Identity and Access Control in the Physical and Virtual Internet of Things

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Project Status Briefing
July 7, 2016

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

Motivating Premises

- Security and privacy will be adopted in IoT to the extent these
  - Provide added value
  - Are achievable at reasonable cost

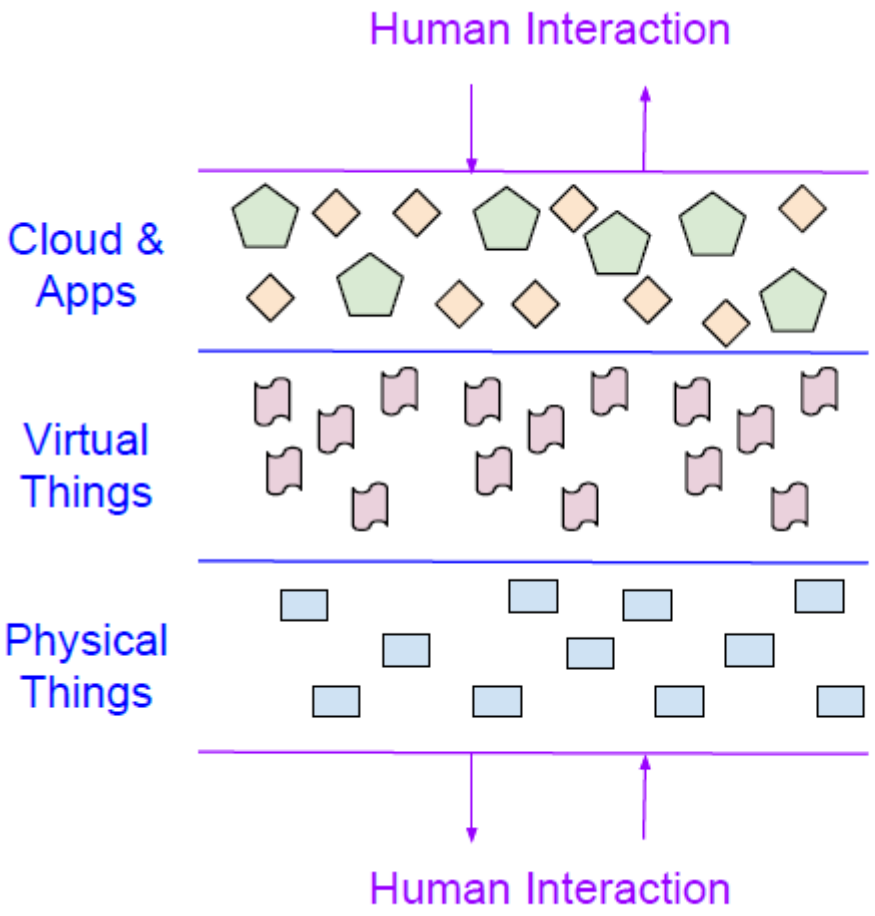
- Academic research can contribute by developing identity and access control models that resonate with industry innovators.
  - Simple to understand and deploy
  - Can accommodate complex policies when appropriate

Project 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.

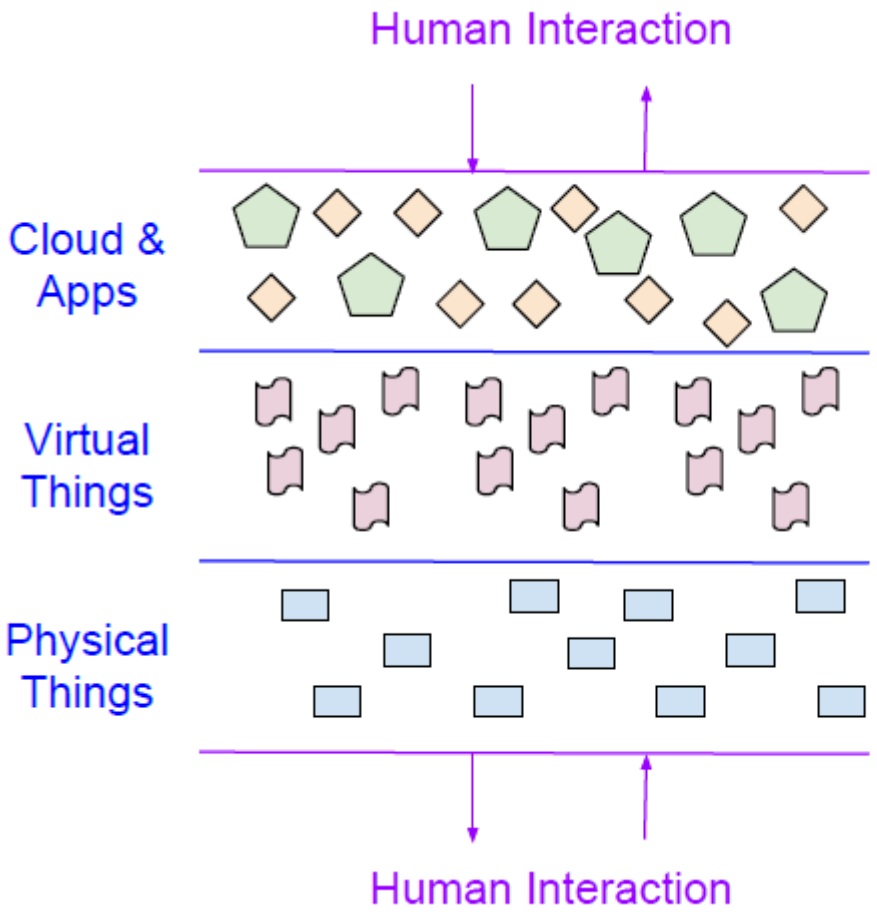
Core Technical Premises



At each layer
Models for
Communications
Administration
Access control

Across adjacent layers
Models for
Interactions
Mappings

Core Technical Premises



1-1 1-n m-1 m-n

Technical Approach

1st Generation
Identity and Access Control Models for IoT

Theories **T**	**Characteristics** **C**	**Use Cases** **U**
Authentication Authorization Trust	Application Characteristics	Concrete assumptions wrt C
DAC, MAC, RBAC, ABAC, ReBAC, PBAC …	Technology Characteristics	Sample "thought experiments"
	System Characteristics	Life-cycle critical points
Adapt & Evolve	*Abstract Models*	*Generic Requirements*

Project Deliverables

- An initial set of identity and access control models for the IoT domain encompassing physical and virtual layers
- An articulation of the three pillars of T, C and U, which underlie these models
- A statement of future R&D efforts required to take the initial set of models to maturity and deployment in practice.