

# SPLIT INTERFACES (SPIN)

Jordi Domingo-Pascual

Universitat Politècnica de Catalunya – BarcelonaTECH (UPC)

VFCS17. ISCTE. Lisboa. October 24, 2017



# **SPLIT INTERFACES (SPIN)**

The main goal is to decouple the devices from the interfaces they use.

Privacy and security should be enforced at all levels.

# Current Trends

- Data is stored in the cloud and may be accessed and shared by several devices.
- Offload the traffic from 3G/4G networks to Wi-Fi for bulk transfers when possible.
- Applications and apps are stored in the user's device. Apps are becoming more demanding in terms of resources, memory storage, computing power and power consumption.
- The number of apps in a mobile device is increasing day by day. From light-weight apps providing the basic user interface and minimal processing the trend is to develop heavier apps eating device resources.
- The user interface is limited by the device. There is a race for finding

# Split Interfaces Architecture

- Data is stored in the cloud.
- Applications and apps are stored and executed in the cloud. Be it the Edge Cloud, Home Cloud or Local Cloud.
- Offload apps workload to the cloud.
- Decouple the User's Device (**UD**) from the I/O devices (**IOD**) providing the interfaces.
- The User Device may be the I/O device, as it is nowadays, or it may use external interfaces too.
- User Devices and I/O Devices are simple interfaces sending and receiving data flows. In case of Virtual Reality or Augmented Reality they may not be so simple.

# Communication Requirements

- Pervasive connectivity (as the power grid provides electricity seamlessly anywhere, anytime).
- Secure lightweight protocol between User Device and each of the I/O devices (Bluetooth-like but with improved security).
- Pervasive connectivity provides basic connectivity and supports control communications between the UD and IODs.
- UD establishes control channels requesting and granting permission for using IODs.
- IOD are connected to a high-speed network (fixed or wireless).

# Objects and Identifiers

- Device identifiers. UD, IOD and Service Devices (SD) have a unique “physical” identifier.
- Network identifier. Maybe the current IP address.
- Service / Application identifier. Each service, application, app has its own identifier.
- User identifier. It is not a personal ID; it is a “user profile” identifier. At the UD user identifiers are associated with the corresponding credentials, allowed device identifiers and service/application identifiers.  
A person may have a user identifier for private, family and friends use, a professional user identifier, and one or more social or community user identifiers. This provides isolation among the different spheres of

# Use Cases (Examples)

- **Entertainment.** From the user's device (smartphone) use the home cinema equipment so that video and audio flows go directly from the contents provider to the home cinema equipment using its high capacity connection and not the device connectivity.
- **Working environment .** Use a large screen, or big-size touch screen as desktop, and other local devices being all of them managed from the User's Device. Think of a working place somewhere with all office facilities connected to the network. From the user's device, devices are associated to and managed from the user's device. User device supports control communications only, while data flow to and from the selected interfaces and the corresponding data and application servers.
- **Personal Health.** A patient through the user's device may access and display complex health records (e.g. geographic TACs) to the doctor's

# SPLIT INTERFACES (SPIN)

Jordi Domingo-Pascual

Universitat Politècnica de Catalunya – BarcelonaTECH (UPC)

VFCS17. ISCTE. Lisboa. October 24, 2017

