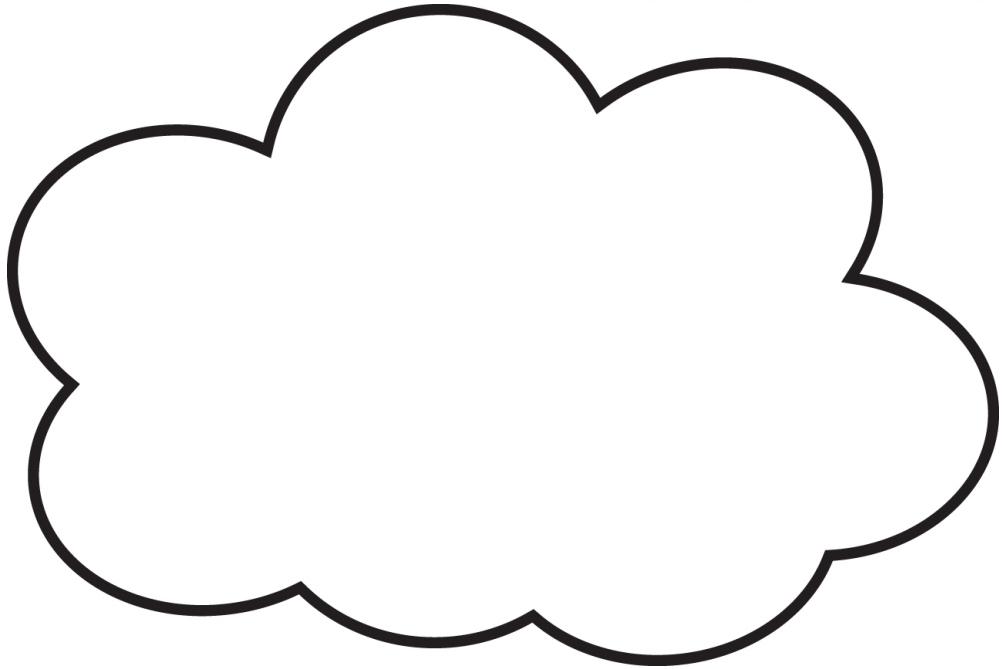


Bob's iMac:
A2: It's on host Bobs.imac.local

Alice's iPhone:
A2: It's on host Alices.iphone.local

Attack Airdrop

Jeff's Macbook:
Connect
https://Bobs.imac.local

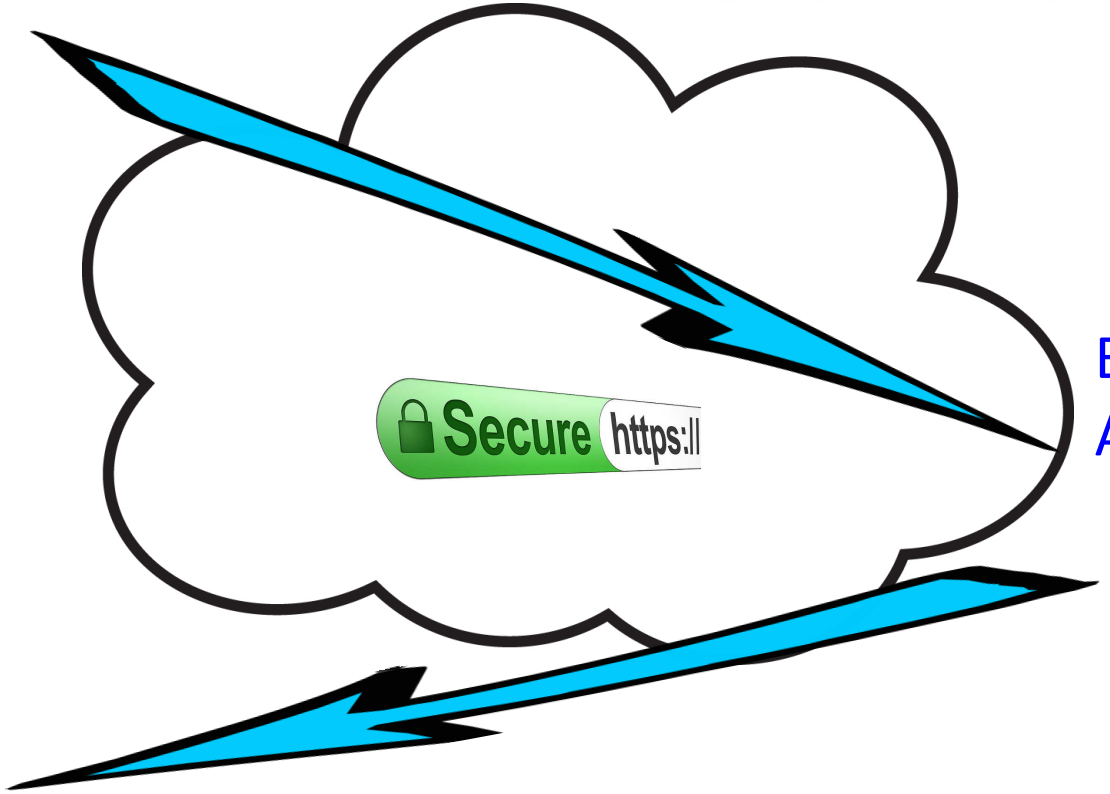


Bob's iMac:
A2: It's on host Bobs.imac.local

Alice's iPhone:
A2: It's on host
Alices.iphone.local

Does TLS help?

Jeff's Macbook:
Connect
https://Bobs.imac.local



Bob's iMac:
A2: It's on host Bobs.imac.local

Alice's iPhone:
A2: It's on host
Alices.iphone.local

TLS in Airdrop

Jeff's Macbook

https://Bobs.imac.local

Server certificate issued to appleid. CDEF …

Bob's iMac

https://Alices.iphone.local

Server certificate issued to appleid.ABCD…

Alice's iPhone

So the certificate in airdrop can hardly be used for authentication.

Jeff's Macbook

https://Bobs.imac.local

Server certificate issued to appleid.CDEF…

Bob's iMac

https://Alices.iphone.local

Server certificate issued to appleid.ABCD…

Alice's iPhone

Domain should match the certificate

Jeff's Macbook

https://Bobs.imac.local

Server certificate issued to appleid.CDEF…

Bob's iMac

https://google.com

Certificate issued to google.com

Domain should match the certificate

Jeff's Macbook

https://Bobs.imac.local

Server certificate issued to appleid.CDEF…

https://Alices.iphone.local

Server certificate issued to appleid.ABCD …

Bob's iMac

Alice's iPhone

What's wrong with TLS in Airdrop

- The certificate in airdrop cannot be used for authentication
  - E.g, certificate should be issued to Alice
  - but indeed issued to appleid.ABCD…
- Linking a human to her certificate is complicated
  - challenge in finding any identifiable information that are
    - well-known
    - no privacy implication
    - and unique

Some customized ZeroConf protocols

- FileDrop
  - TCP packets for discovery
  - elliptical curve cryptography for security
  - Failed in authentication
    - challenge in linking a human to her public key

1. ZeroConf Concept
2. ZeroConf How

3. ZeroConf Breaking

Case 3: Apple’s Vulnerable framework

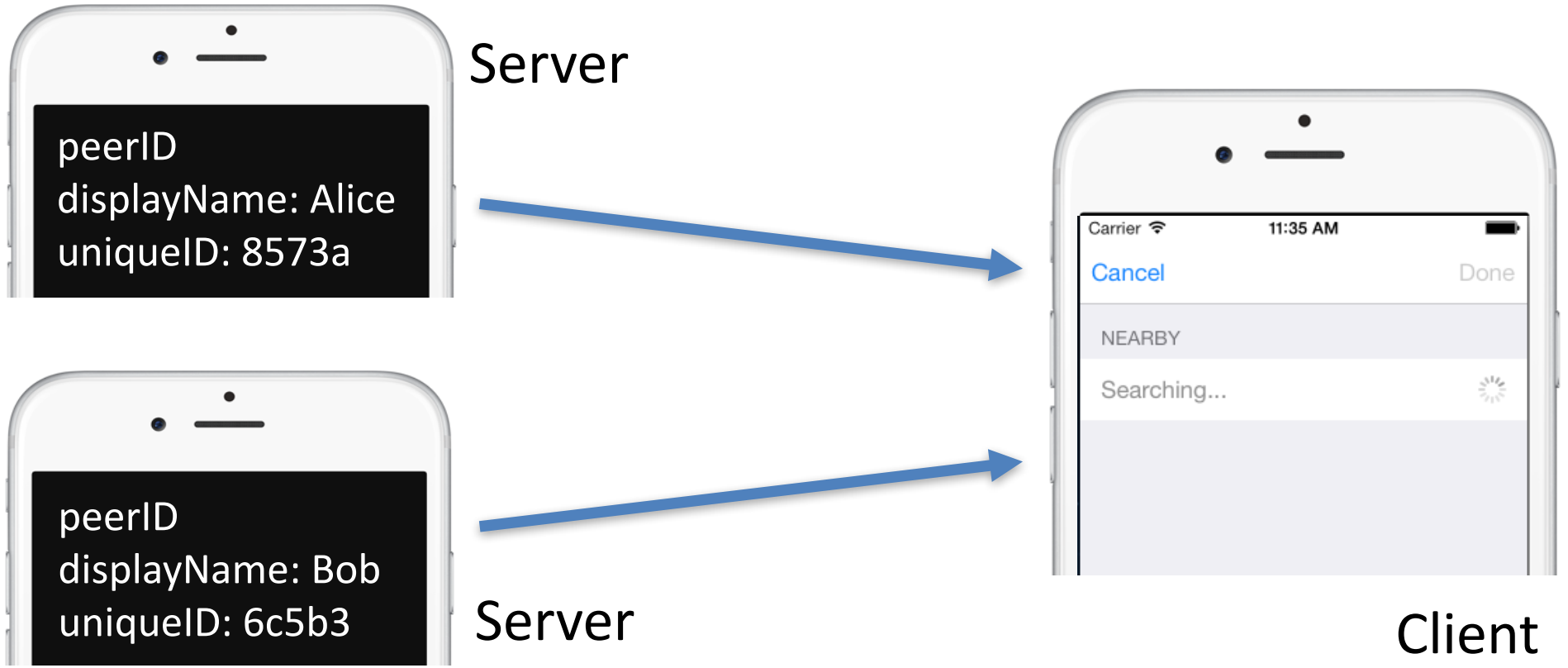
Apple’s Vulnerable framework

- Multipeer Connectivity (MC)
  - A framework for automatic service discovery between nearby devices across Wi-Fi and Bluetooth without configuration
- Object to identify each app: peerID
  - displayName (public) & uniqueID (private)



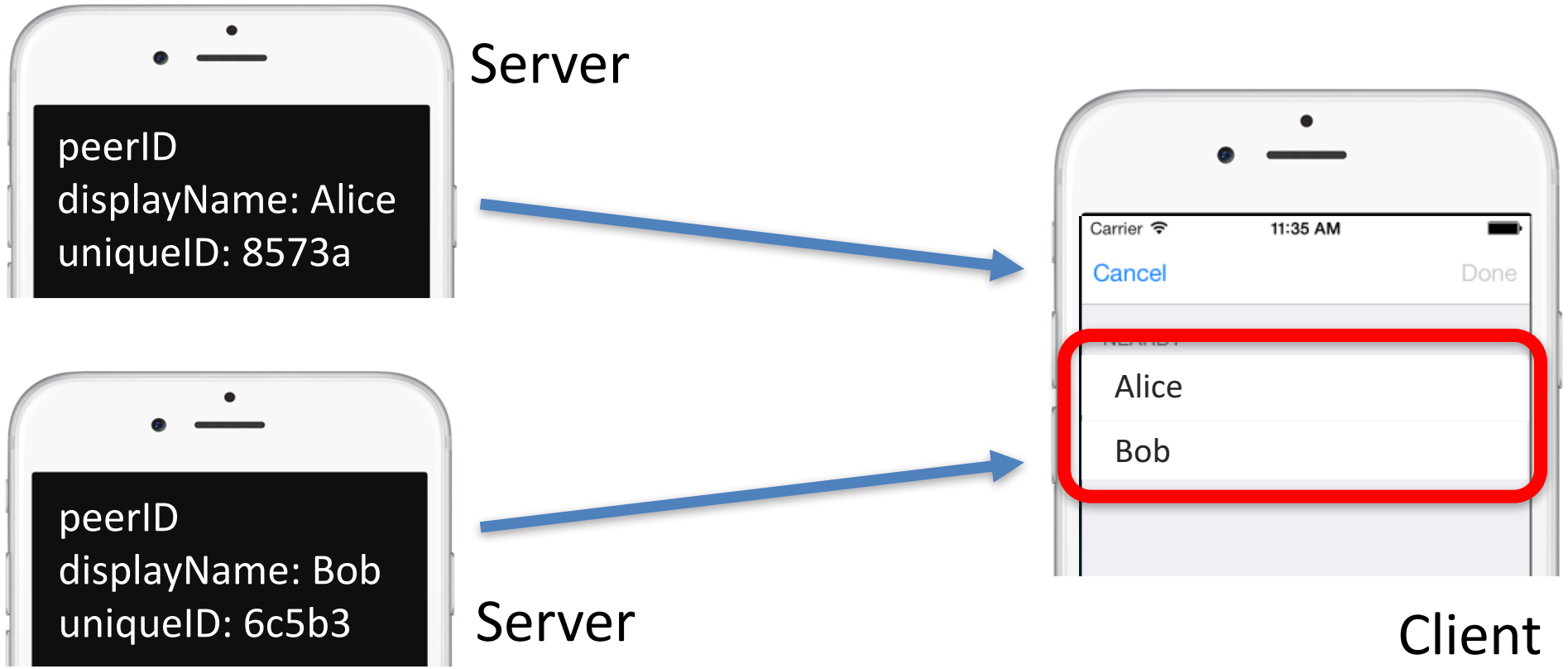
Normally

- Automatic Service Discovery Without Configuration
  - Servers advertise peerIDs



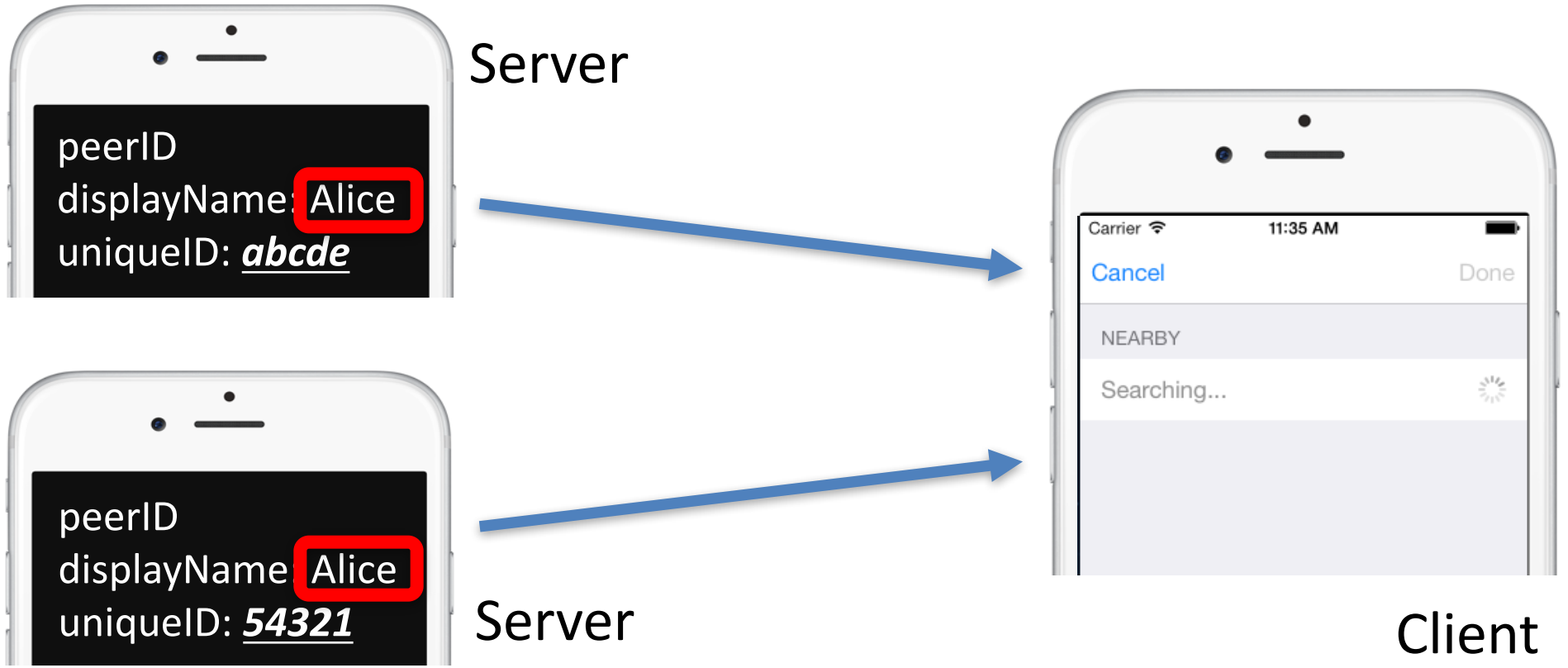
Normally

- Automatic Service Discovery Without Configuration
  - Servers advertise peerIDs, Client browse peerIDs (show displayName)



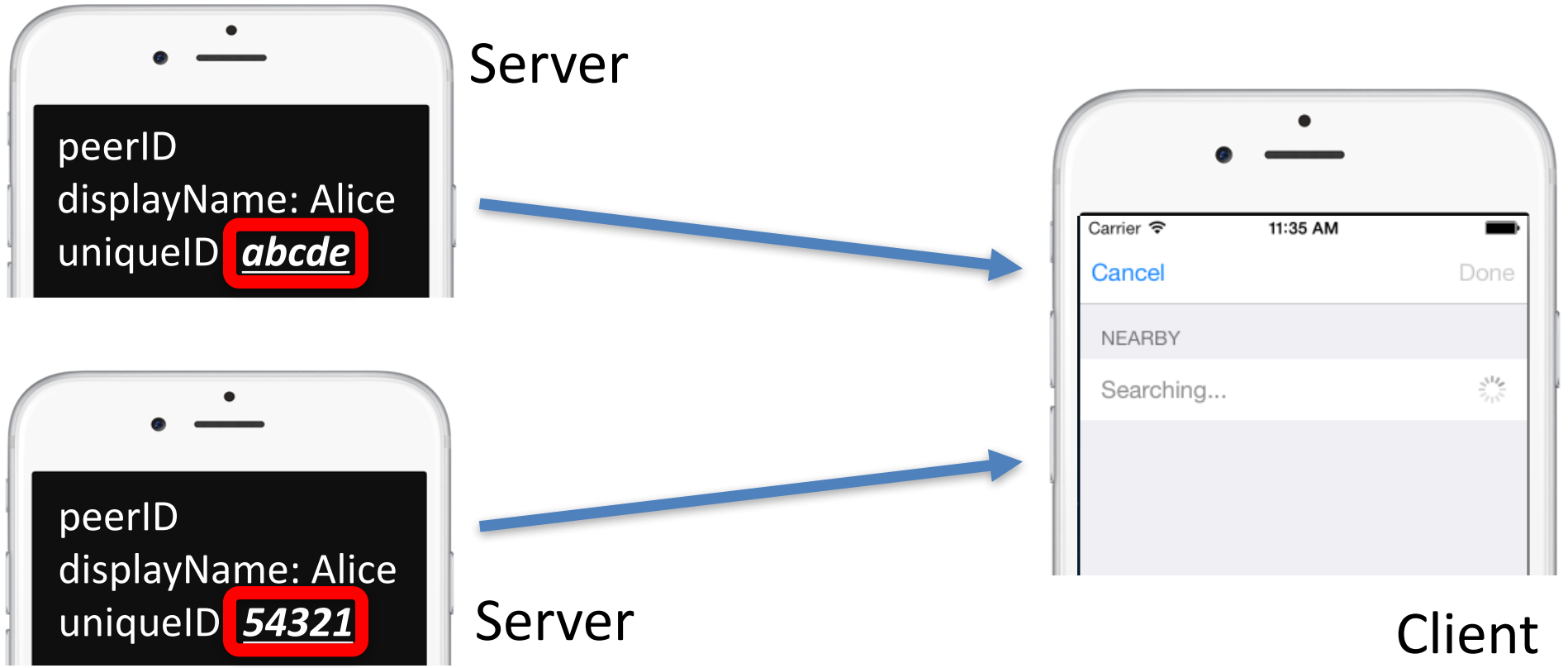
Normally

- Even if servers have the same displayName



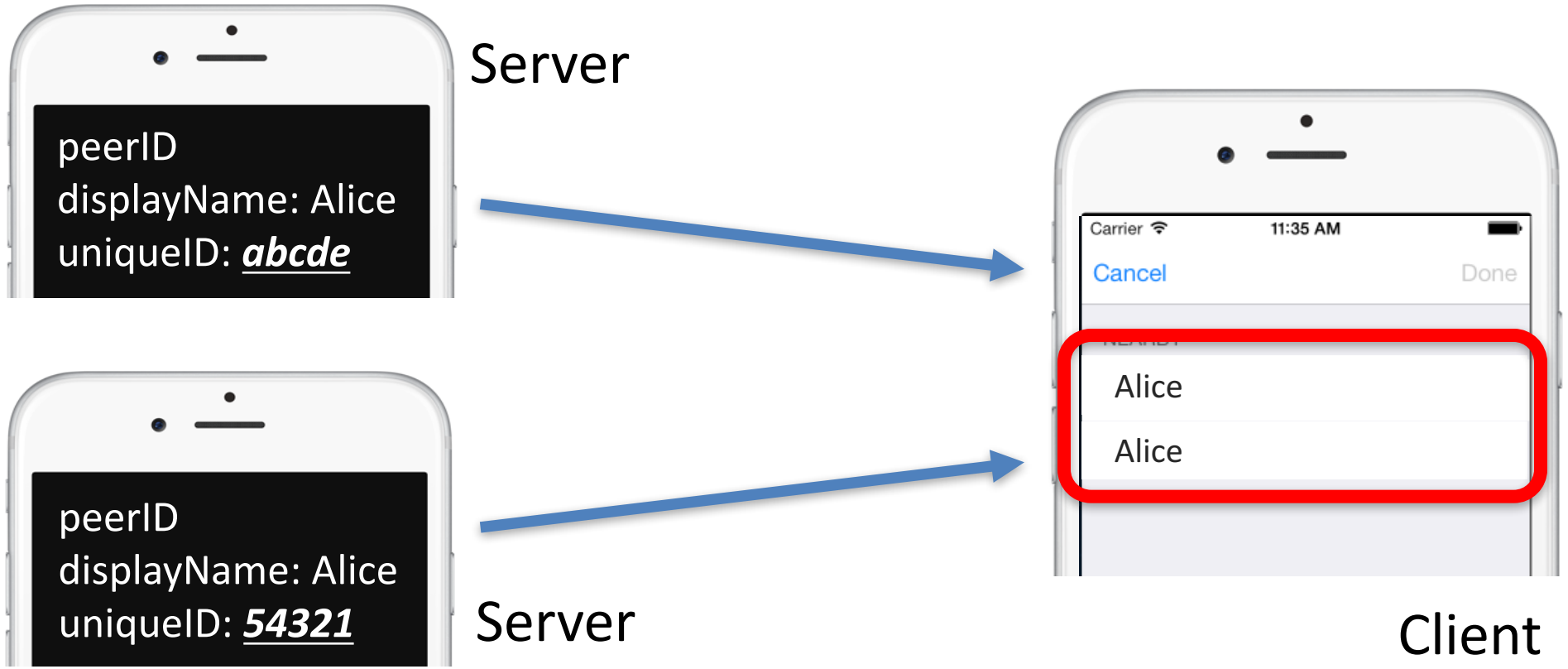
Normally

- Even if servers have the same displayName
  - uniqueIDs generated by MC will always be different



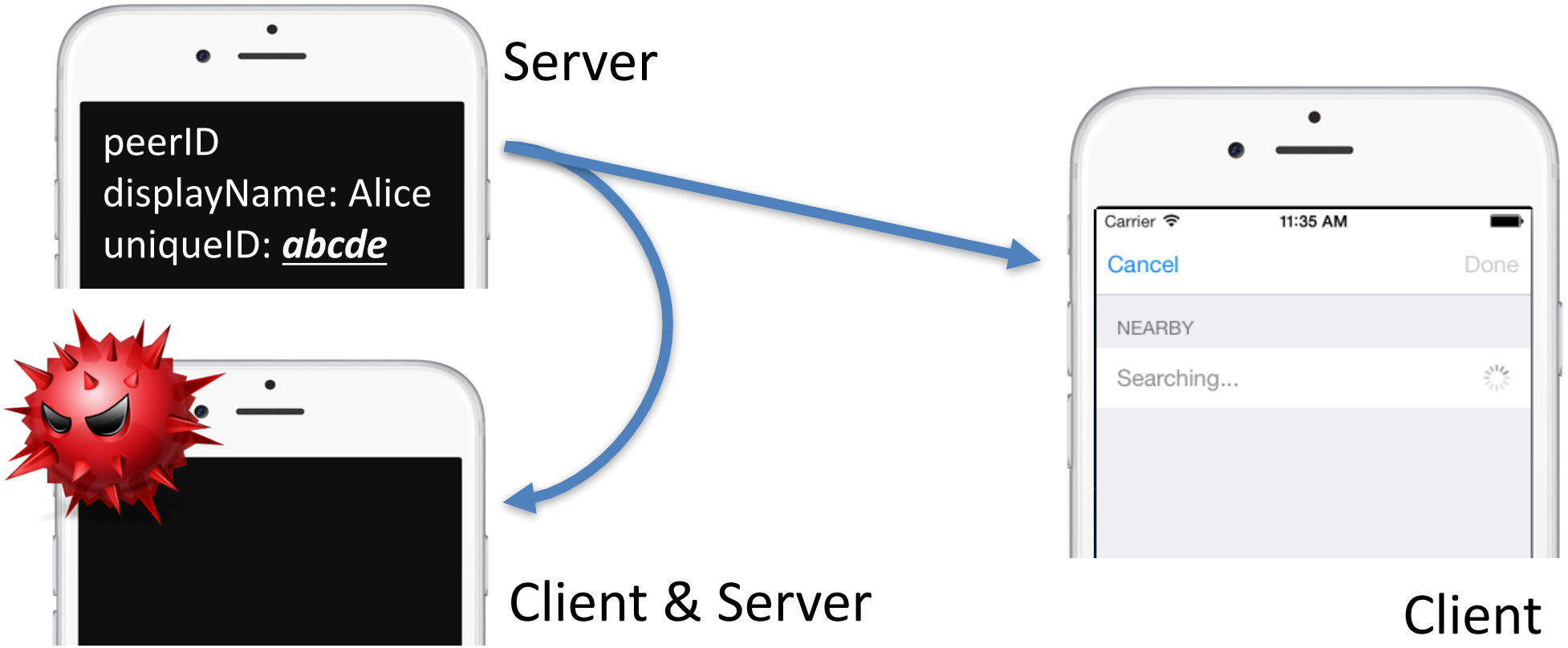
Normally

- Even if servers have the same displayName
  - uniqueIDs generated by MC will always be different



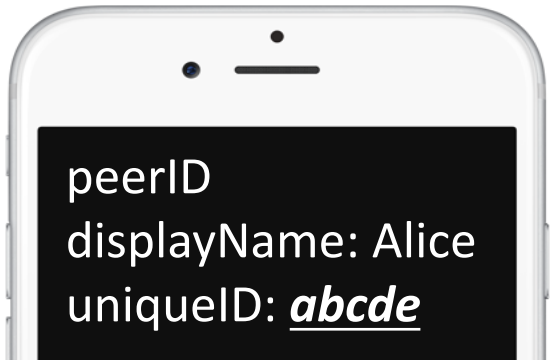
What Can Go Wrong?

- Attacker acts as both client and server
  - Browse and acquire peerID object from victim server



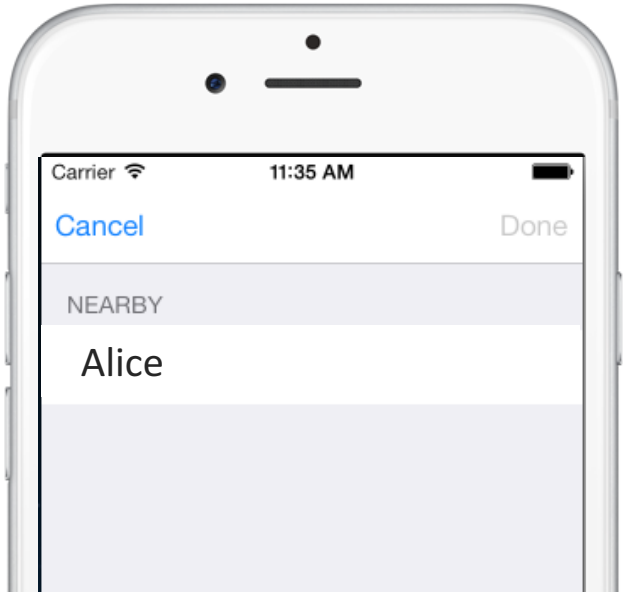
What Can Go Wrong?

- Attacker acts as both client and server
  - Advertise using the same peerID object



Server

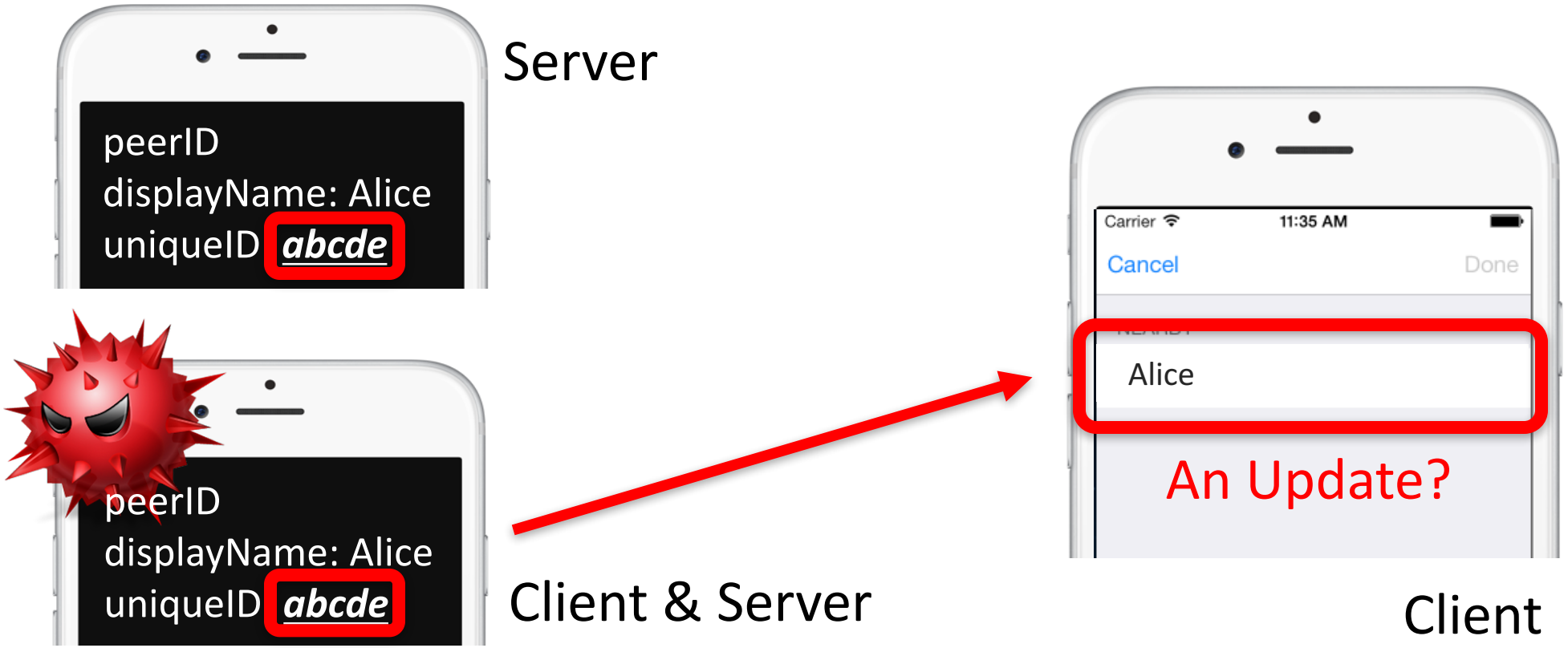
Client & Server



Client

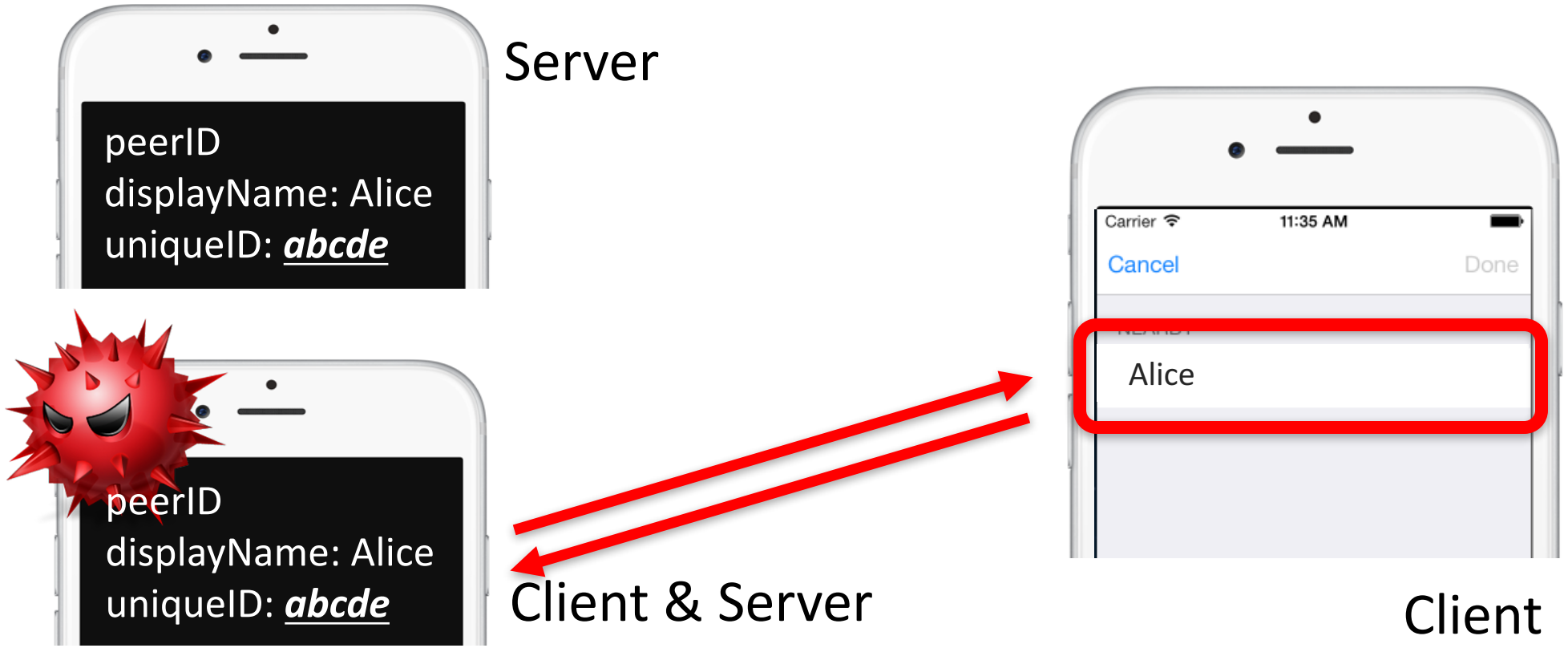
What Can Go Wrong?

- Client can not distinguish because of same uniqueID



What Can Go Wrong?

- Client can not distinguish because of same uniqueID
- Client maps the only peer to attacker's address **(MitM)**

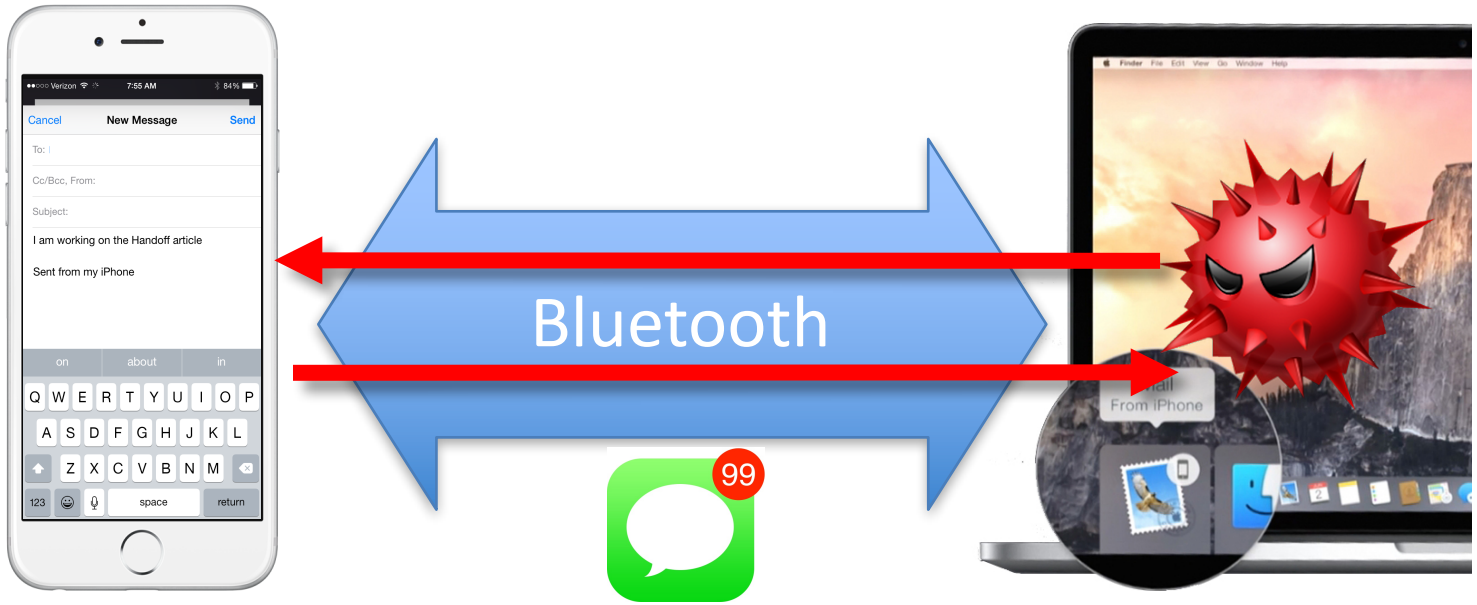


1. ZeroConf Concept
2. ZeroConf How
3. ZeroConf Breaking

Case 4: Bluetooth

All your iOS notifications belong to me

- ZeroConf on Bluetooth: Apple Handoff
  - Handoff creates Bluetooth channel without configuration
- Malicious app on Mac can steal notifications on iPhone
- For details, please refer to our paper



Summary of attacks

- Attacks on Apple ZeroConf channels
  - Printer (Bonjour)
  - Airdrop (Bonjour)
  - Multipeer Connectivity (MC)
  - Handoff
- Attacks on other channels (please refer to our paper)
  - BLE
  - Customized ZeroConf protocols
- All vulnerabilities were reported to vendors, acknowledged by most vendors

1. ZeroConf Concept
2. ZeroConf How
3. ZeroConf Breaking
4. Impact

Impact

- Measurement
  - We analyzed 61 popular Mac and iOS apps working with ZeroConf
  - 88.5% are vulnerable to man-in-the-middle or impersonation attacks

ZeroConf Channels	Vulnerable/ Sampled	Sensitive Information Leaked
Bonjour	18/22	files, directories and clipboard synced, documents printed, instant message
MC	24/24	files and photos transferred, instant message
BLE	10/13	User name and password for OS X
Customized protocols	2/2	remote keyboard input and files transferred

1. ZeroConf Concept
2. ZeroConf How
3. ZeroConf Breaking
4. Impact
5. Protecting ZeroConf

Protecting ZeroConf

- Problem: linking a human to her certificate is complicated
- Speaking out Your Certificate (SPYC)
  - Voice biometrics ties certificate to identity
  - Human Subject Study: convenient and effective
- For more details, please refer to our paper

Conclusion

- Apple's ZeroConf techniques are not secure as expected
  - The usability-oriented design affects security
- Addressing such security risks is nontrivial
  - Challenge in binding a human to her certificate
- Our Defense: SPYC
  - Voice biometrics ties certificate to identity

ZeroConf

- The ZEROCONF Working Group's requirements and proposed solutions for zero-configuration networking over IP essentially cover three areas:
  - addressing (allocating IP addresses to hosts)
  - naming (using names to refer to hosts instead of IP addresses)
  - service discovery (finding services on the network automatically)