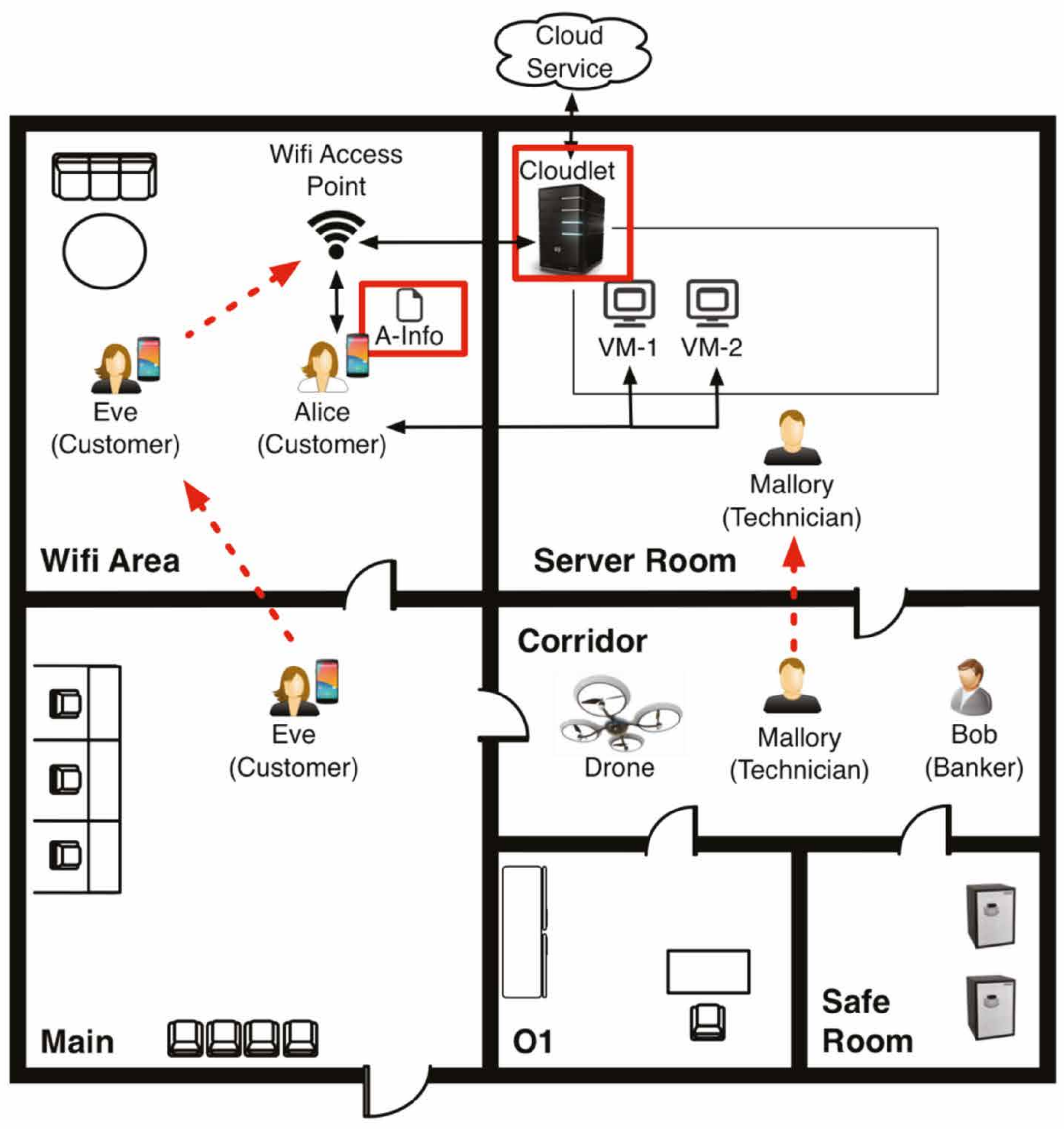
On the Interplay between Cyber and Physical Spaces for Adaptive Security

Dr. Liliana Pasquale, Supervised by: Prof. Bashar Nuseibeh

1 Motivation

Cyber-physical systems (CPS) host/manage physical and digital assets.



Physical and cyber spaces of a modern bank branch

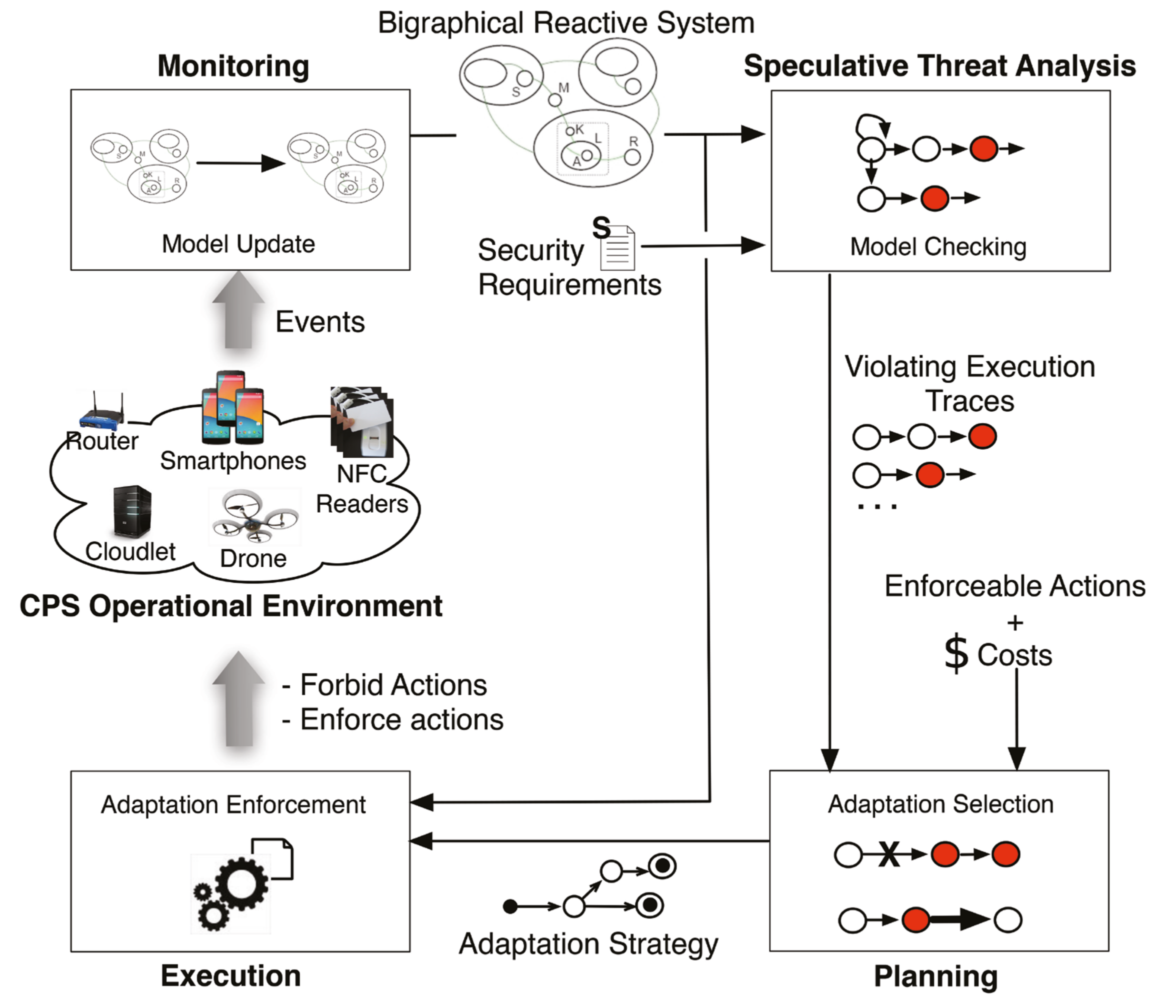
- **Cyber-enabled** and **physically-enabled** attacks exploit the interplay between cyber and physical spaces that CPS inhabit.
- **Changes** in the cyber and physical spaces can bring unforeseen threats.

2 Topology Awareness

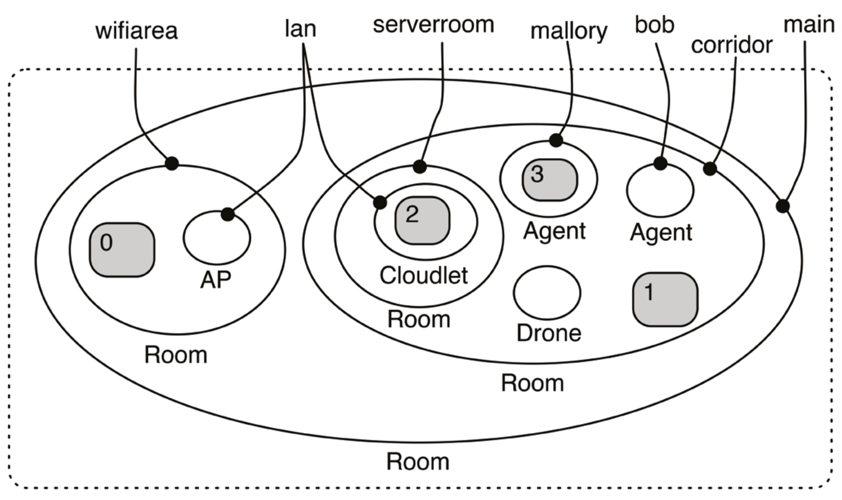
helps identify relevant security concerns

Security Concern	Topological Concept
Assets	Agent, Object
Threat	Agent
Attack	Topology Structure and Relationships
Vulnerability	Characteristic of an object or area
Security Control	Location of assets and vulnerabilities

Topology Aware Adaptive Security



3 Modeling Cyber-Physical Spaces with BRS



CPS topology

Bigraph

a. Place graph
   i. Hierachical structure (containment)

b. Link graph
   i. Communication
   ii. Identifiers

CPS Dynamics

Reaction rules

$$(Agent_n.-_0|Room_r.-_1|-_2) \longrightarrow (Room_r.(Agent_n.-_0 \mid -_1) \mid -_2)$$

Security Requirements

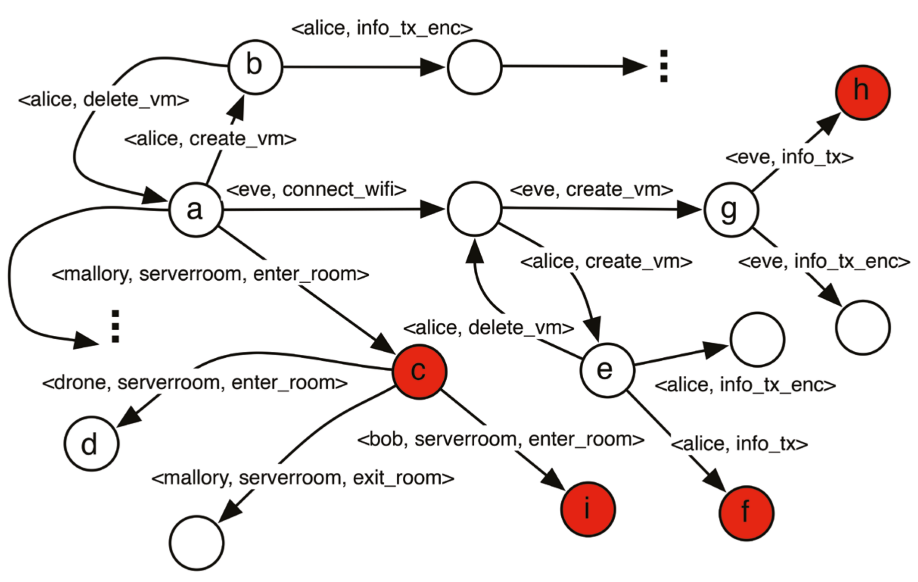
SR1: An Agent should not be colocated with the Cloudlet without the Drone performing surveillance

$$AG\neg(Room_s.(Cloudlet_{lan}.-_0 \mid Agent_m.-_1))$$

SR2: An info Token transmitted by an Agent should never be received by another Agent

$$AG\neg(Agent_n.Phone_{wifi}.(Info_y \mid -_0))$$

Speculative Threat Analysis

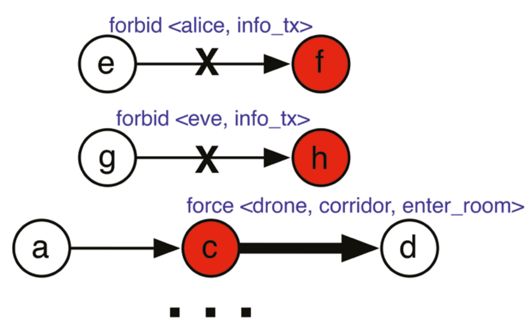


1. Interpration of a BRS over an LTS
   Future topological evolution of the cyber-physical space
2. Model Checking Security Requirements

4 Planning

Whenever an alarm state is entered, an **adaptation strategy** can:

a. **forbid** actions that would lead to a violating state;
b. **force** an action that would correspond to entering a safe state;
c. allow the environment to bring the system into a violating state and then immediately **force** actions that would bring it to a safe state.



Alarm states: e, g, a

Violating states: f, h, c

Safe states: d

Results

- BRS is a suitable formalisms to model topology of cyber-physical spaces and security properties.
- Performance degrades when the size of the model increases.

Space and Time overhead for Analysis and Planning

	#States	#Trans	Analysis Time	#VStates	Planning Time
L4	288	937	12.2 sec	115	0.3 sec
L6	786	3443	39.3 sec	221	0.8 sec
L8	1548	7909	76.1 sec	416	4.2 sec
Full	3893	25923	~5 min	1738	16.4 sec

- Small look-ahead depth → adaptation strategy re-generated frequently at runtime
- Full model → an adaptation strategy is re-generated sporadically, only when an exogeneous change takes place or at design time.

lero THE IRISH SOFTWARE RESEARCH CENTRE
Science Foundation Ireland sfi For what's next
University of Limerick Ollscoil Luimnigh
Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union European Regional Development Fund
United Technologies Research Center
SOUTHERN Regional Assembly Promoting our Region