TEXAS TECH UNIVERSITY

A Semantic Model For Action-Based Adaptive Security

Sara Sartoli, Akbar S. Namin
Texas Tech University

April 2017

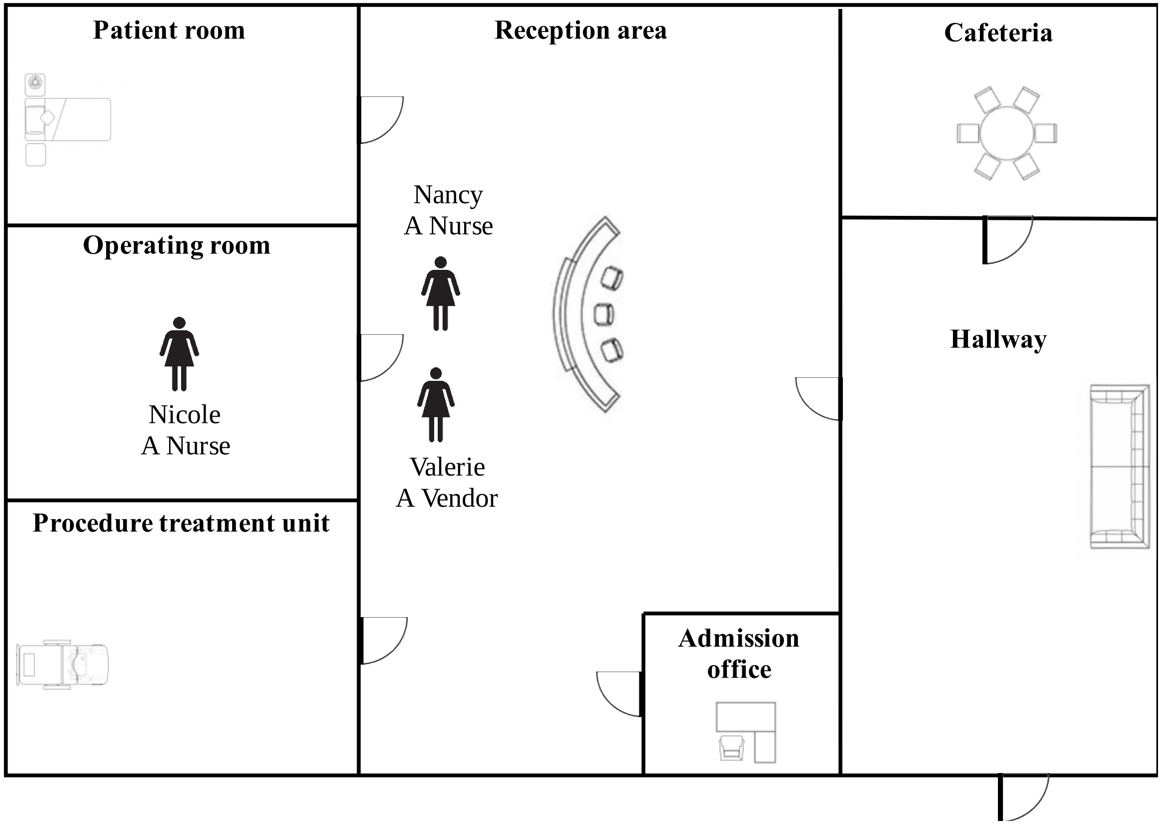
SAC 2017 MARRAKECH

Contents

- Motivation
- Introduction
- Contributions
- Why Answer Set Programming ?
- Running Example
- Security Requirements Model
- Topological Model: Structure and Evolution
- Analysis Stage
- Planning Stage
- Evaluation
- Conclusion and Future work

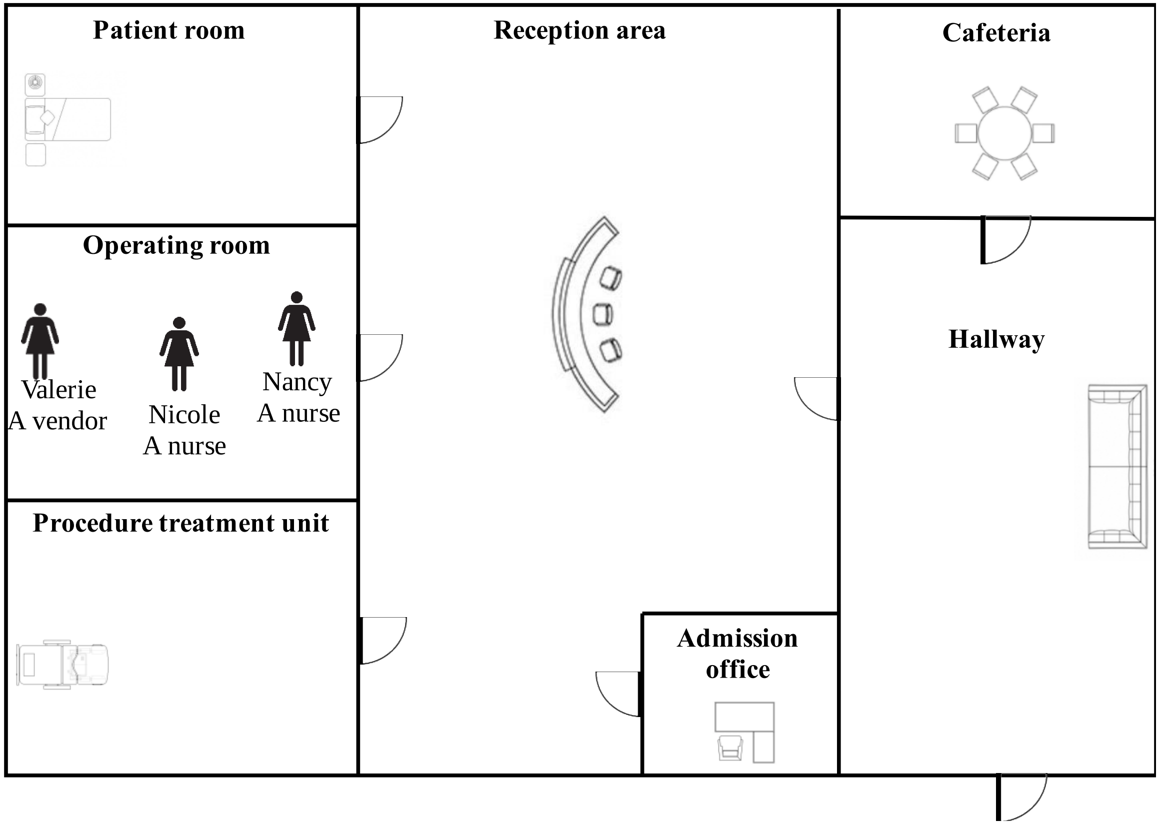
Motivation
Example 1

- Unless accompanied by a nurse, vendors are not allowed to be present in the operating room.



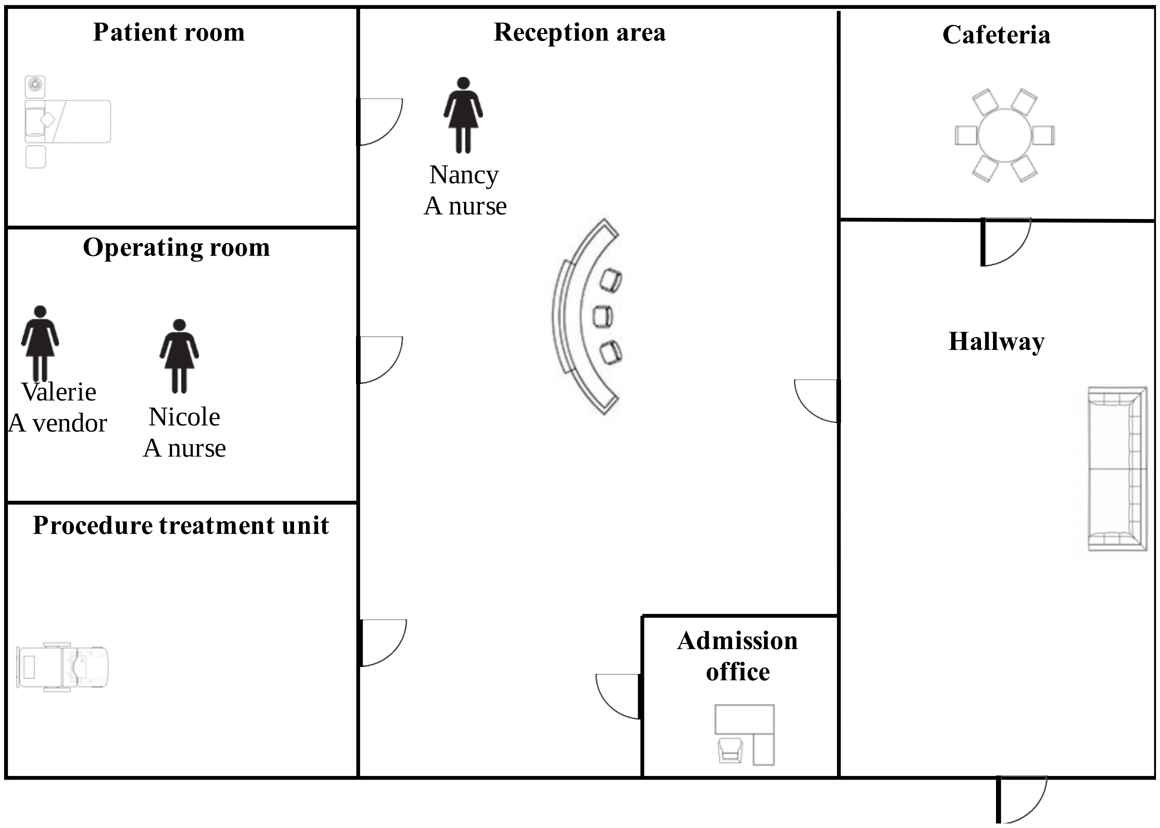
Motivation
Example 1

- Unless accompanied by a nurse, vendors are not allowed to be present in the operating room.



Motivation
Example 1

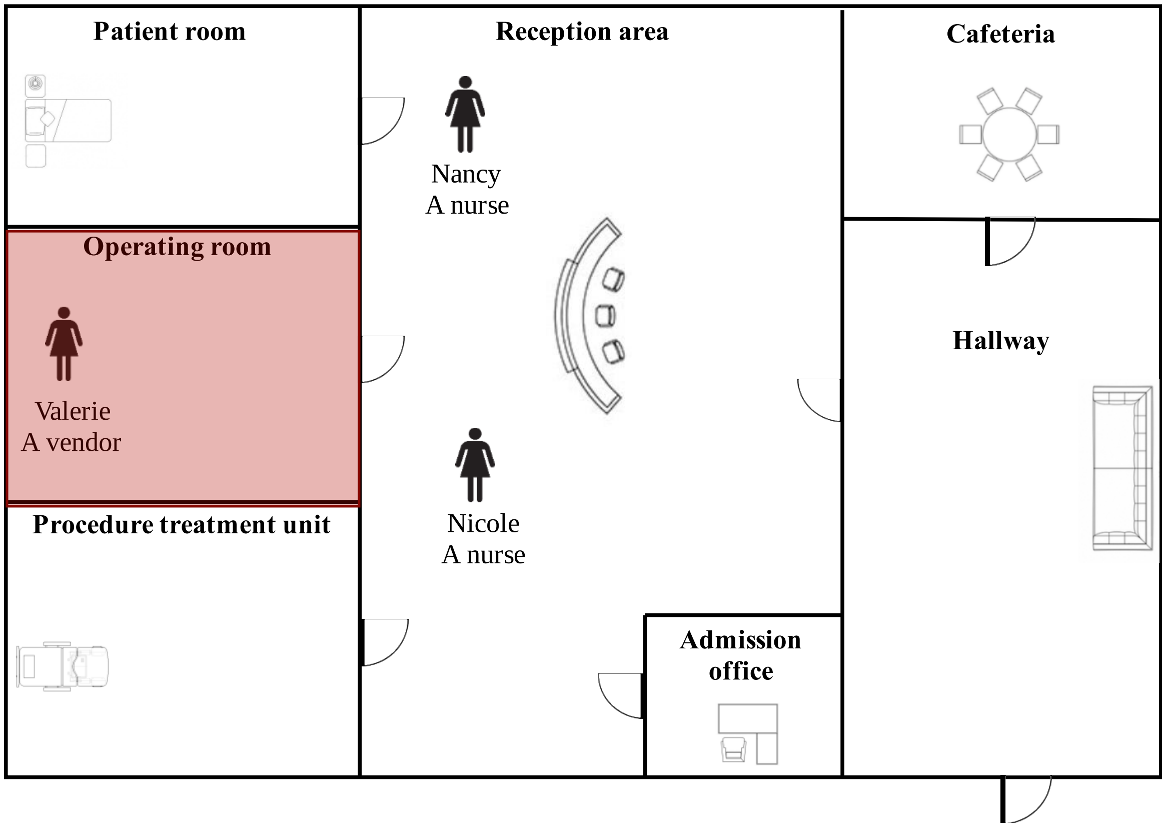
- Unless accompanied by a nurse, vendors are not allowed to be present in the operating room.



Motivation

Example 1

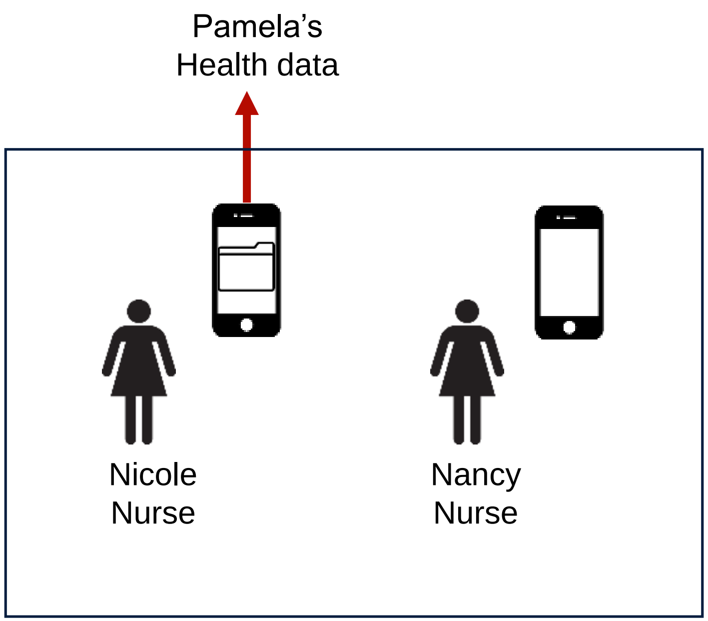
- Unless accompanied by a nurse, vendors are not allowed to be present in the operating room.



A Sequence of Permitted Actions can Cause a Violation

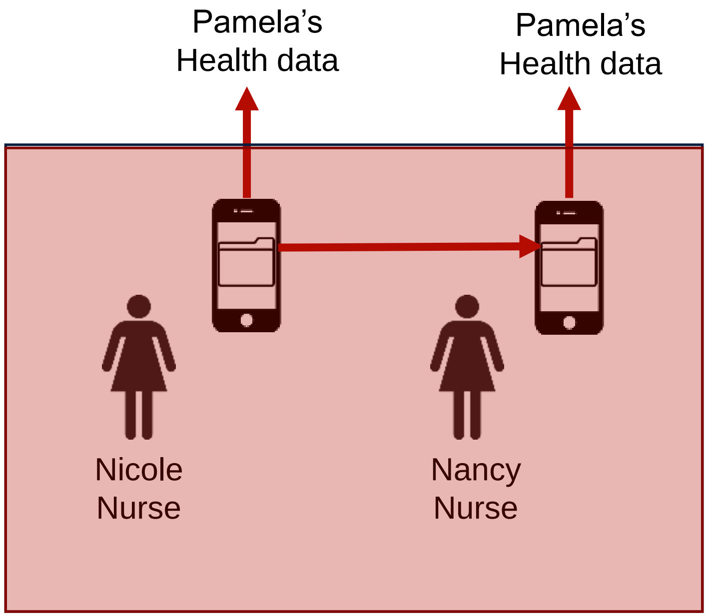
Motivation
Example 2

- Authorized employees are allowed to use their own device for accessing and storing patients' health information.
- Only authorized personnel are allowed to store patients' health information on their device.



Motivation
Example 2

- Authorized employees are allowed to use their own device for accessing and storing patients' health information.
- Only authorized personnel are allowed to store patients' health information on their device.

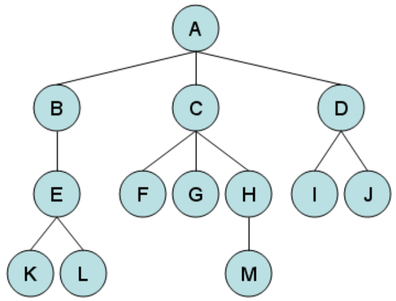


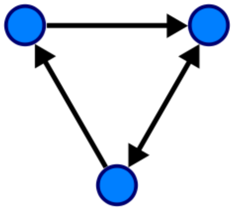
A Sequence of Permitted Actions can Cause a Violation

Introduction

Adaptive Security aims at enabling software systems to adjust their protection mechanisms in highly changing operating environments.

Topology A representation of physical or digital elements and their structural relationship such as containment and communication relationships.





Introduction
Challenging Problem and Related Work

- Runtime Verification of security requirements and enforcing action-plans to continue satisfying the requirements.

- Appropriate Formalisms are needed to represent topology and track its changes at runtime. [Pasquale, L., et al. SEAMS 2014]

- Ambient calculus-based dynamic topological model is used to support adaptive security. [Tsigkanos, C., et al. ICSE 2015]

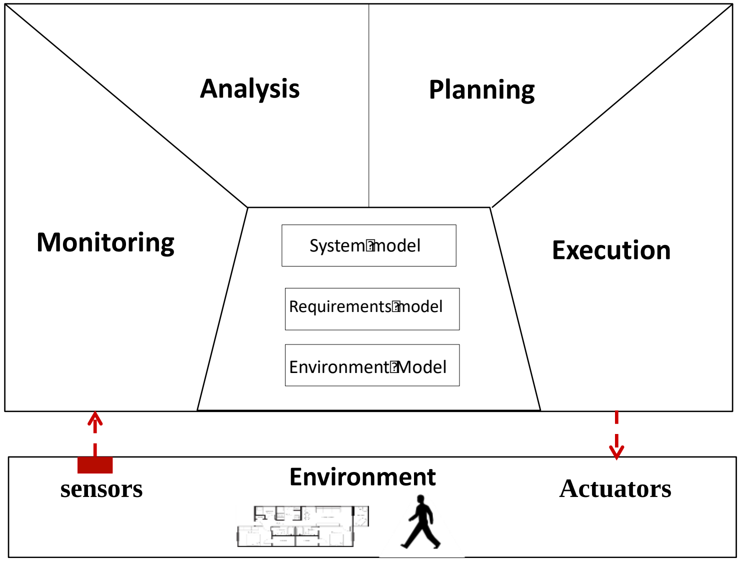
Pasquale, Liliana, et al. "Topology aware adaptive security." *Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*. ACM, 2014.

Tsigkanos, Christos, et al. "Ariadne: Topology aware adaptive security for cyber-physical systems." *Software Engineering (ICSE), 2015 IEEE/ACM 37th IEEE International Conference on*. Vol. 2. IEEE, 2015.

Reference Model

Runtime Verification Requires:

- monitoring operating environment
- maintaining knowledge about requirements, environment and system
- detecting possible violations
- determining an action-plan to mitigate possible violations



Contributions

- Present a **Answer Set Programming (ASP)** based semantic model.
  - Security Requirements
  - Environment Model, i.e. Topological structure
  - System Model, i.e. Evolution of topology
- Describe analysis activity: generating violation scenarios.
- Describe planning activity: recommending action-plans to mitigate possible violations.

Why Answer Set Programming ?

- A declarative language with roots in non-monotonic reasoning and default reasoning.
- Reasoning in uncertain situations.
- Suitable for nondeterministic, dynamic environments.

- Basic ASP rules

Negation as failure

$$a_1 \mid \ldots \mid a_n \text{ :- } b_1 , \ldots , b_i , not\ c_1 , \ldots , not\ c_j$$

Epistemic disjunction

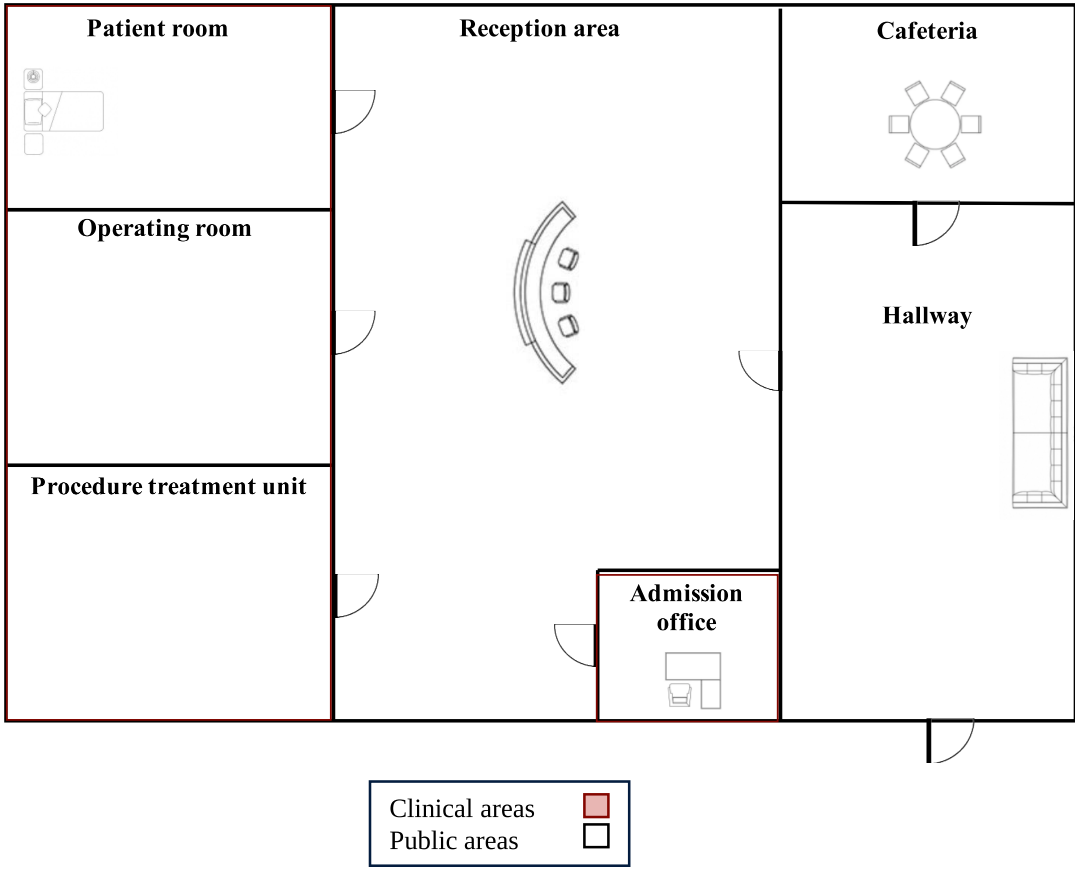
- At least one of a_is is believed if $b_1 , \ldots , b_i$ are believed whereas $c_1 , \ldots , c_j$ are not believed.

Running Example

Hypothetical Hospital

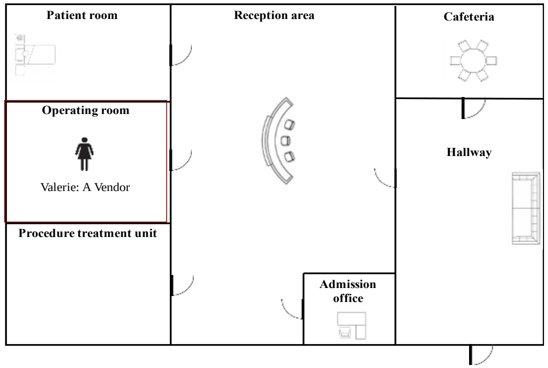
Assumptions

- Clinical areas are protected by secure doors.
- Wi-Fi Internet is provided in the clinical area.
- Employees are allowed to bring their own device.
- Employees can store encrypted data on their own device.
- Employees can transmit data to other authorized employees.

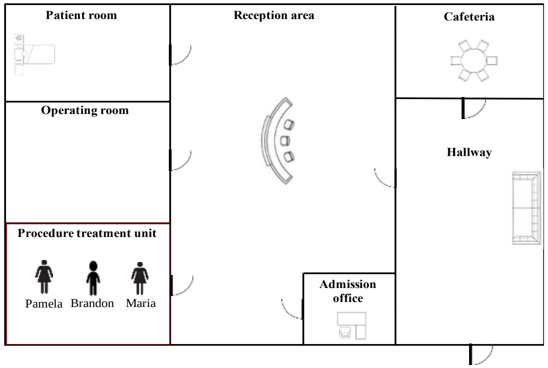


Security Requirements

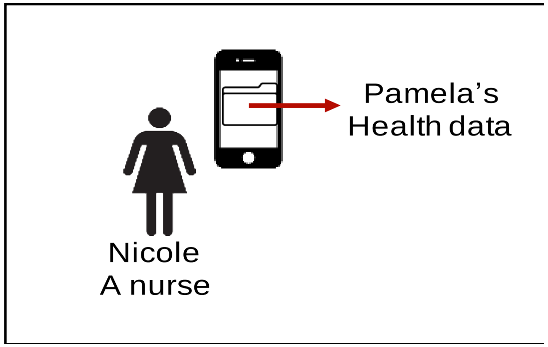
SR1. Unless accompanied by a nurse, vendors are not allowed to be present in the operating room. [OHIO State University Medical Center policy]



SR2. No more than one significant other may accompany adult patients, in procedural treatment unit. [Ronald Reagan UCLA medical center policy]



SR3. Patients' health information might only be transmitted to authorized personnel who are allowed to access the information.[University of Michigan Health system policy]

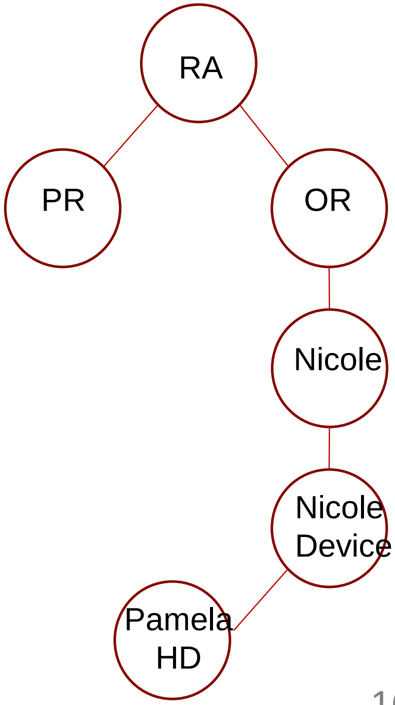


Topological Model
Environment Model

Representing Structure of Topology

- Containment hierarchy
  - Being enclosed: Nicole is in the operating room
  - Possession: Nicole has a device
  - Accessibility: Operating room(OR) and patient room(PR) are accessible from reception area(RA)
  - Storage: Pamela’s health data is stored on Nicole's device

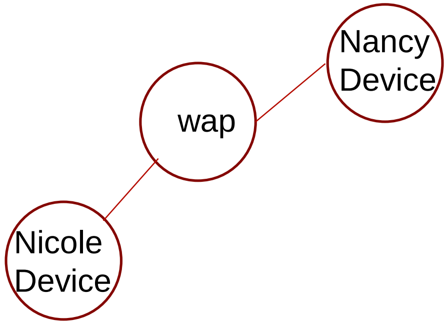
```
contains(reception_area,operating_room).
contains(reception_area,opatient_room).
contains(operating_room, nicole).
contains(nicole, nicole_device).
contains(nicol_device, Pamela_data).
```



Representing Structure of Topology

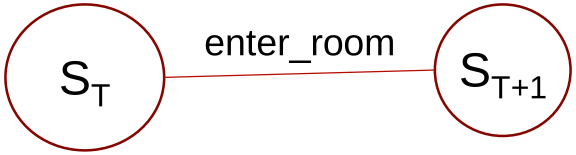
- Communication graph
  - Being connected to an access point

```
connected(nicole_device,wap).
connected(nancy_device,wap).
```



Representing Evolution of Topology

- Represents the execution path of the cyber physical system
  - State: a topological structure
  - Transition: an action exercised by an agent
  - Transition function
    - **Direct effect of actions**
    - Indirect effect of actions
    - Inertia law




```
holds(contains(Loc2, Agent), T+1) :-  occurs(enter-room(Agent, Loc2), T).
```

Topological Model
System Model

Representing Evolution of Topology

- Represents the execution path of the cyber physical system
  - State: a topological structure
  - Transition: an action exercised by an agent
  - Transition function
    - Direct effect of actions
    - **Indirect effect of actions**
    - Inertia law

```
- holds(contains(Loc1,Agent), T):- holds(contains(Loc1, Agent), T),  Loc1!= Loc2.
```

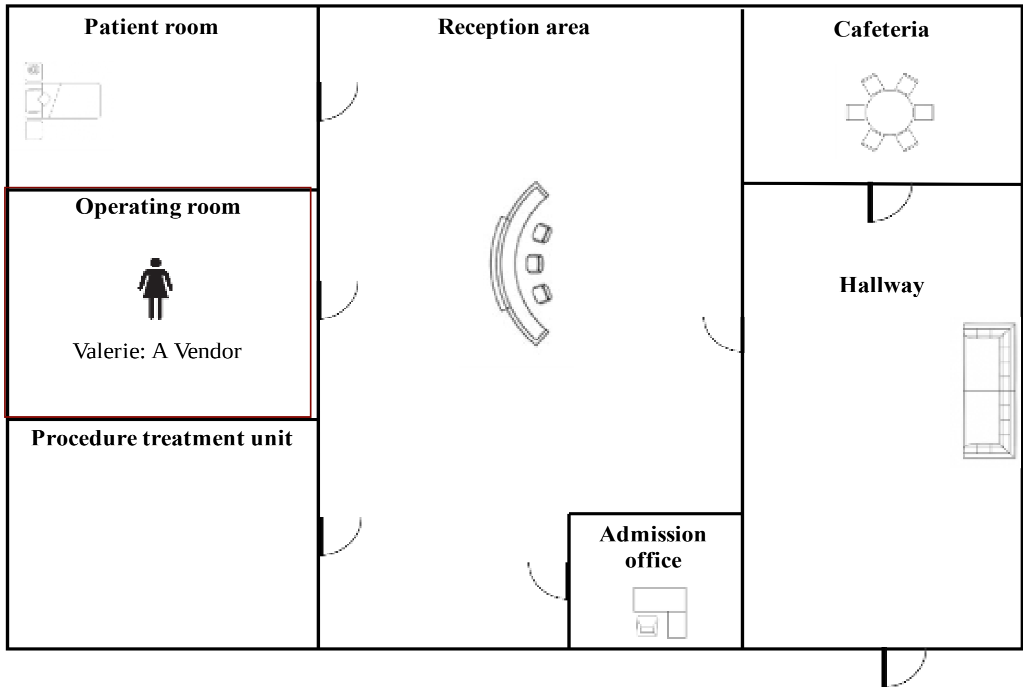
Representing Evolution of Topology

- Represents the execution path of the cyber physical system
  - State: a topological structure
  - Transition: an action exercised by an agent
  - Transition function
    - Direct effect of actions
    - Indirect effect of actions
    - **Inertia law**

```
 holds(F, T+1) :-  holds(F, T), not -holds(F, T+1).
- holds(F, T+1) :- -holds(F, T), not holds(F, T+1).
```

Requirements Model
Security Requirement 1

SR1. Unless accompanied by a nurse, vendors are not allowed to be present in the operating room.



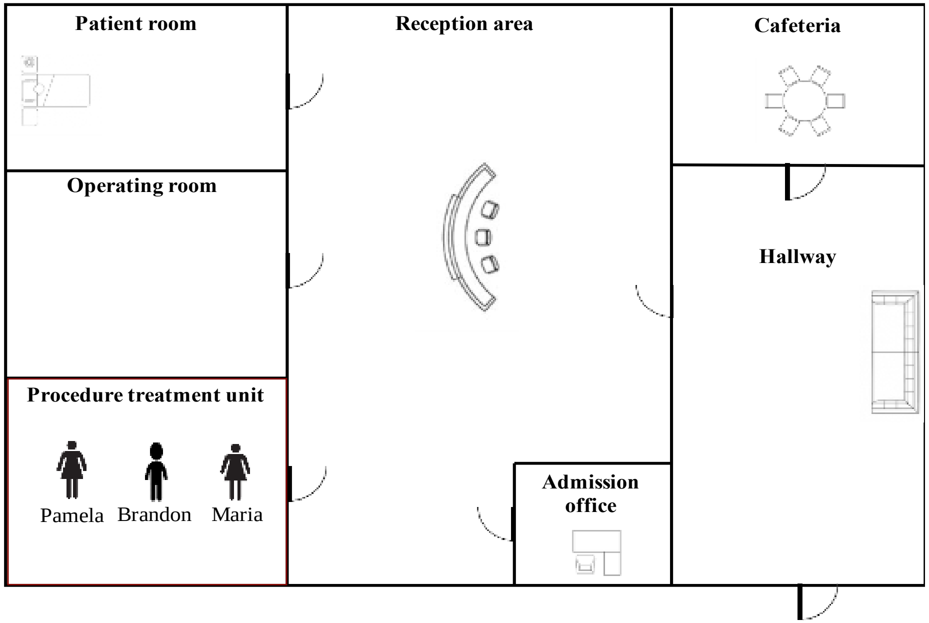
Violated(SR1, T):- not holds(accompanied(opr,valerie),T).

Holds(accompanied(opr,valerie),T) :- holds(contains(opr,valerie),T), holds(contains(opr, Agent),T).

Requirements Model

Security Requirement 2

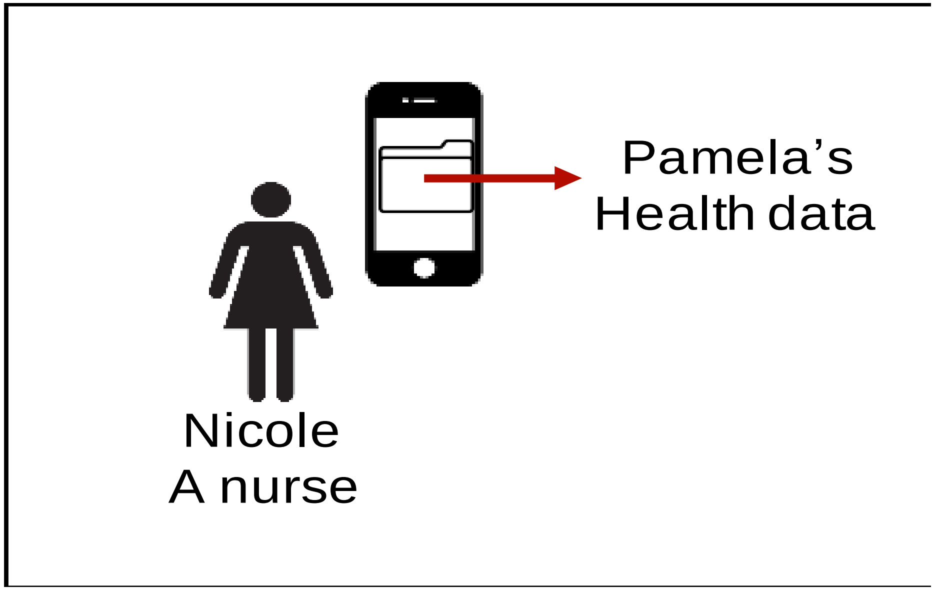
SR2. Only one significant other may accompany adult patients, in procedural treatment unit.



Violated(SR2, T):-
#count{Agent:holds(contains(ptu,Agent),T), sign_other(Agent, Patient), adult(patient)} >1.

Requirements Model
Security Requirement 3

SR3. Patients' health information might only be transmitted to authorized personnel who are allowed to access the information.



Violated(SR3, T):-
holds(accompanied(Device,Data),T),
holds(accompanied(Agent,Device),T),
unAuthorized(Agent,Data).

Analysis: generating violation scenarios

Input

a topological model(TM) and security requirements(SR)

Output

all possible violation scenarios, i.e. possible execution paths on which some security requirement is violated.

Main Idea

build an ASP program, *analysis(TM, SR)*, whose **answer sets** correspond to all possible **violation scenarios**.

analysis(TM, SR)= TM + SR + **Action Generation Module**

```
occurs(Action ,T)| -occurs(Action, T):- T < k.
:- occurs(Action1, T), occurs(Action2, T), Action1 != Action2.
:- not violated(SR, T).
```

Planning: determining an Action Plan

Input possible violation scenarios

Goal Identify Action-plans to enact an adjustment to each of possible violation scenarios by **revoking permissions** or **suggesting action**

```
revoke_permission(Action, T):-
        occurs(Action, T),
        violation(SR, T+1).
suggest(Action, T+1):-
        occurs(Action, T),
        violation(SR, T+1),
        occurs(Action2, T+1),
        not violation(SR, T+2).
```

- revoke permission to an action if the occurrence of the action causes a violation state in the next time step.
- suggests a corrective action if the occurrence of the action changes the system from a violation state to a safe one.

Evaluation

- What are the action-plans generated for each of two examples Illustrated as motivation ?

- We represent:
  - Initial structure and evolution of topology
  - Security requirements
  - Let analysis and planning activities look 2 time steps ahead

- Report action-plans generated by the proposed reasoning scheme

Evaluation Results

Case 1

- 94 answer sets are generated
- In 38 cases planning stage suggests that vendor needs to leave operating room

  i.e. suggests(*enter-room(Valerie, ra)*)
- In 28 cases planning stage suggests that Nancy enters operating room

  i.e. suggests(*enter-room(Nancy, opr)*)
- In 28 cases planning stage suggests that Nicole enters operating room,

  i.e. suggests(*enter-room(Nancy, ra)*)

Case 2

- 24 answer sets are generated
- In All 24 cases planning stage suggests prohibiting transferring data from Nicole's device to Nancy's device,

i.e. revoking *transfer(pamela-data,nicole-device,nancy-device)*

Conclusion and Future Work

- An ASP topological model, based on actions and changes, to describe structure and evolution of operating environment.
- We formulated security requirements based on the structure of operational environment.
- We proposed to use ASP-solver to detect violations proactively and suggest mitigations during analysis and planning activities.
- A case study is presented to demonstrate the feasibility of our approach.

- In future, we plan to extend our work by generating potential insider threats and determining action-plans to prevent them.

We’d Love to Hear your Feedbacks and Answer your Questions

sara.sartoli@ttu.edu