



# On Attacker Models and Profiles for Cyber-Physical Systems

---

MARCO ROCCHETTO and Nils Ole Tippenhauer

Singapore University of Technology and Design

## CPS

- systems that consist of networked embedded systems, which are used to **sense, actuate, and control physical processes**.
- Examples: industrial water treatment facilities, electrical power plants, public transportation infrastructure, or even smart cars.

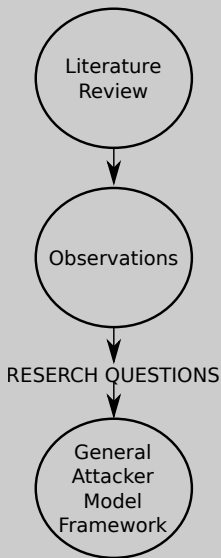


- researchers from different fields -> different ideas of attackers
- no established terminology or attacker model
- we need a uniting set of models, a common language covering not only Cyber attacks, but physical attacks as well
- what can attackers do? What motivates them? What will be the impact?



- Define and apply a **taxonomy** of 10 different features to classify and compare attacker models
- We provide an **overview** of work discussing **terminology**, **attacks** and **attackers** on CPS
- We propose an **attacker framework** and a more formal and standardized definition of attacker model for CPS
- Using that framework, we extract **attacker profiles** from related work, analyze those profiles, and propose six attacker profile archetypes that distill common intuition behind related work

```
Terminal - x@y: ~/repos/espire/attackerModelTool
File Edit View Terminal Tabs Help
1.Attacker Model (Dimensions & Metrics)
2.Load Attacker Models and Frameworks
3.Existing Attacker Models (29)
4.LaTeX tables
5.New attacker model
6.Modify attacker model
7.Create New Framework
8.Existing Frameworks (19)
9.Clustering
10.WEKA input
11.Diff profiles
12.Quit
```





## Attacker Profile

**generic** description of the **setting and intuition**, and not an exhaustive listing of possible actions, motivations, or capabilities of the attacker

## Attacker Model

- define **constraints for the attacker** (e.g. finite computational resources, no access to shared keys)
- fully characterize the possible **interactions** between the attacker and the system under attack

## Attack Model

- one can consider an attack model as an **instantiation of the attacker model** on a specific system configuration
- interactions between the attacker and a **specific configuration** of the **system under attack + goals**



- 1 If different attacker **profiles** are discussed, and how many
- 2 The **dimensions** used by authors to define the attacker
- 3 The number of **actions** types available to the attacker
- 4 Use of a **system model** (or constraints on the type of system)
- 5 **Validation** of attack(er) models
- 6 **Generality** of model (specific for one CPS or general)
- 7 Supporting **case studies** (and if they are ad-hoc, real)
- 8 Whether the authors considered **time** in their models
- 9 **Terminology** used by authors and how it fits to **our terminology**
- 10 The main **research goal** of the reviewed work



Publication	#Profiles	#Dimensions	#Actions	System Modeling	Validation	Generic/Specific	#Test Cases	Time	Terminology used	Our terminology	Research Goal
Amin et al. [2]	1	2	1	○	○	S	1	●	AtkM	AtkM	Threat Assessment
Esfahani et al. [12]	0	0	0	●	●	S	1	●	SM	SM	Risk Analysis
Krotofil et al. [17]	0	1	1	○	○	S	1	●	AdM	AtM	Security Analysis
Lin et al. [19]	0	1	1	●	●	S	1	●	TM	AtM	Attack Simulation
Liu et al. [20]	0	3	1	●	●	S	2	●	SM	SM	Attack Simulation
Taormina et al. [33]	0	2	1	●	●	S	1	●	AtM	AtM	Attack Simulation
Urbina et al. [36]	1	4	1	○	○	S	1	●	AtM	AtkM	Testing
Adepu et al. [1]	0	1	1	●	○	S	1	○	AtM	AtM	Security Analysis
Cardenas et al. [5]	4	2	1	○	○	G	0	●	AdM	AtP	Overview
Cardenas et al. [7]	2	4	1	○	○	G	0	●	TM	AtM	Risk Analysis
Corman et al. [9]	4	4	0	○	○	G	0	○	Ad	AtP	Risk Analysis
Heckman [15]	9	5	0	○	○	G	1	○	TM	AtP	Risk Analysis
Basin et al. [4]	0	2	2	●	○	G	4	●	IM	AtM	Security Analysis
Le May et al. [18]	4	8	0	●	●	G	2	●	AdP	AtM	Risk Analysis
McEvoy et al. [22]	0	2	3	●	●	G	1	○	Ad	AtM	Intrusion Detection
Mo et al. [24]	0	0	8	●	○	G	0	●	AtM	AtM	Survey
Orojloo et al. [25]	0	5	0	●	○	G	1	●	SM	SM	Quantitative Evaluation
Teixeira et al. [34]	0	4	0	●	○	G	1	●	AdM	AtM	Security Analysis
Vigo [37]	0	2	5	●	○	G	0	○	AtM	AtM	Definition

● = argument discussed, ○ = not discussed, At=Attacker, I=Intruder, Ad=Adversary, T=Threat, S=System, Atk=Attack, M=Model, P=Profile





- >30% explicitly use different **attacker profiles**
- >30% explicitly use 17 different **dimensions**
- 2 works defines a **system model** and perform risk analysis without attacker model
- ~100% use **actions** to characterize the attacker
- ~100% use actions similar to the **usual cyber-attackers**
- ~100% attacker is **NOT identified with the network** (precise location in the network)

## Take-home messages

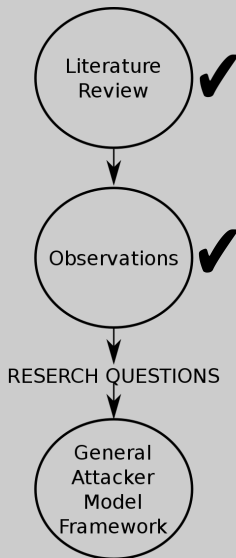
- trend of defining an attacker model (for CPS security analysis)
- various way to model the attacker, 2 main categories:
  - 1 use different **attacker profiles** with different properties (e.g., to distinguish between insider and a nation-state attackers)
  - 2 define a set of dimensions, e.g., knowledge, to define one specific **attacker model**.



- ~50% define how to create a **model of a CPS**, but
- ~25% **validate** the model against an attacker model
- ~30% use more than **1 test case** (~25% **no** test case)
- >70% consider **time**
- NO common terminology

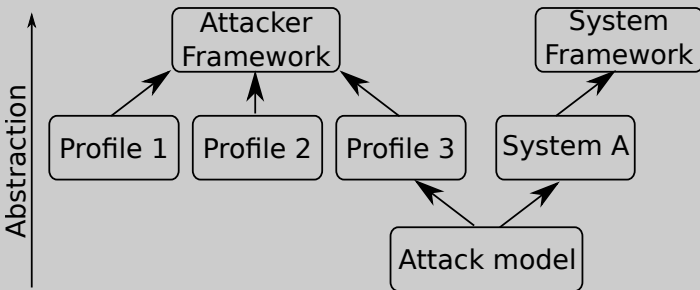
## Take-home messages

- an attack has to be **carefully timed** to go through defense mechanisms.
- techniques proposed are quite **specific**.





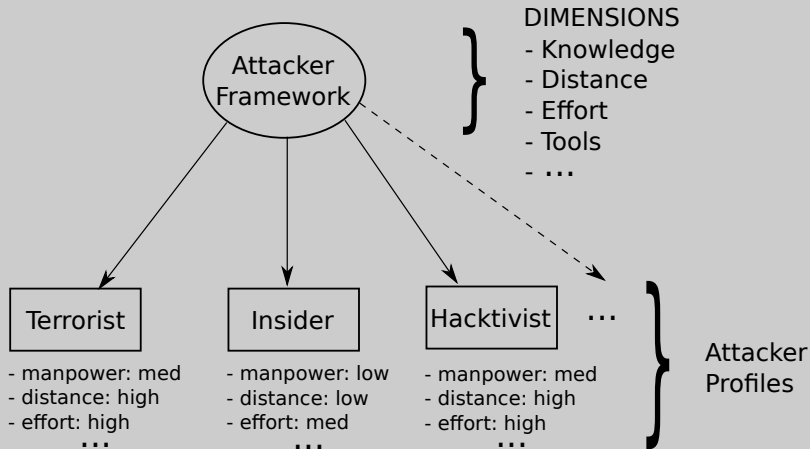
- 1 Is there a way to define **one general attacker model** for CPS?
- 2 Which is the **best way** to define an attacker model for CPS?
- 3 Are **CPS too heterogeneous** for one general attacker model?



## Attacker Framework

- set of **structured dimensions** which quantitatively represent a characteristic of an attacker
- a **metric** is associated to each dimensions
- when the dimensions are instantiated, the framework produces an **attacker profile**

# Attacker Framework



## Dimensions

Quantitative description of different aspects of an attacker

### Knowledge

- Offensive
  - ▶ Physical
  - ▶ Network
  - ▶ Software
- System
  - ▶ Source Code
  - ▶ Protocols
  - ▶ Credentials

### Resources

- Distance
- Manpower
- Effort
- Tools
- Financial Support

### Psychology

- Honesty
- Periodicity
- Camouflage
- Aim-Physical (CIA)
- Aim-Virtual (CIA)
- Determination
- Strategy

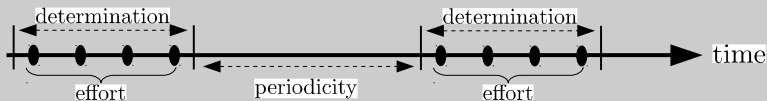


Table 3: Categorization of attacker profiles found in the related work

Dimensions	Cardenas [5] Cybercriminal	Cardenas [5] Insider	Cardenas [5] NationState	Cardenas [5] Terrorist	Corman [9] Adaptive/persistent	Corman [9] Hacktivist	Corman [9] OrganizedCrime	Corman [9] Shill	Heckman [15] Hacktivist	Heckman [15] Hobbyist	Heckman [15] Insider	Heckman [15] NationState	Heckman [15] OrganizedCrime	Heckman [15] ScriptKiddie	Heckman [15] StructuredHacker	Heckman [15] Terrorist	Heckman [15] UnstructuredHacker	Le May [18] DisgruntledEmployee	Le May [18] LoneHacker	Le May [18] NationState	Le May [18] System-Administrator	Le May [18] Terrorist	Urbina [36] Insider
Knowledge	●																						
Offensive																							
Physical																							
Network																							
Software																							
System	●																						
Source code																							
Protocols																							
Credentials	●																						
Resources	○	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Distance	●																						
Manpower					●																		
Effort																							
Tools					●	●	○	○															
Financial support	○								●														
Psychology	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Honesty	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Periodicity	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Camouflage																							
Aim-Physical					●																		
Integrity																							
Confidentiality																							
Availability					●																		
Determination									●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Strategy	●																						
Aim-Virtual	●	○	○	○	○	○	○	○															
Integrity																							
Confidentiality																							
Availability	●	●	○	○	○	○	○	○															

A metric on each dimensions is expressed on the (strict) partially ordered set  $\{○ < ○ < ●\}$

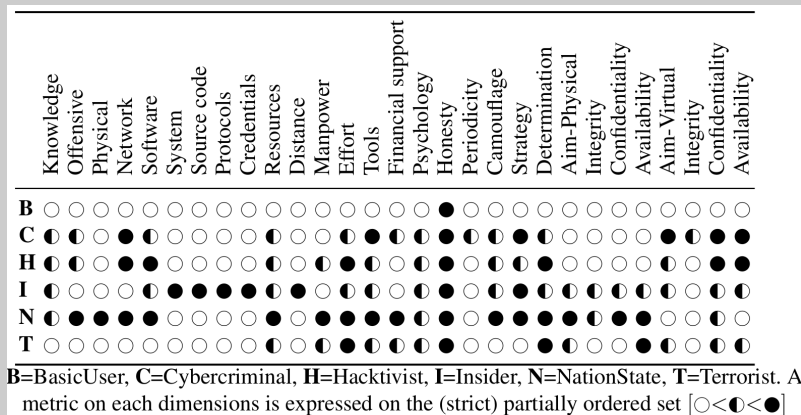




## Definition of Archetypes

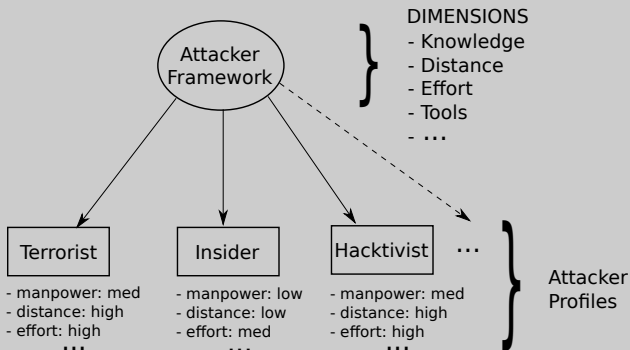
- 1 mapping of all proposed profiles into our framework
  - 2 adjusting distances (Euclidean) wrt to archetypes
- 
- 1 **Basic user.**
    - ▶ unstructured hackers (aka script kiddies)
  - 2 **Insider.**
    - ▶ disgruntled employees or a social engineering victims
  - 3 **Hacktivist.**
    - ▶ hacker + activist (to promote political agenda)
  - 4 **Terrorist.**
    - ▶ politically motivated attacker (disruption or widespread fear)
  - 5 **Cybercriminal.**
    - ▶ Hacker - extensive security knowledge and skills
  - 6 **Nation-State.**
    - ▶ An attacker sponsored by a nation/state

# Attacker Profiles (Dimension instantiation)



**21/23 cases perfect match** with the literature

- related work is based on implicit profiles
- profiles closely approximate the common intuitions
- our results link the related work and pave the way for extensions



- **taxonomy** to classify and compare attacker models
- **overview** of related work
- **attacker model framework**
- **attacker profile** archetypes
- **next steps:** @ICFEM 2016