Towards ABAC in Hadoop Ecosystem

Prof. Ravi Sandhu
Executive Director and Endowed Chair
Institute for Cyber Security, University of Texas at San Antonio
ravi.sandhu@utsa.edu, www.profsandhu.com

Ford EEIT & GDIA
Big Data Access Control Symposium
Dearborn, Michigan
May 2, 2017
PEI Models: 3 Layers

Security and system goals (objective policy)

Policy Models

Enforcement Models

Implementation Models

Actual Code

Necessarily Informal

Formal/quasi-formal

System block diagrams, protocol flows

Pseudo-code

© Ravi Sandhu

World-Leading Research with Real-World Impact!
PEI Models: 3 Layers

Security and system goals (objective policy)

Policy Models

Enforcement Models

Implementation Models

Actual Code

Necessarily
Informal

Formal/
quasi-formal

System block
diagrams,
protocol flows

Pseudo-
code

© Ravi Sandhu
World-Leading Research with Real-World Impact!
Multi-Layer Authorization

Data and Objects

Services

Cluster Resources and Applications
Hadoop Ecosystem Enforcement Model

Policy Manager: Apache Ranger, Apache Sentry
Gateway: Apache Knox
Ecosystem Service (ES): Apache Hive, HDFS, Apache Storm, Apache Kafka, YARN
PEI Models: 3 Layers

Security and system goals (objective policy)

Policy Models

Enforcement Models

Implementation Models

Actual Code

Necessarily
Informal

Formal/
quasi-formal

System block
diagrams,
protocol flows

Pseudo-code
**Users (U), Groups (G), Subjects (S)**

**Hadoop Services (HS):** NameNode, YARN ResourceManager

**Hadoop Service Operations (OP<sub>HS</sub>):** access / communicate

**Objects (OB):** Files and Directories in HDFS

**Operations (OP):** read, write, execute
Ecosystem Service (ES) : Hive, HDFS, Kafka, HBase
Objects (OB) : Files and Directories in HDFS; Tables, columns in Hive
Operations (OP) : read, write, execute, select, create
Tag : PII, top-secret
AC Model: Sentry View

Roles (R)

© Ravi Sandhu  World-Leading Research with Real-World Impact!
Proposed OT-RBAC Model

Object-Tagged RBAC
Adding Attributes to OT-RBAC
PEI Models: 3 Layers

1. Security and system goals (objective policy)
   - Necessarily Informal

2. Policy Models
   - Formal/quasi-formal

3. Enforcement Models
   - System block diagrams, protocol flows

4. Implementation Models
   - Pseudo-code

5. Actual Code
