Protecting Multicast Usage with Entitlements

Tommy Pauly
MBONED
IETF 112, November 2021, Virtual

Local Network Restrictions

iOS 14 introduced Local Network Privacy features

Apps must get user permission before communicating with hosts on the local network

Apps must declare a static list of Multicast DNS (dns-sd) service types they use

Apps must have an entitlement to send and receive generic multicast/broadcast

Motivation

Arbitrary scanning of the local network opens up privacy risks

SDKs embedded within apps could fingerprint networks to track user location

APIs where specific service types are specified are preferred in order to open up only what is needed

Non-standard protocols like SSDP have known security vulnerabilities (DDoS), and are the most common request for multicast

Looking forward

Apps with legitimate reasons for needing custom multicast can be approved

Common SDKs should move to use a system-supported API that doesn't require entitlements

Currently, this is Bonjour / mDNS

Are there other uses that this community thinks should be added?

Resources

WWDC presentation

https://developer.apple.com/videos/play/wwdc2020/10110/

Multicast networking article

https://developer.apple.com/news/?id=0oi77447

Questions?