Carlo Motta

Assessment and enforcement of resilience and security properties in control systems

Tutor: Prof. De Tommasi

co-Tutor: Prof. Santini

Cycle: XXXVI

Year:First

My background

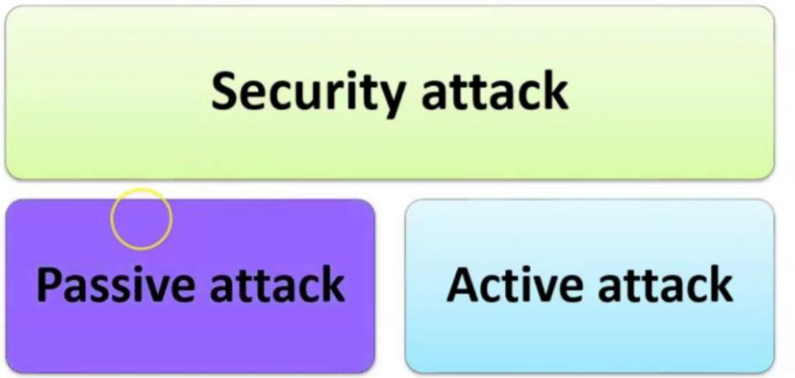
- **MSc degree in Automation Engineering, University of Naples Federico II**
- **Working team: DAiSyLab (Prof. Gianmaria De Tommasi)**
- **Co-Tutor: Prof. Stefania Santini**
- **Collaboration: UniSa (Prof. Francesco Basile); DIETI (RO group)**
- **PhD start date: Academic Year 2020-2021**
- **Scholarship type: "UNINA"**

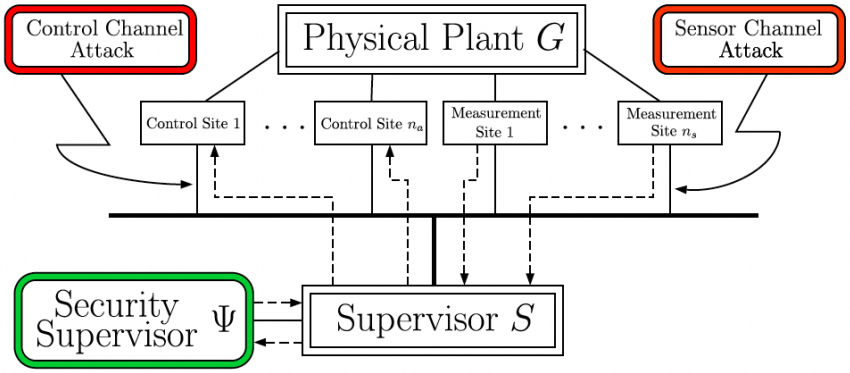
Research field of interest

- To design supervisory control systems that are resilient (robust) to (cyber-) attacks.

- Security and privacy problems can be modeled in the framework of Discrete Event Systems.

- A system can be designed to be resilient to attacks, otherwise supervisory control can be used to enforce security by restricting the closed-loop behaviour





Summary of study activities

Courses

- **Stohastic Modeling;**
- **From observability to privacy and security in discrete event systems;**
- **Scientific Programming and Visualization with Python;**

Conference

- **AIRO -** Associazione Italiana di Ricerca Operativa, University of Naples Federico II, 08-12/02/2021
  5th AIRO Young Workshop and AIRO PhD School 2021 –
  Presentation of paper: Optimization-based assessment of Initial-State Opacity in Petri Nets

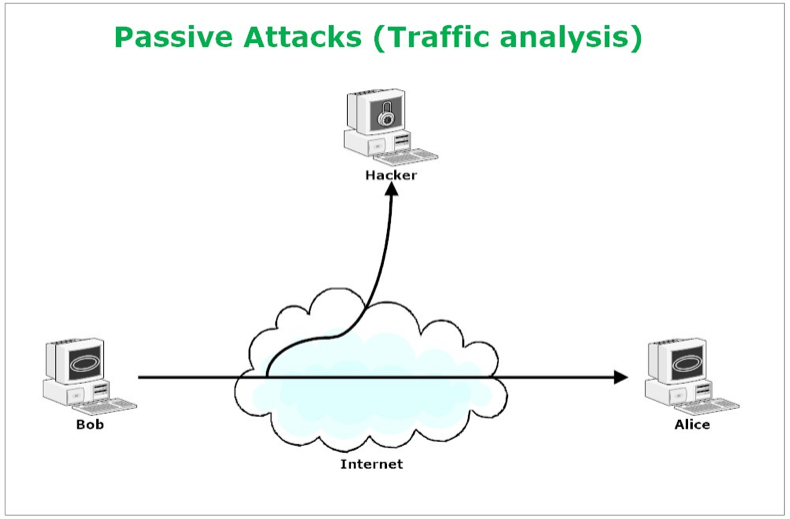
Other courses

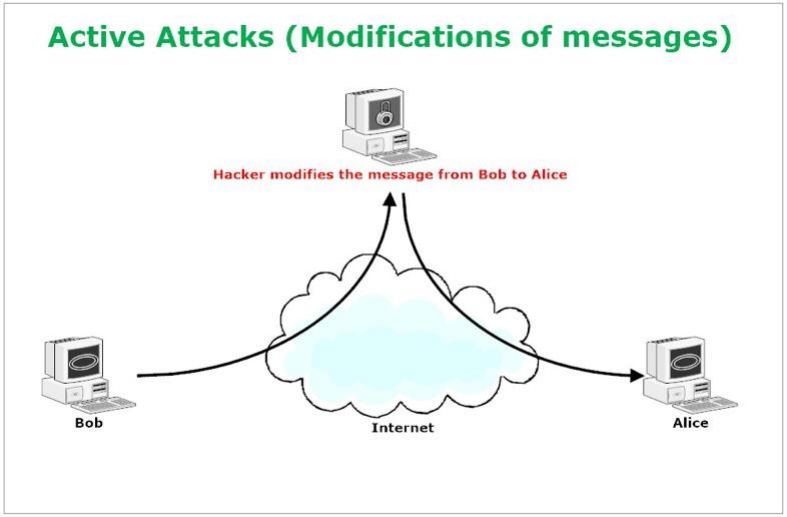
- Digital Forensics
- Corso di imprenditorialità accademica

Research activity (1/3)

- Preventing an intruder to infer a secret and interact in a malicious way with safety-critical functions.

- In a distributed control system, information leaks and deceptions represent a threat to the system itself. The attacker's goal could be either to inflict damage or to learn secrets about the system.



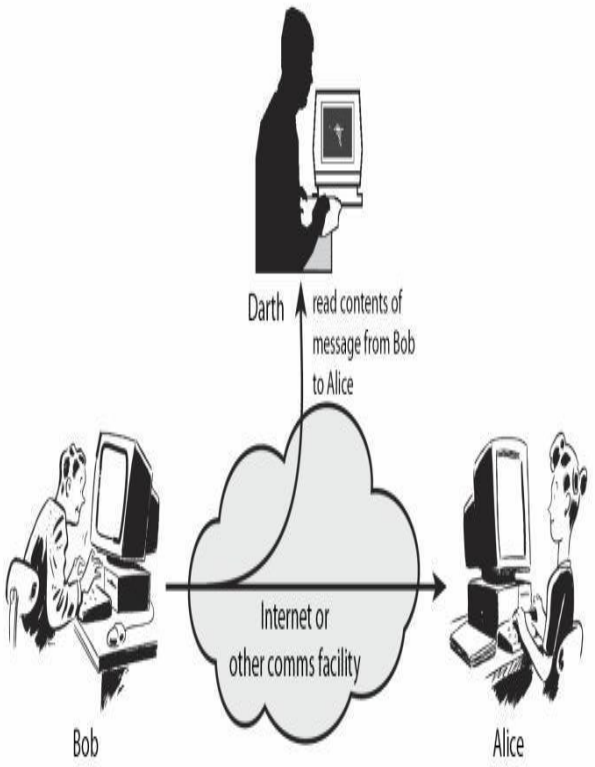


Research activity (2/3)

- Passive attacks: the system is *opaque* if a user cannot infer any secret if granted a partial observation of the system.
  - the system's initial state represents the *secret* → *Initial State Opacity (ISO)*
- Introduced a sufficient condition to conclude if a DES modeled as a Petri net (PN) is not ISO based on the solution of Integer Linear Programming (ILP).

  Accepted paper → "Optimization-based assessment of Initial-State Opacity in Petri Nets"

- This study is suited for PN models with a high level of parallelism such as control systems of industrial plants

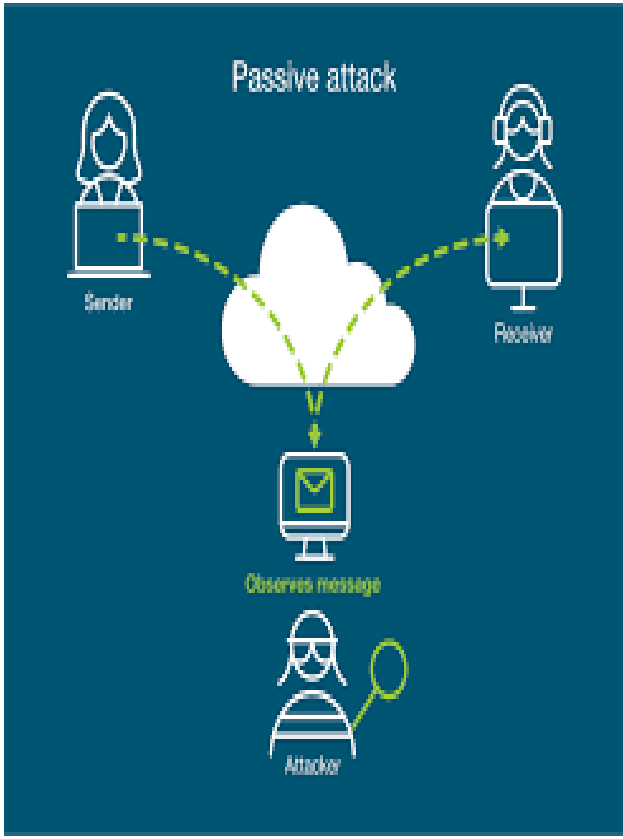


Research activity (3/3)

- Passive attacks: a system is non-interferent if there are no information leaks between different domains in the system (high- and low- level users)
  - The secret is the occurrence (*SNNI*) or the not occurrence (*BSNNI*) of an event
- Introduced necessary and sufficient conditions to conclude if a DES modeled as a PN system is non-interferent

  Submitted journal paper → "An optimization-based approach to assess non-interference in labeled and bounded Petri net systems"

- This study is suited for PN models with a high level of parallelism such as control systems of industrial plants



Products

[P1]	Gianmaria De Tommasi; Carlo Motta; Alberto Petrillo; Stefania Santini *AIRO Springer Series* Optimization-based assessment of Initial-State Opacity in Petri Nets

Next year

- Active attack: The attacker's goal is to inflict damage on the system by counterfeiting the information exchanged between the actors.
  - Case study: in automated highway system we considered multiple platoons interacting to synchronize their movements and modeled an attacker trying to make them reach an unsafe state
- Review of literature about supervisory control resilient wrt attive attacks with automata
- Extension to the PN modeling framework to avoid explicit state space representation