

CERIAS

the center for education and research in information assurance and security

Generalized Spatio-Temporal Role Based Access Control Model

Arjmand Samuel, Arif Ghafoor and Elisa Bertino

GOALS

A spatio-temporal access control model to,
control access to secure resources based on time and location ;
exploit the semantic relationship between locations to compose rich spatial constraints; and
handle spatial hierarchy and separation of duty.

Generalized Spatio-Temporal Role Based Access Control Model (GST-RBAC):

- Extends Generalized Role-Based Access Control (GTRBAC) model in the spatial dimension
- Exploits topological relationship between locations (disjoint, meet, overlap, equal, contains, ...)
- Distinguishes between physical (symbolic or geometric) and virtual locations
- Provides formalism to compose rich spatial constraints for role enabling/disabling/(de-)activation
- Offers spatial separation of duty and role hierarchy dependent on location

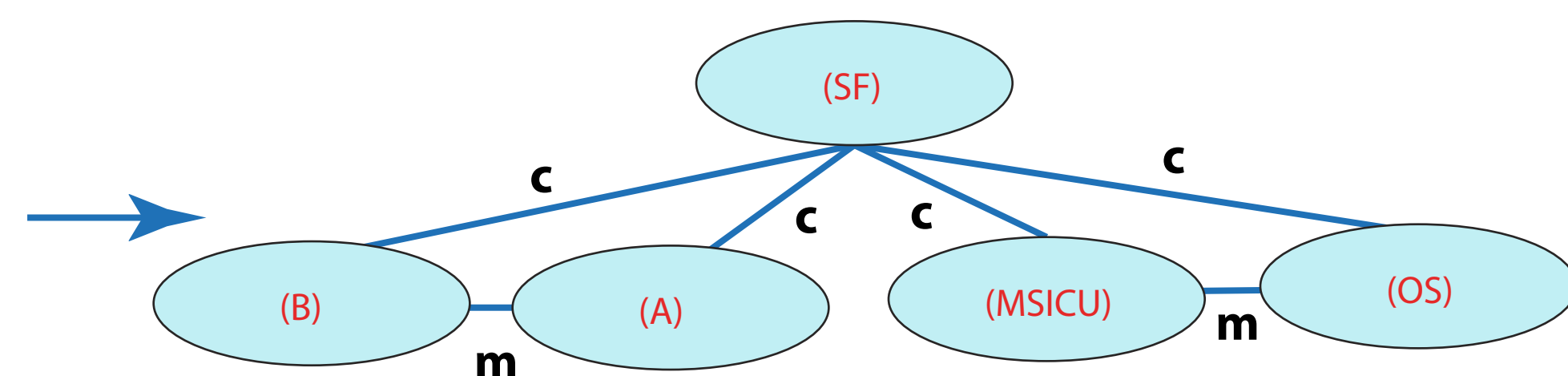
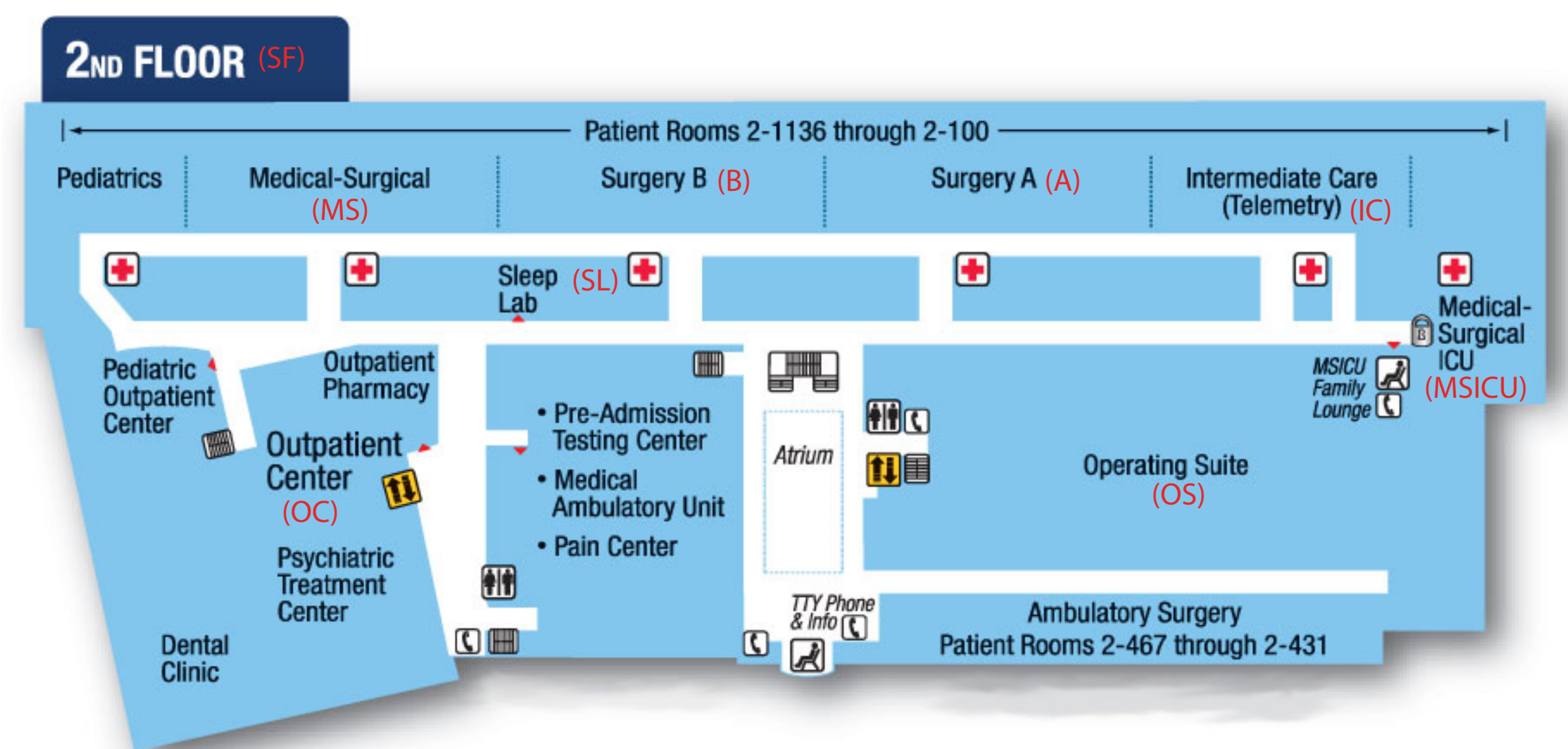
Use Case A: Electronic Health Record (EHR) element available to user Adam assuming *DaySurgeon* role and at time *DayTime* and Locations A, B, OS, MSICU of second floor (SF)

Use Case B: EHR element available to user Mark assuming *NightSurgeon* role at time *NightTime* and locations MSICU, B

Use Case C: EHR element available to user Beth assuming *SeniorNurse* role at locations MS, SL, OC, IC at all time.

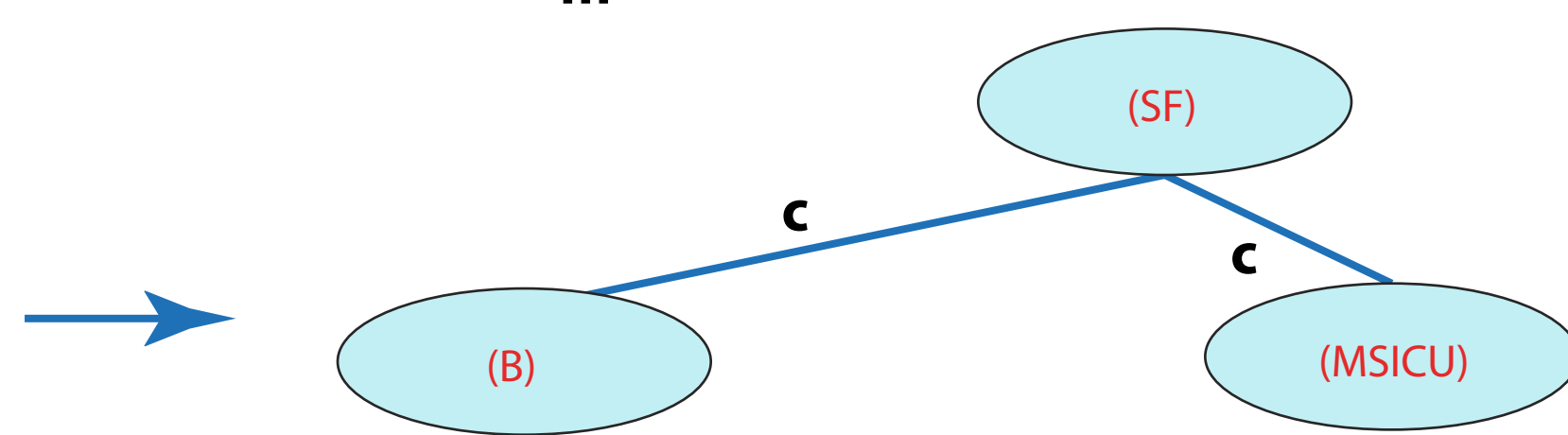
Use Case D: EHR permissions available to *SeniorNurse*, also available to *JuniorNurse* at location IC

Use Case E: No user can activate role *SeniorNurse* and *JuniorNurse* at location OC at the same time



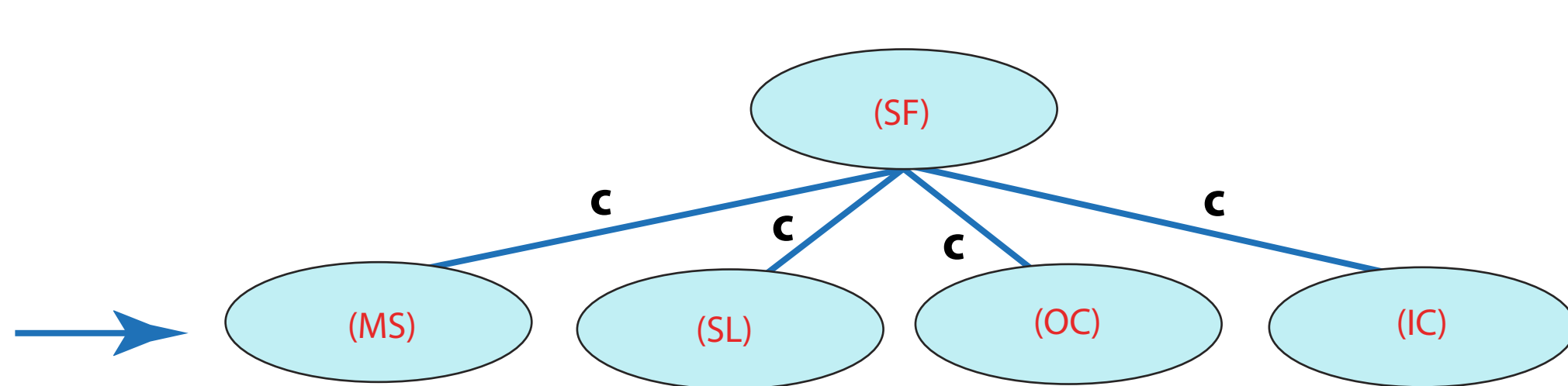
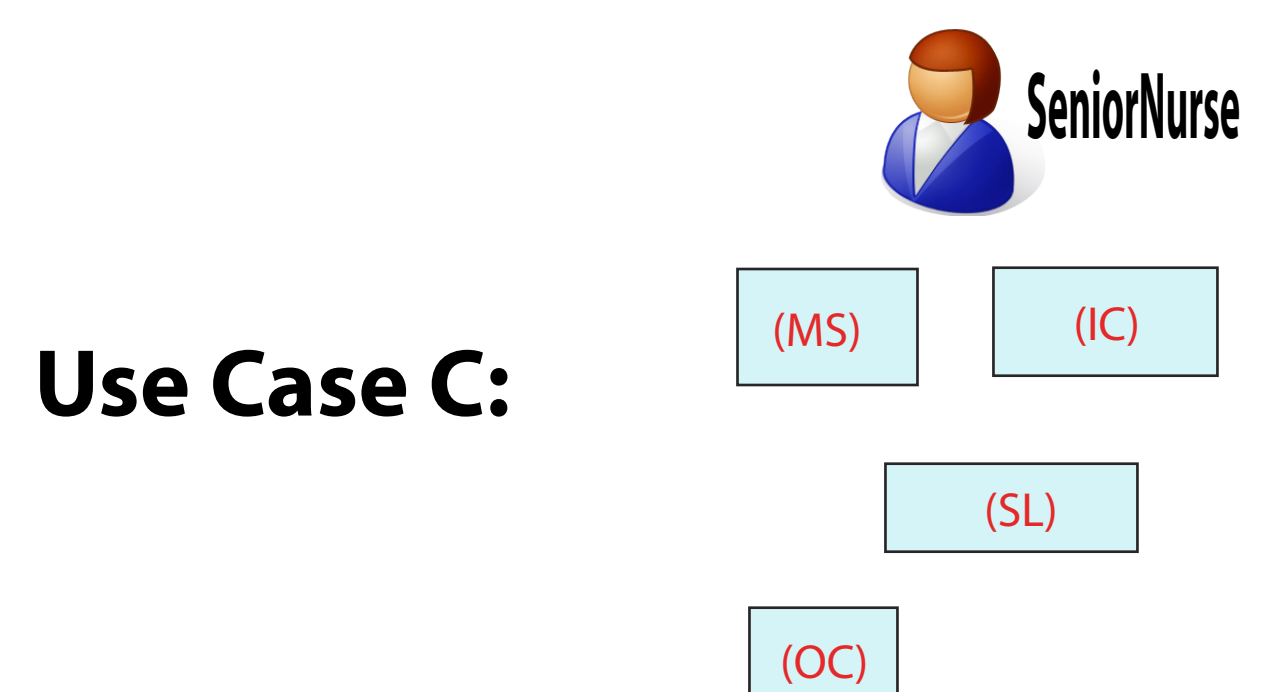
$$SpC1 = ((A \sqsubseteq (m)B) \cup (OS \sqsubseteq (m)MSICU)) \sqsubseteq (c)SF$$

(Daytime, $SpC1$, activate_r, Adam, *DaySurgeon*)



$$SpC2 = (B) \sqsubseteq (c)SF$$

(Nighttime, $SpC2$, activate_r, Mark, *NightSurgeon*)



$$SpC3 = ((MS \sqsubseteq (m)SL) \cup OC \cup IC \sqsubseteq (c)SF)$$

(All, $SpC3$, activate_r, Beth, *SeniorNurse*)



$$SeniorNurse \geq_{IC} JuniorNurse$$



$$spSoD(SeniorNurse, JuniorNurse, OC)$$