Requirements for Access Control: US Healthcare Domain

Konstantin Beznosov
Baptist Health Systems of South Florida
beznosov@baptisthealth.net

Yi Deng
Florida International University
deng@cs.fiu.edu

Access Control Requirements -- Moving Target

• Existing & Upcoming Federal Regulations
  – DHHS, JCAHO, Medicare, Food and Drug Administration

• Differences from state to state

• Increased rate of merges

• Different business models
  – pay for service, Health Maintenance Organization (HMO), physician
groups, home-health, clinics, diagnosis services.
What is Needed to Get the Target?

• Decoupling application logic from authorization logic
• Centralized administration of enterprise access control mechanisms
• Expressive and flexible access control mechanisms and languages

Expressive and Flexible Mechanisms and Languages

• Support high-level domain-oriented abstraction
• Use workflow-specific factors
• Use factors specific to vertical domain
• Can easy accommodate workflow changes
Authorization Factors:
Affiliation, Role

- Affiliation factor supports
  - Frequent merges
  - Contracts between physicians and several hospitals
- Role factor provides
  - Subordination and workflow-oriented AC
  - Lower administration overhead

Authorization Factors:
Location, Time

- Location factor allows to:
  - Accommodate different physical security in different parts of hospitals
  - Have trust domains
  - Have authorization based on location units
  - Derive emergency context
- Time factor facilitates
  - AC for shift-oriented jobs
  - Team-based AC
Authorization Factors: Relationship

access control based on relationships between patients and care-givers

• Relationship types in healthcare
  – Patient’s primary, admitting, attending, referring, consulting physician and their assistants
  – Patient’s immediate family
  – Patient’s legal counsel or guardian
  – Personal pastoral care provider

Conclusions

• Healthcare access control requirements are a moving target.
• Roles are important for efficient access control administration.
• Other factors, such as patient--caregiver relationship, are essential for authorization decisions in healthcare.
• Languages and mechanisms incorporating notion of affiliation, location, time, role, relationship are needed.