Security Analysis of Apple's Continuity



Apple's Continuity and proximity features rely on peer-to-peer connectivity. Historically, AWDL has powered major Apple peer-to-peer capabilities, and it has been studied as a proprietary 802.11-based ad hoc protocol at scale. At the same time, AirDrop has a known history of design and implementation issues, including demonstrated man-in-the-middle and tracking-related vulnerabilities in prior work. The current moment introduces a new and unusually rich research setting: regulatory-driven interoperability is pushing Apple to support Wi-Fi Aware alongside AWDL, as reflected in EU DMA-related documentation that explicitly references both AWDL and Wi-Fi Aware. In parallel, Google has announced Quick Share interoperability with AirDrop, initially rolling out to Pixel 10, creating a heterogeneous multi-vendor implementation environment. This creates precisely the type of multi-stack transition period where protocol confusion and downgrade surfaces historically emerge.

During the internship, the intern will focus on security invariants rather than assuming a specific exploit. The intern will reconstruct the protocol involved in AirDrop-like sharing and selected Continuity workflows, then extract security parameters such as the algorithm used, key binding, authenticity, downgrade resistance, replay and reordering tolerance, and what exactly user approval binds. The intern will then implement a controlled adversarial testing harness that exploits the insecurities found. The core goal is to identify any security regressions or ambiguities introduced by cross-ecosystem interoperability. As a secondary validation, the intern will repeat a subset of tests in an Apple and Android setting using Quick Share and AirDrop interoperability to evaluate whether heterogeneity amplifies protocol confusion risks.

Practicalities

Supervisors:	Sayon Duttagupta	sayon.duttagupta@esat.kuleuven.be	office B01.17
	Amit Singh Bhati	amitsingh.bhati@3milabs.tech	office B01.17

Nature of the work:	20% theoretical work, 80% software (implementation on embedded devices)
Number of students:	1 or 2

 © 2025-2026 COSIC