Dynamic System Modeling for Threat Analysis

Tithnara N. SUN, Ciprian TEODOROV, Joël CHAMPEAU & Philippe DHAUSSY
ENSTA Bretagne, 2018
tithnara.sun@ensta-bretagne.org, ciprian.teodorov@ensta-bretagne.fr,
joel.champeau@ensta-bretagne.fr, philippe.dhaussy@ensta-bretagne.fr

Threat-Driven Cyber Security

Define the **scope** of the analysis. Exhibit the system, **attack surface** and critical resources.

Gather **information** relevant for the defined scope.

Correlate the gathered pieces of information to **identify** the **threats**, **vulnerabilities** and potential **attacks**.

Make **intelligence - driven decisions** and take **action** against threats.

Dynamic Attack-Defense Model

How to model and build a **dynamic simulation** of a **running system** in a **cyber security** context *i.e.* in an environment where **threat actors** evolve ?

Attack Surface Reification

Concepts identification and description. Relevant **structures** and **abstractions** choices.

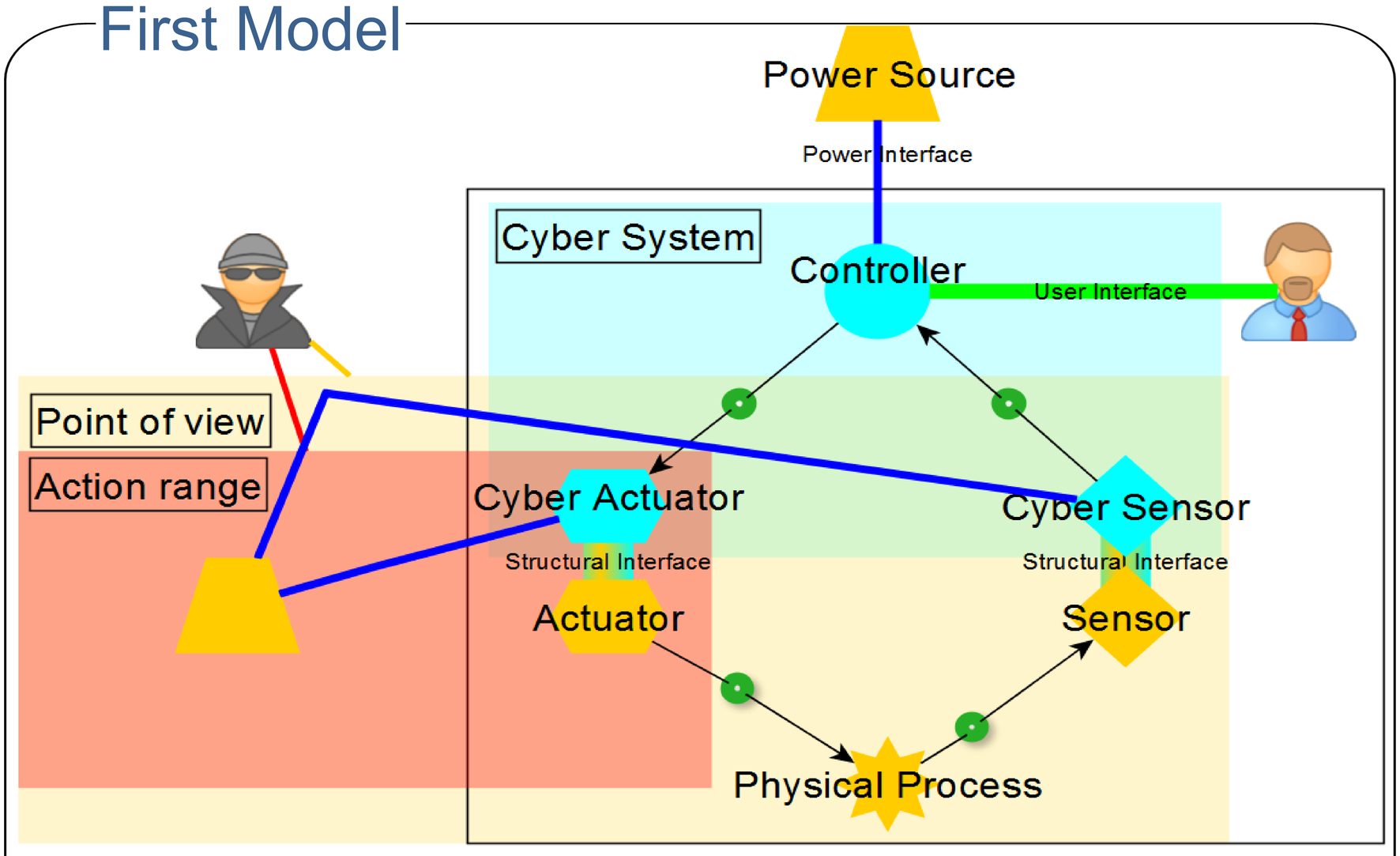
Dynamic Model

Lifecycle of the system. **Temporal** dimension, **interactive** system and evolving **attackers** and **defenders**.

Implementation & Simulation

Runnable and non-cyber-agent-**user-friendly** simulation. **Compatibility** with other security **tools**.

First Model



Cyber Physical System: Group of **interacting entities**. **Target** of the attackers. Definition in an **environment**.

Actor: **Attacker** or **defender** of the system. Interactions with the system through an evolving **point of view** and **action range**.

Actions: Available **evolution** attempts of an actor's interactions with the system. (modification, insertion, deletion)

Research Directions

Cyber Threat Intelligence
Cyber-related vocabulary

Operational Design
Military operation planning

Embedded Systems
Cyber physical system modeling

Attack Trees
Step-by-step attack modeling

Model-Checking
Formal verification method

Game Theory
Multiplayer scenarii modeling

Temporal Graphs
Evolving data structure

Automata
Conditional state-machines

Composite Structure
Both textual and graphical

[Bar14] Sean Barnum. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* MITRE, 2014.
[FB15] Jon Friedman and Mark Bouchard. *Definitive Guide™ to Cyber Threat Intelligence.* CyberEdge Group, LLC, 2015.
[KLP15] Christopher Kiekintveld, Viliam Lisý, and Radek Píbil. *Game-theoretic foundations for the strategic use of honeypots in network security.* In Cyber Warfare, 2015.
[KPCS14] Barbara Kordy, Ludovic Piètre-Cambacédès, and Patrick Schweitzer. *DAG-based attack and defense modeling: Don't miss the forest for the attack trees.* Computer science review, 13:1–38, 2014.
[Sch99] Fred B. Schneider. *Trust in cyberspace.* Technical report, Committee on Information Systems Trustworthiness, 1999.