

- Proximity Services
 - IoT Device Management
 - Automatic configuration of nearby IoT devices
 - More fluent interaction via voice control
 - Case study: Bluetooth Low Energy Beacons
 - Automatic Device Grouping
 - Modalities: sound, ultrasound, light
 - Scenario: Meeting with known and unknown people, group devices, enable data sharing functionality
- Privacy
 - Adaptable data protection mechanism depending on data sensitivity
 - Device classification based on network traffic analysis to infer whether a device is malicious or friendly



- Which other scenarios do you have in mind for automatic device grouping based on environment data?
- What means data sensitivity and how to achieve this goal?
- Is it realistic to infer whether a device is malicious or friendly via network traffic?