Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Workshop on Privacy in Collaborative & Social Computing (PiCSoC)
Pittsburgh, PA
November 2, 2016

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu

Asma Alshehri and Ravi Sandhu
Institute for Cyber Security &
Department of Computer Science

© Ravi Sandhu
World-Leading Research with Real-World Impact!
Goals

- Develop an initial set of identity and access control models for IoT within a robust framework, which can

- Support further maturation and elaboration of this initial set.
IoT Proposed Architectures

Application Layer

Middle Layer

Object Layer
IoT Proposed Architectures

- Application Layer
- Application Layer
- Application Layer
- Application Layer
- Middle Layer
- Network Layer
- Service Layer
- Middleware Layer
- Network Layer
- Object Layer
- Object Layer
- Object Layer
- Object Layer

World-Leading Research with Real-World Impact!
IoT Proposed Architectures

- Application Layer
- Service Management Layer
- Object Abstraction Layer
- Object Layer

Application Layer
Service Composition Layer
Service Management Layer
Object Abstraction Layer
Object Layer

Application Layer
Application Layer
Cloud Computing Layer
Object Layer
Object Layer
Object Layer
Access Control Oriented Architecture for IoT (ACO-IoT)

User and Administrator Interaction

Application Layer

Cloud Services Layer

Virtual Object Layer

Object Layer

User Direct Interaction
Simple Use Case of ACO-IoT Architecture

User and Administrator Interaction

Application Layer

Policy

Cloud Services Layer

PDP

Analysis

Data Storage

Virtual Object Layer

update

update/accept

subscribe

publish

Object Layer

User Direct Interaction
Use Case Sample Enhancements

(a) one-to-one association

(b) many-to-one association

World-Leading Research with Real-World Impact!
User and Administrator Interaction

Application Layer

Cloud Services Layer

Virtual Object Layer

Object Layer

User Direct Interaction
Access Control Issues in ACO-IoT

- Communication Access Control
  - Intra-Layer
  - Cross-Layer
- Data Access Control
  - Micro Data
    - All Layers
  - Big Data
    - Cloud Services Layer

World-Leading Research with Real-World Impact!
Access Control Issues in ACO-IoT

Access Control

Communication

Data

Users

Administrators

Applications

Clouds

Virtual Objects

Objects

Sub-Data

Individual Collected Data

Accumulated Data

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Example using ABAC

Authorization Policy

Authorization_publish (vo:VO, 'update':T)
≡ Type1(vo) = 'apple switch' and Location(vo) = 'home1'

Authorization_subscribe (vo:VO, 'update':T)
≡ Type1(vo) = 'apple bulb' and Location(vo) = 'home1'

Authorization_Access (app:APP, HSC:Data)
≡ Type2(app) = 'apple switch-bulb' and Located-objects (app) = 'home1'

Analysis

app1_attributes
Type2 = 'apple switch-bulb'
Located-objects = 'home1'

HSC
Past-color = 'red'
Past-color = 'green'
Past-color = 'red'

HCC
Past-color = 'red'
Past-color = 'green'
Past-color = 'red'

VO1
Type1 = 'apple switch'
Location = 'home1'
Current-color = 'blue'
Past-color = 'red'
Future-color = null
Publish = 'update'
Subscribe = 'update/accept'

VO2
Type1 = 'apple bulb'
Location = 'home1'
Current-color = 'blue'
Past-color = 'red'
Future-color = null
Publish = 'update/accept'
Subscribe = 'update'
Integrated Access Control Models

- Attributes and Roles
  - ABAC, RBAC
- Integrated Access Control
- Relationships
  - ReBAC
- Provenance
  - PrBAC