Issues in Security Architecture of Computerized Patient Record

Konstantin Beznosov

May 7, 1998

Baptist Health Systems
of South Florida

BAPTIST HOSPITAL OF MIAMI • SOUTH MIAMI HOSPITAL
HOMESTEAD HOSPITAL • MARINERS HOSPITAL

We Will Discuss

- What is a CPR Enterprise
- Categories of Issues in CPR security architecture

  1. Any enterprise / Any distributed computing technology
  2. CPR enterprise / Any distributed computing technology
  3. Any enterprise / CORBA technology
  4. CPR enterprise / CORBA technology

- Goal Priorities
- Conclusions

What is CPR Enterprise

- Set of object services and clients distributed across a healthcare enterprise
- Backbone – CORBA-compliant ORBs
- First CORBA-based service – February 1998
- Next 12 months
  - Person Identification Service (PIDS)
  - PIDS and COAS-compliant Anatomy Pathology system

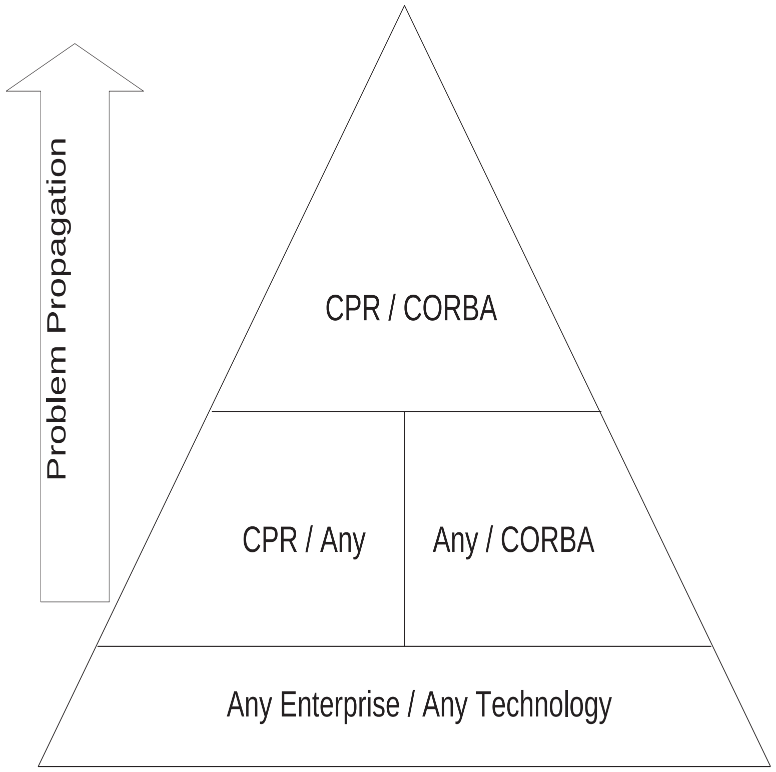
CPR Enterprise Specifics

- Many different application systems (about 200)
- Some narrow niches with few vendors
- Heterogenous environments
- Application vendors after more conservative customers
- No "borders" between staff and outside visitors
- Different levels of urgency, confidentiality and service availability
- Little to no in-house development

Security Architecture Issues: 4 groups

	Any Enterprise	CPR Enterprise
CORBA technology		
Any technology		

Security Architecture Issues: Upward Propagation



Any enterprise / Any technology

- Increasing complexity and size
- Business gets faster
- Multiple user repositories
- Coupled access logic. IDEALLY only these factors should matter:
  - User security credentials
  - Enterprise security policies
  - Business workflow constraints
- No standard administration interface ⇒ Inconsistent security models

CPR enterprise / Any distributed computing technology

- "YES/NO" access control
- Vanilla security administration
- Non-configurable authentication mechanisms

Based on CORBA technology

✔ Any Enterprise

- Heavy-weight desktop

✔ CPR enterprise

- Interoperability of security services
- “Heavy” security domains
- Coarse-grain access control

Goals and Priorities

✔ Long Term Important Goals

1. Central user security attributes repository
2. Fine grain uniform access decision model across all application services
3. Ability to “plug” various authentication mechanisms
4. Domain-specific security administration abstraction

✔ Short Term Critical Goals

1. Interoperability of CORBA Security service implementations
2. Light-weight downloadable CORBA security services

Conclusions

- Near plans
  - Central user security attributes repository
  - Access Decision Facility
  - Configurable authentication mechanisms
- Detailed discussion at http://www.bhssf.org/IT/Projects/cpr/security/architecture-issues/