Securing Ownership Change of IoT Devices

Threats of Ownership Change
• IoT devices contain privacy sensitive user data.
• Change of owner → unauthorized access
• Automatic handling of ownership change mitigates the threat

Privacy Enhancement
• Verification of ownership change based on trusted device
  • Trusted device authentication using challenge response
  • Security association using Diffie–Hellman key exchange
• Data protection based on encryption.
  • Encryption: AES-CCM with 128 bit key
• Data protected under owner profiles
  • Owner profile management
• Profile retrieval based on owner authentication
  • Password based authentication
• Packet based communication protocol running on top of UDP (Wi-Fi / Bluetooth)

Our Solution: Detect & Manage Change of Ownership
• Automatic detection of ownership change
  • Leverage context to detect ownership change
  • Context = Wi-Fi SSID
• Privacy Enhancement
  • Verification of ownership change
  • Data protection
  • Owner profile + management system
  • Owner authentication & data retrieval

Previous Owner

Device

Cloud

Device Storage

New Owner

Authentication & Data Retrieval

Data Protection

Ownership Change Detection

Previous Owner

New Owner

Owner Profile Management

Control Device of Owner 3

Profile Management

Smart Home Device

Protected

Owner 1

Owner 2

Owner 3

Profile Elements

Known context list

Trusted device identity list

Salt

Profile name

Profile Elements

Known context list

Trusted device identity list

Salt

Profile name

Profile Elements

Known context list

Trusted device identity list

Salt

Profile name

Profile Elements

Known context list

Trusted device identity list

Salt

Profile name

Profile Elements

Known context list

Trusted device identity list

Salt

Profile name