Modelling Human Threats in Socio-Technical Systems

Rosario Giustolisi

Joint work with Giampaolo Bella and Carsten Schuermann

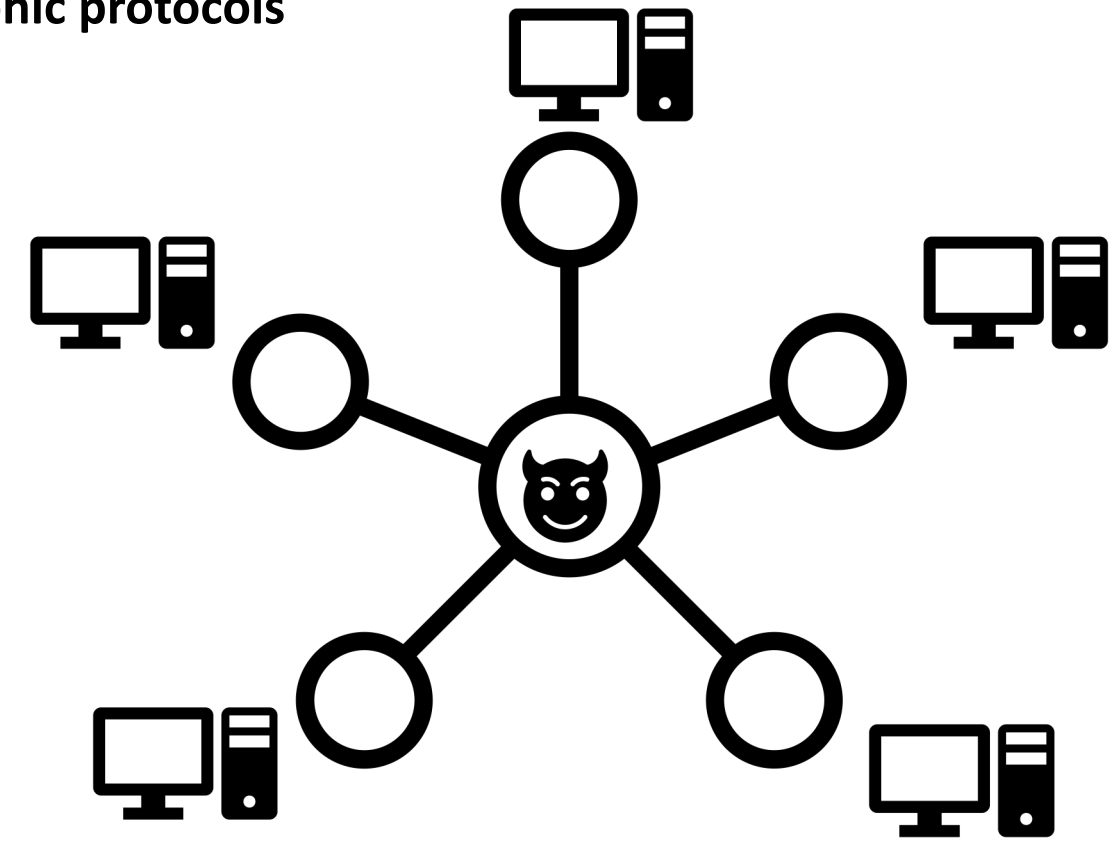
Context

- Sociotechnical System
  - A sociotechnical system is the term usually given to any instantiation of socio and technical elements engaged in **goal directed behaviour**. (*Wikipedia*)
  - A technical system extended with its **human** users.
  - **Security Ceremony**: A security **protocol** extended with its human users.

- Examples
  - Flight boarding, safety
  - Voting, complex
  - POS transaction, security

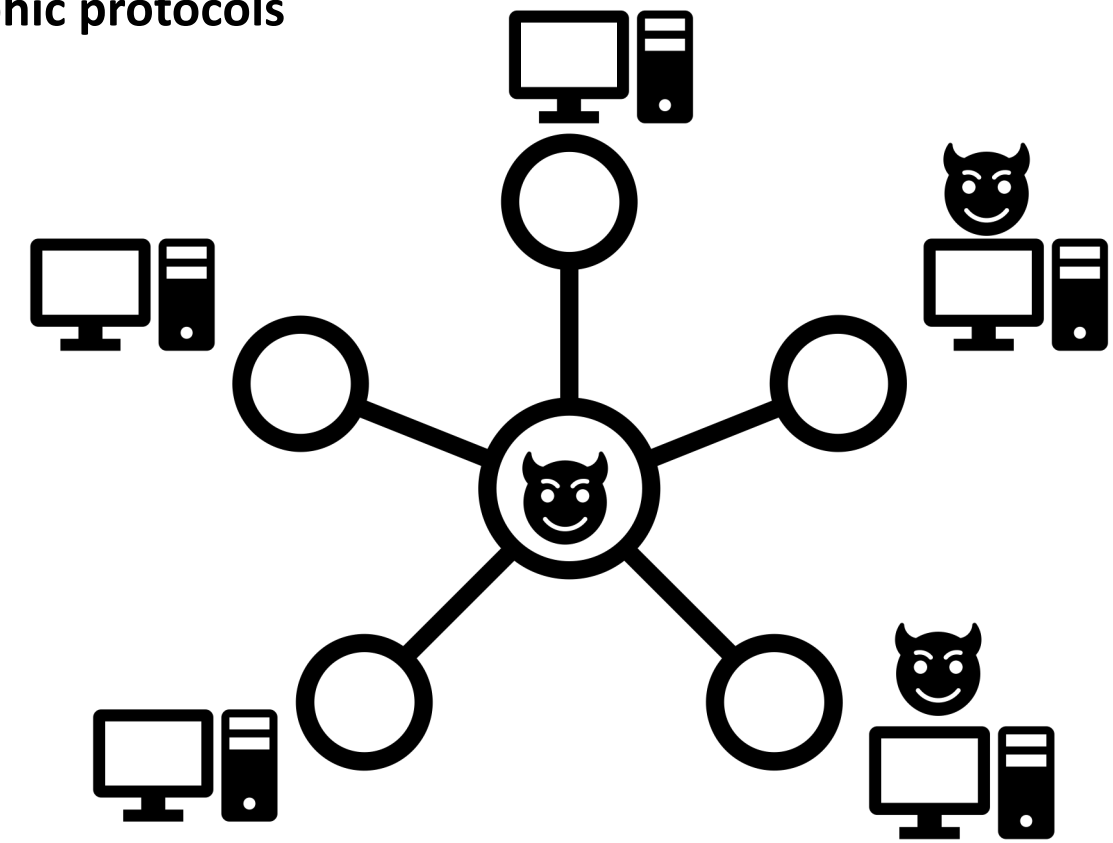
“Not a problem”

- (formal) security analysis of
  - **Cryptographic protocols**



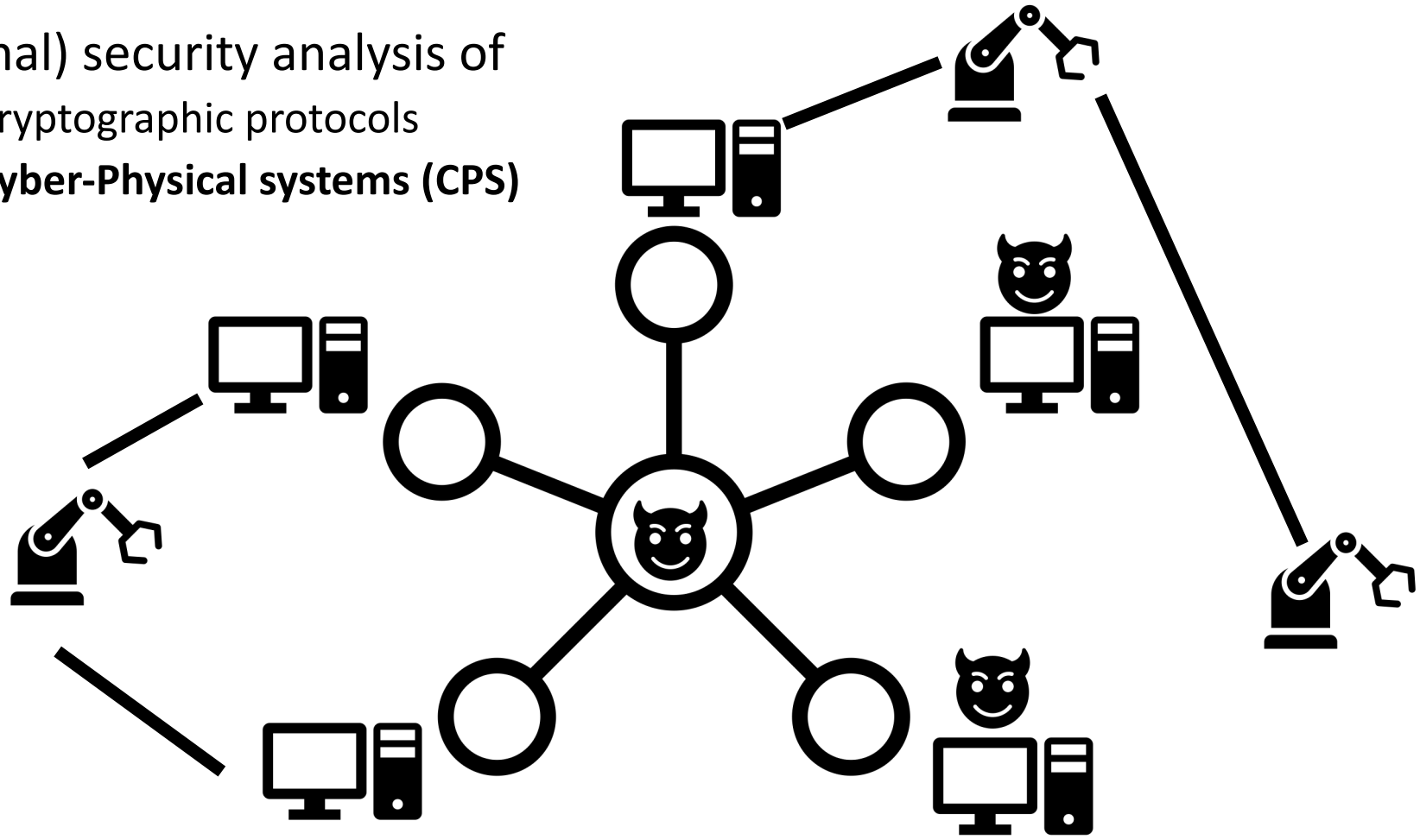
“Not a problem”

- (formal) security analysis of
  - **Cryptographic protocols**



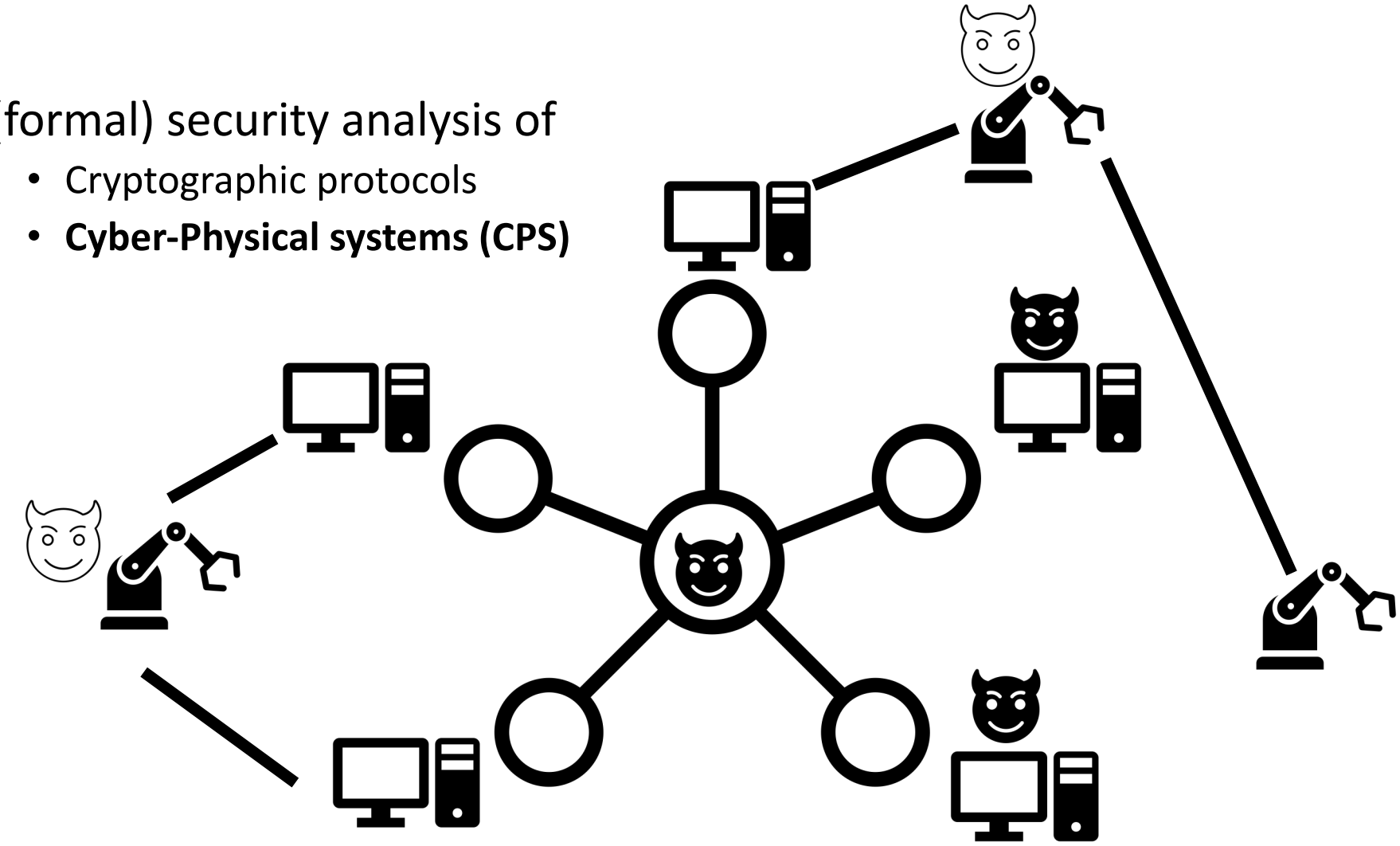
“Not a problem”

- (formal) security analysis of
  - Cryptographic protocols
  - **Cyber-Physical systems (CPS)**



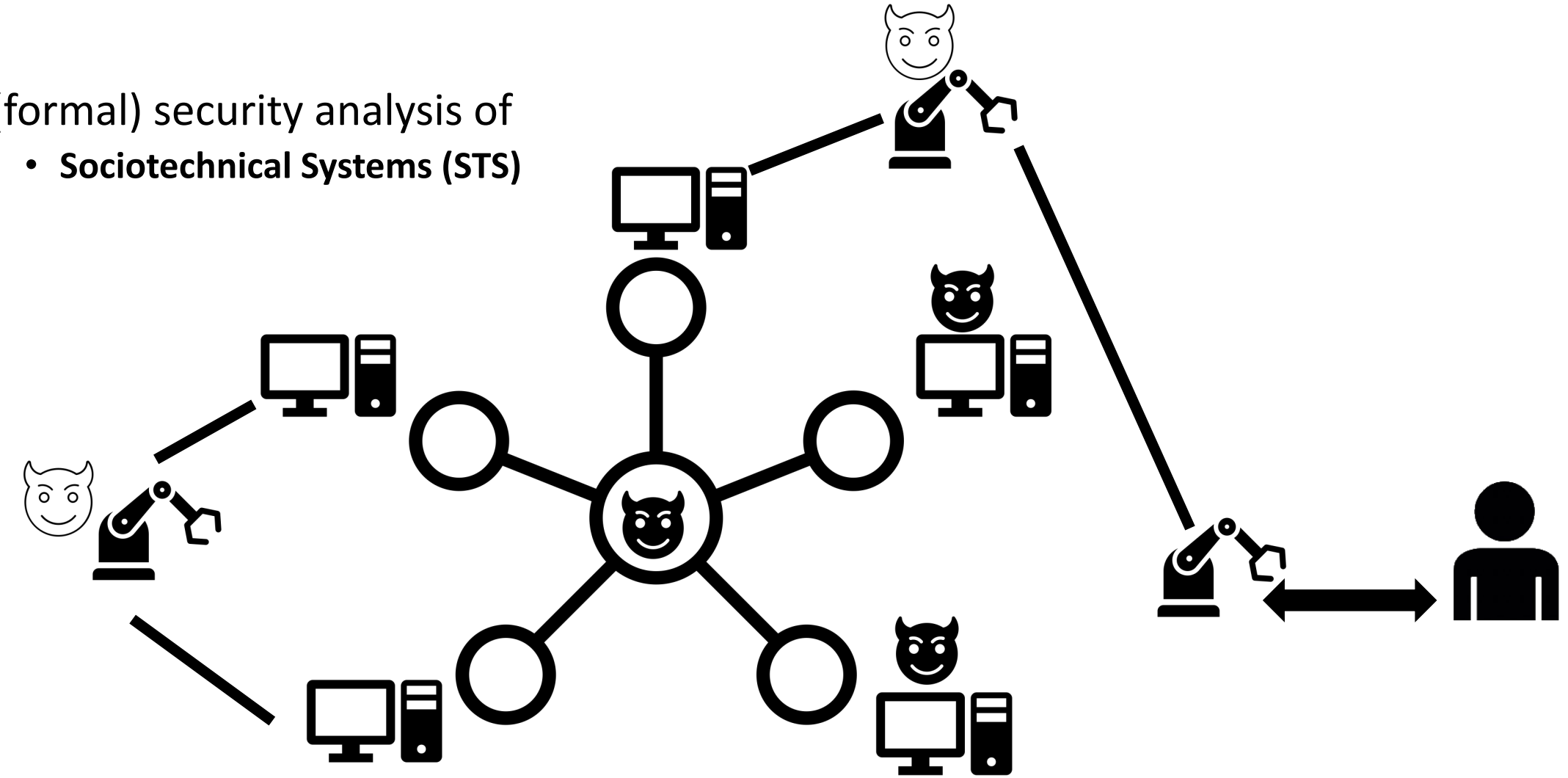
“Not a problem”

- (formal) security analysis of
  - Cryptographic protocols
  - **Cyber-Physical systems (CPS)**



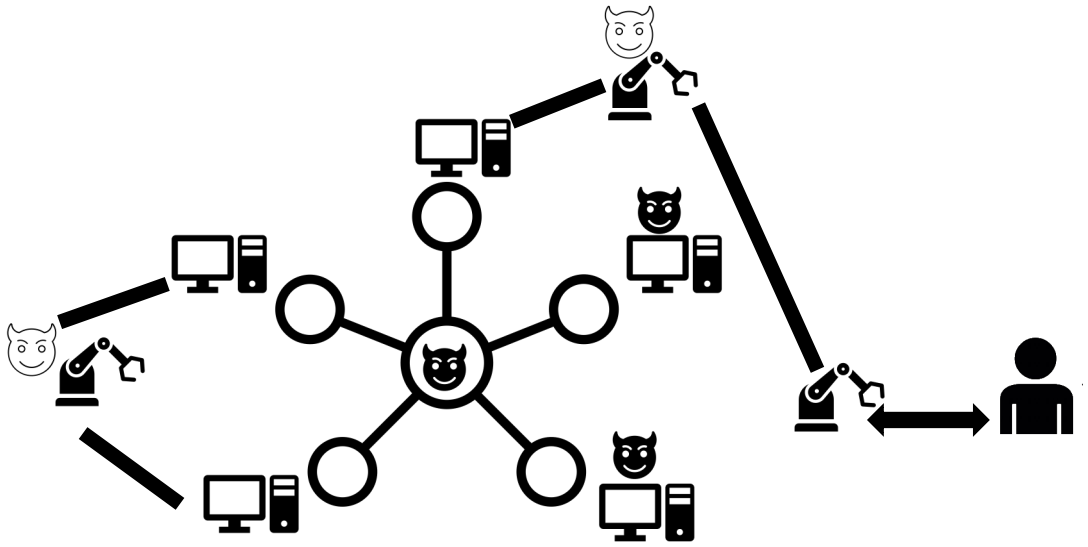
Problem

- (formal) security analysis of
  - **Sociotechnical Systems (STS)**



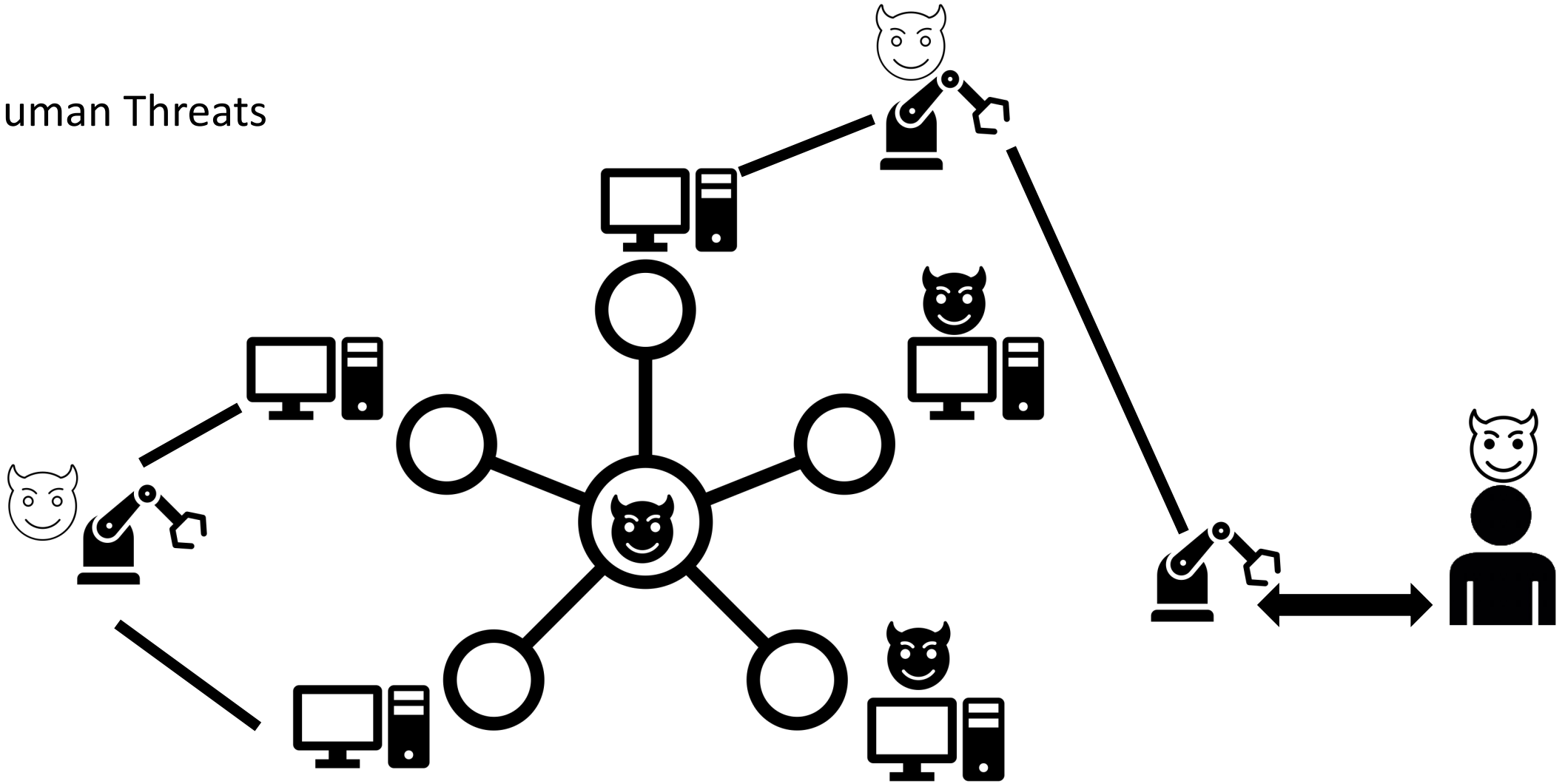
Problem

- Few works focus on the formal security analysis of STS
  - Bella and Coles-Kamp [IFIPSEC12], focus on human-computer interaction
  - Basin et al.[CSF16], focus on human errors
  - Sempreboni and Vigano [EuroSP20], focus on “mutations” of humans and of the underlying technical components



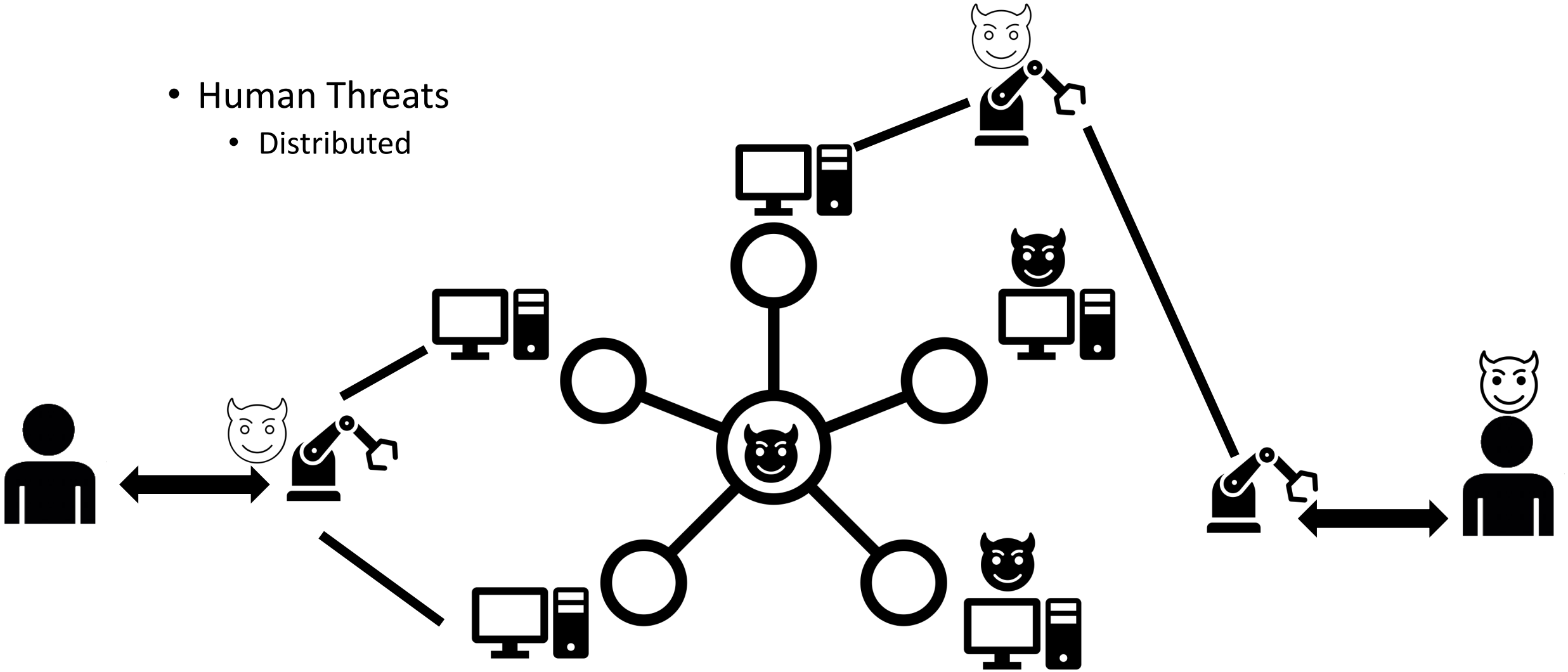
Focus

- Human Threats



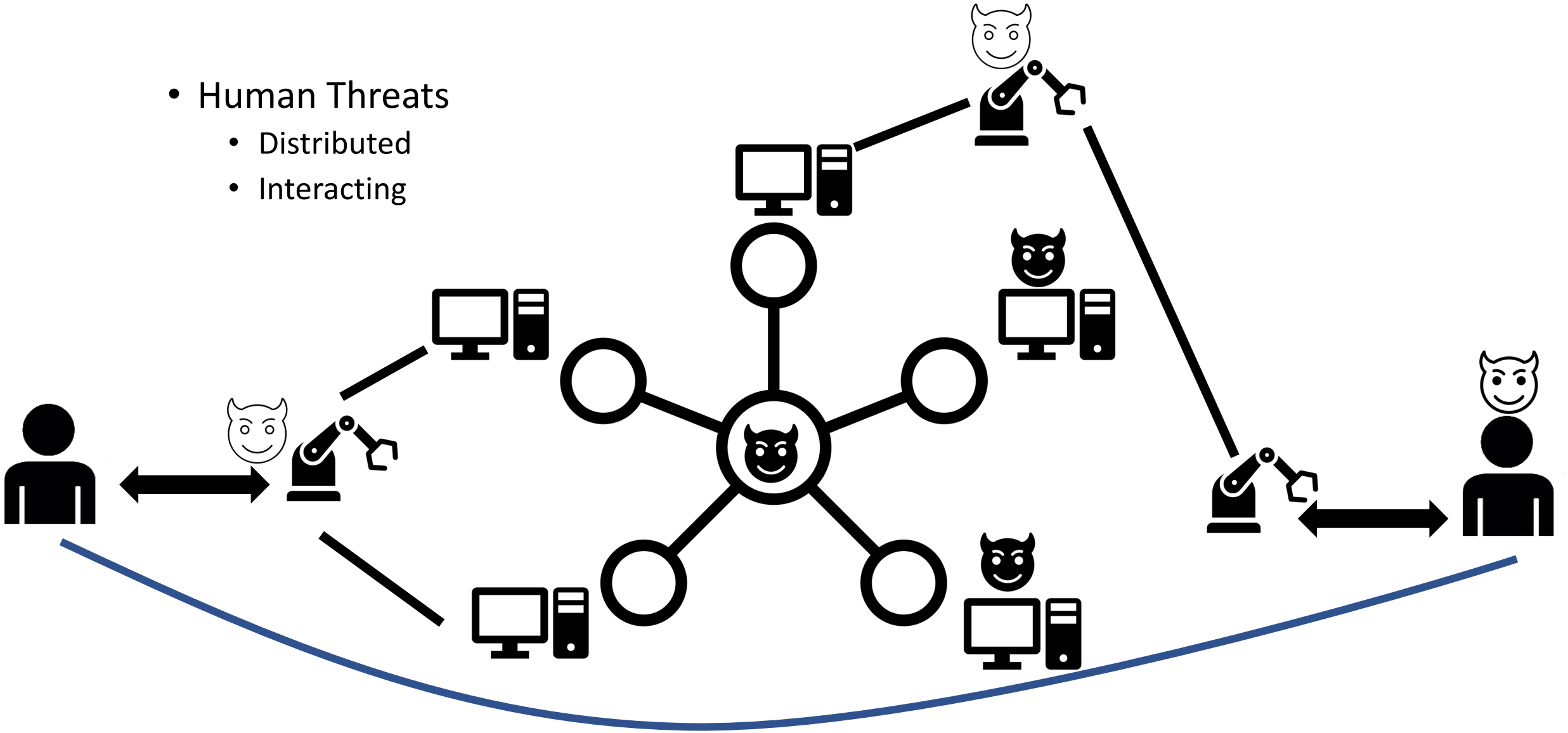
Focus

- Human Threats
  - Distributed



Focus

- Human Threats
  - Distributed
  - Interacting



Outline

- Definitions in **epistemic modal logic of human threats** to STS
- Formal analysis of (Danish) **Deposit Return Systems** in Tamarin
- Definition of a **lattice of human threat** models
- Search methodology for finding **maximal threat models** not breaking security properties

A threat model for interacting humans

- Essentially
  - *Honest*, **follows** the rules of a given ceremony precisely
  - *Chatty*, discloses their own **information**
    - e.g. reveals their passwords or the content printed on a ticket.
  - *Cocky*, gives out own **objects** that are relevant to the given ceremony
    - e.g., hands a physical token or a paper ticket.
  - *Forger*, **counterfeits** objects out of known information about them
    - e.g., builds physical token (provided they know the crypto material) via a 3D printer
    - *Receipt forger*, counterfeits printouts out of known information

Epistemic modal logic

$$\text{Terms} \qquad t ::= x \mid f(t_1, \ldots, t_n)$$

$$\text{Formulas} \quad F, G ::= 1 \mid P(t_1, \ldots t_n) \mid F \multimap G \mid F \otimes G \mid [\![K]\!]F \mid [K]F$$
$$\mid \forall x.\, F \mid \exists x.\, F \mid \Pi K.\, F \mid \Sigma K.\, F$$

$$(Look) : \Pi P.\, \forall o.\, [P]object(o) \multimap ([\![P]\!]info(o) \otimes [P]object(o))$$

Epistemic modal logic

$$(Chatty) : \Pi P.\, \Pi Q.\, \forall o.\, [\![P]\!]chatty \otimes [\![P]\!]info(o) \multimap [\![Q]\!]info(o)$$

$$(Give) \;\; : \Pi P.\, \Pi Q.\, \forall o.\, [\![P]\!]cocky \otimes [P]object(o) \multimap [Q]object(o)$$

$$(Hand) : \Pi P.\, \Pi Q,\, \forall r.\, [\![P]\!]cocky \otimes [P]receipt(r) \multimap [Q]receipt(r)$$

$$(Print) \;\; : \Pi K.\, \forall o.\, [\![K]\!]Rforger \otimes [\![K]\!]info(o) \multimap [K]receipt(QR(o))$$

$$(Build) : \Pi K.\, \forall b.\, [\![K]\!]Oforger \otimes [\![K]\!]info(b) \multimap [K]object(b)$$

Deposit Return System

DANSK RETUR SYSTEM

Kæmpe boom i antallet af pantflasker: Hele 1,7 mia. flasker og dåser blev afleveret i 2020

22.3.2021 12:35:29 CET | Dansk Retursystem

Problem

- Security protocols models are normally available
  - E.g. RFC, open-source, reverse engineering, etc.
- Sociotechnical system models are normally **not** available

How to Board a Plane

http://www.wikihow.com/Board-a-Plane

Navigating the Airport

1. Print your boarding pass and check your luggage.
2. Head to security.
3. Find your gate/terminal.
4. Hang out and wait for your plane.

Boarding the Plane

1. Wait for the announcement to board.
2. Get your boarding pass checked.
3. Walk down the hallway that leads up to your plane.
4. Enter the aircraft.
5. Stow your carry-on items.
6. Get settled in.

Problem

- Security protocols models are normally available
  - E.g. RFC, open-source, reverse engineering, etc.
- Sociotechnical system models are normally **not** available

DANSK RETUR SYSTEM

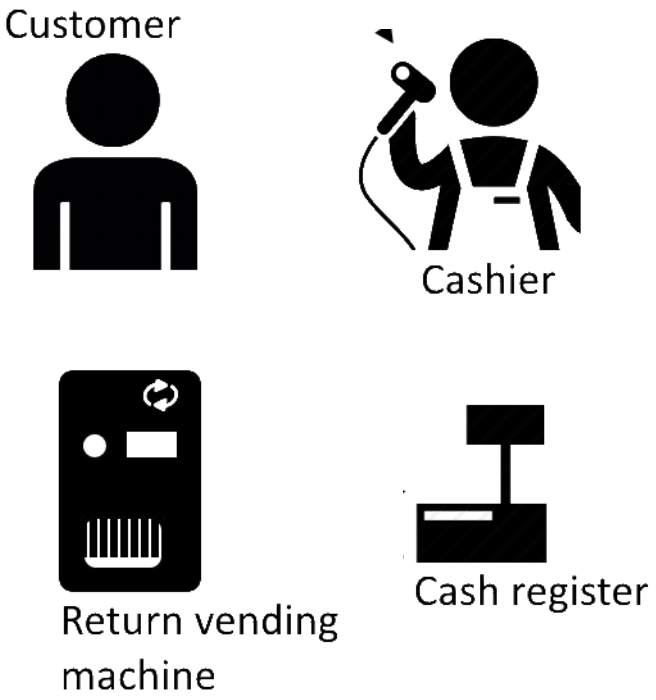
coop | Kvickly

TOMRA

NETTO

Solution

- Field observation
  - To collect human behaviour
- Patents' analysis
  - To understand the technicalities
- Playing detective
  - To refine drafts of the ceremony



Playing detective

Supermarket chain

Store

Counter

EAN-13 check

Playing detective

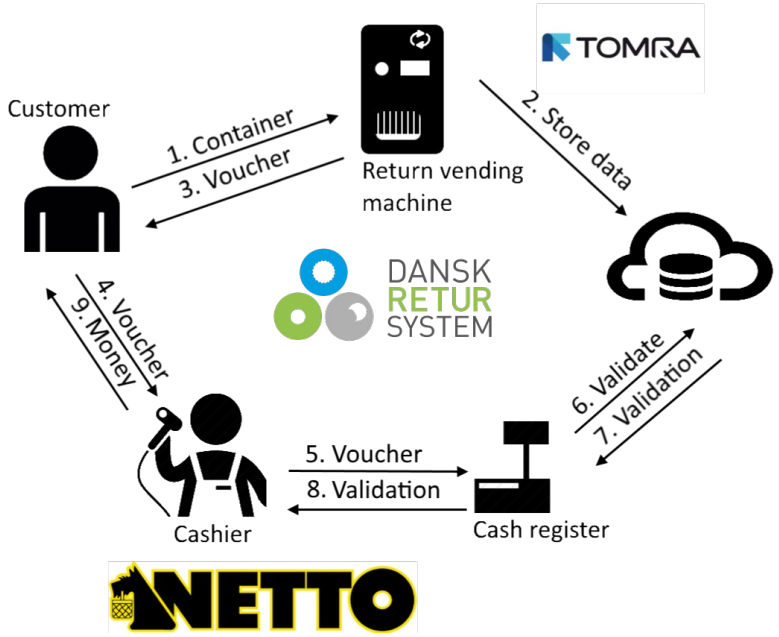
Supermarket chain

Store

Counter

EAN-13 check

Deposit Return System



$$(Purchase) : \Pi S.\, \Pi C.\, \forall c.\, [\![S]\!]seller \otimes [\![C]\!]customer \otimes [S]object(c) \multimap [C]object(c)$$

$$(Return) : \Pi C.\, \Pi V.\, \forall c.\, [\![C]\!]customer \otimes [\![V]\!]rvm \otimes [C]object(c) \multimap [V]object(c)$$

$$(Output) : \Pi V.\, \Pi Ca.\, \Pi C.\, \forall c.[\![V]\!]rvm \otimes [\![Ca]\!]cashier \otimes [\![C]\!]customer \otimes [V]object(c) \multimap [\![Ca]\!]info(c) \otimes \exists id.[C]receipt(QR(c, id))$$

$$(Hand) : \Pi C.\, \Pi Ca.\, \forall r.[\![C]\!]customer \otimes [\![Ca]\!]cashier \otimes [C]receipt(r) \multimap [Ca]receipt(r)$$

$$(Cash) : \Pi Ca.\, \forall id,\, \forall c.\, [\![Ca]\!]cashier \otimes [Ca]receipt(QR(c, id)) \otimes [\![Ca]\!]info(c) \multimap 1$$

Formal analysis

- Tamarin
  - Essentially a *constraint solver*
  - **Parties and threat specs using *multi-set rewriting***
  - **Properties spec using *metric first-order logic***
  - Proofs constructed using *backward search*

Encoding epistemic modal logic ➡ Tamarin

Encoding epistemic modal logic ➡ Tamarin

- Properties as metric first-order logic
  - E.g. forall traces, *Cash* is always preceeded by a container *Hand*.

$$(Purchase) : \Pi S.\, \Pi C.\, \forall c.\, [\![S]\!]seller \otimes [\![C]\!]customer \otimes [S]object(c) \multimap [C]object(c)$$

$$(Return) : \Pi C.\, \Pi V.\, \forall c.\, [\![C]\!]customer \otimes [\![V]\!]rvm \otimes [C]object(c) \multimap [V]object(c)$$

$$(Output) : \Pi V.\, \Pi Ca.\, \Pi C.\, \forall c.[\![V]\!]rvm \otimes [\![Ca]\!]cashier \otimes [\![C]\!]customer \otimes [V]object(c) \multimap [\![Ca]\!]info(c) \otimes \exists id.[C]receipt(QR(c, id))$$

$$(Hand) : \Pi C.\, \Pi Ca.\, \forall r.[\![C]\!]customer \otimes [\![Ca]\!]cashier \otimes [C]receipt(r) \multimap [Ca]receipt(r)$$

$$(Cash) : \Pi Ca.\, \forall id,\, \forall c.\, [\![Ca]\!]cashier \otimes [Ca]receipt(QR(c, id)) \otimes [\![Ca]\!]info(c) \multimap 1$$

Encoding epistemic modal logic ➡ Tamarin

- Properties as metric first-order logic
  - E.g. forall traces, *Cash* is always preceeded by a container *Hand*.

$$(Purchase) : \Pi S.\, \Pi C.\, \forall c.\, [\![S]\!]seller \otimes [\![C]\!]customer \otimes [S]object(c) \multimap [C]object(c)$$

$$(Return) : \Pi C.\, \Pi V.\, \forall c.\, [\![C]\!]customer \otimes [\![V]\!]rvm \otimes [C]object(c) \multimap [V]object(c)$$

$$(Output) : \Pi V.\, \Pi Ca.\, \Pi C.\, \forall c.[\![V]\!]rvm \otimes [\![Ca]\!]cashier \otimes [\![C]\!]customer \otimes [V]object(c) \multimap [\![Ca]\!]info(c) \otimes \exists id.[C]receipt(QR(c, id))$$

$$(Hand) : \Pi C.\, \Pi Ca.\, \forall r.[\![C]\!]customer \otimes [\![Ca]\!]cashier \otimes [C]receipt(r) \multimap [Ca]receipt(r)$$

$$(Cash) : \Pi Ca.\, \forall id,\, \forall c.\, [\![Ca]\!]cashier \otimes [Ca]receipt(QR(c, id)) \otimes [\![Ca]\!]info(c) \multimap 1$$

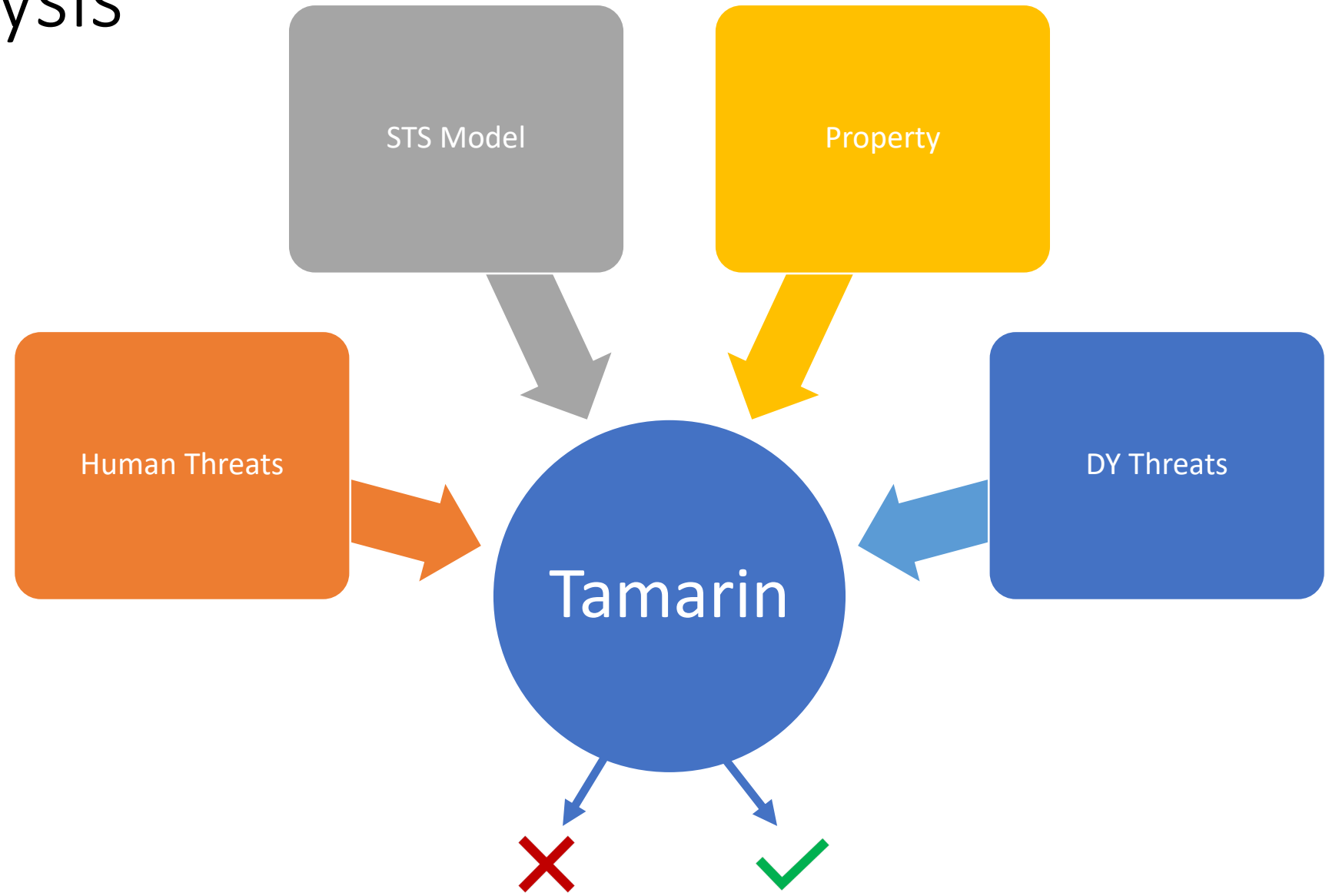
$$\forall Ca\ C\ id\ c\ \#i.\ Cash(Ca, id, c)@i \implies \exists\, \#j.\ Hand(C, Ca, QR(c, id))@j \wedge j < i$$

Properties

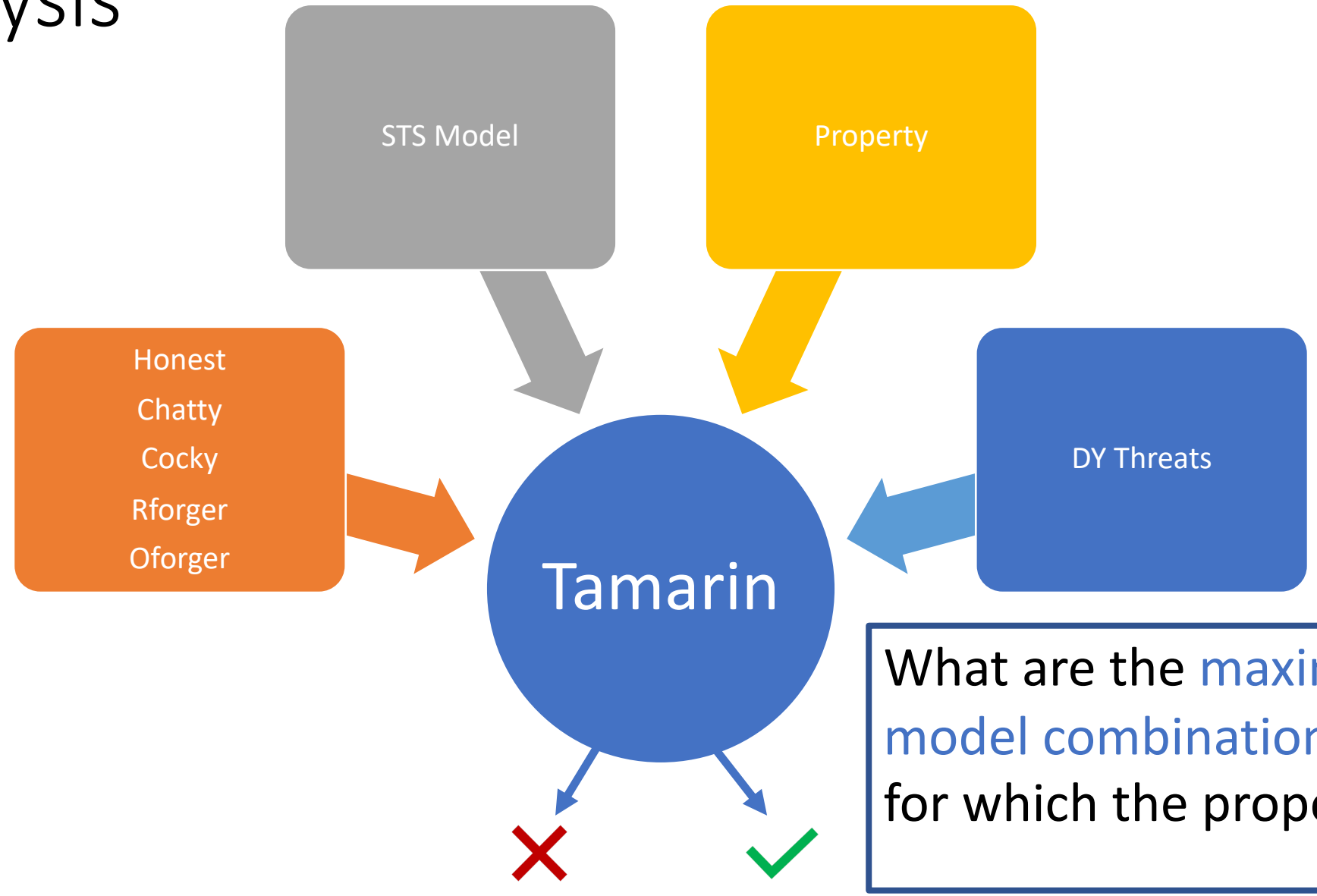
If a cashier cashes out a voucher, then a corresponding…

Cash for voucher	… receipt has been printed earlier by a RVM
Cash for container	… container has been returned earlier to a RVM
Strong cash for container	… container has been returned earlier to a RVM by the buyer
Cash for purchase	… container has been bought earlier
Strong cash for purchase	… container has been bought earlier by the same customer

Analysis

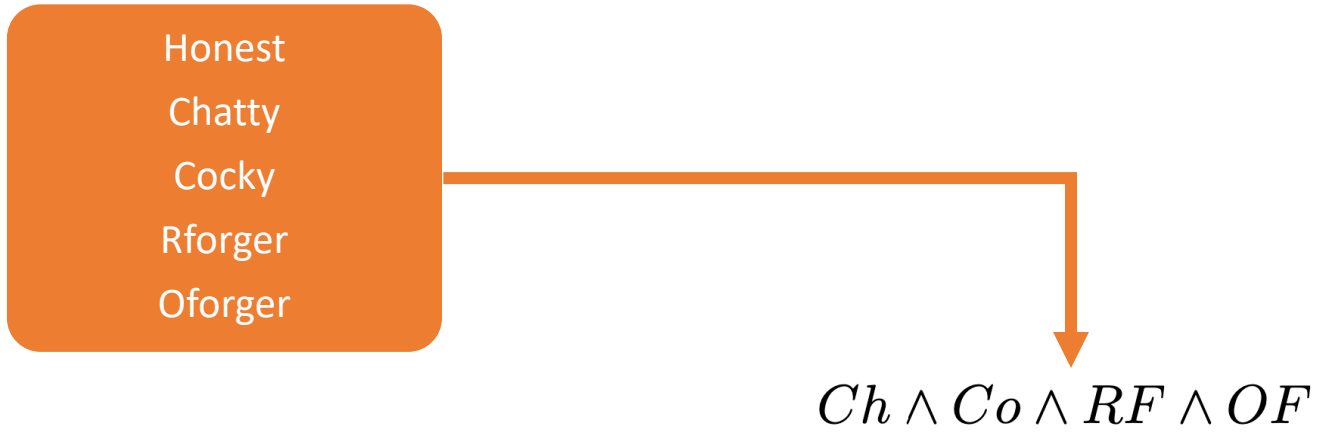


Analysis



What are the maximal threat model combinations (MTMC) for which the property holds?

Lattice of human threats



Lattice of human threats

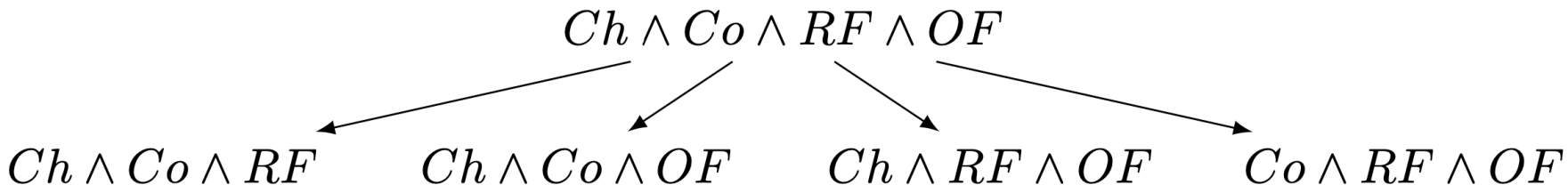
Honest

Chatty

Cocky

Rforger

Oforger



Lattice of human threats

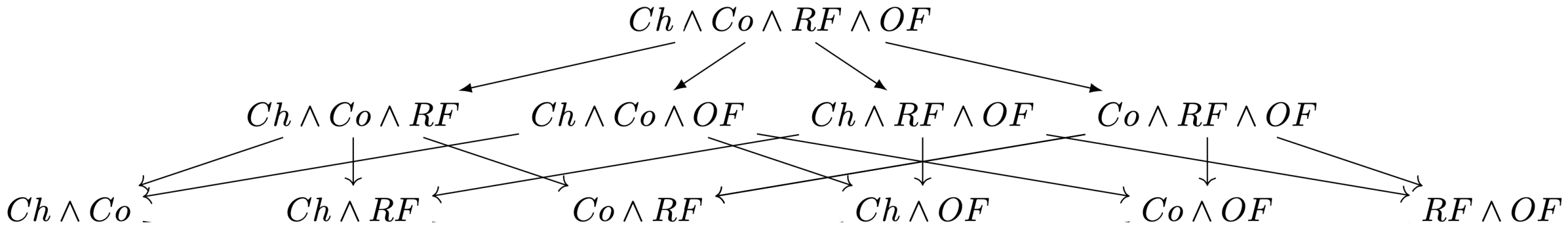
Honest

Chatty

Cocky

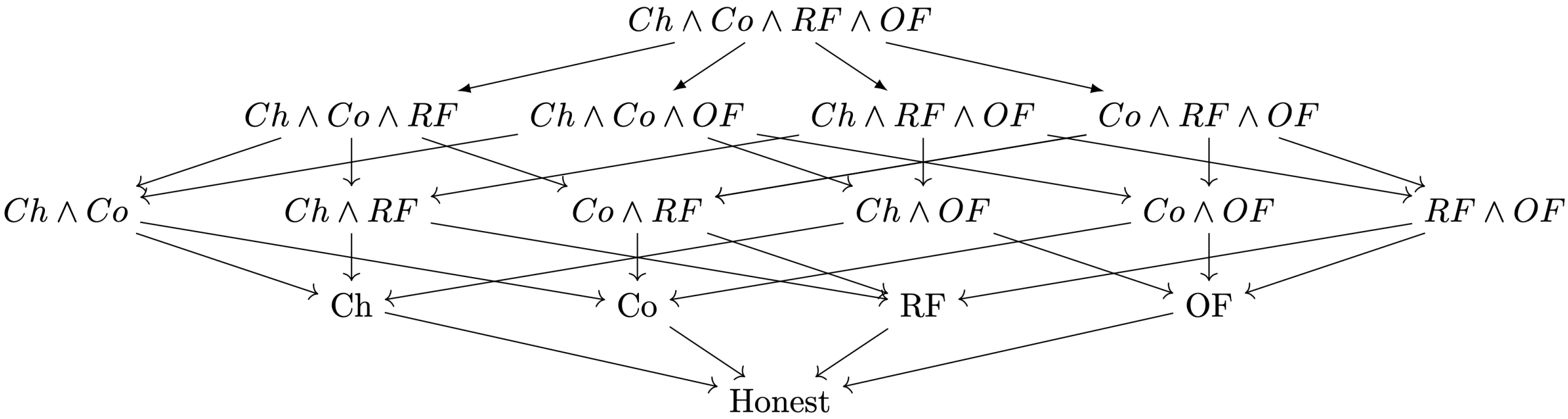
Rforger

Oforger



Lattice of human threats

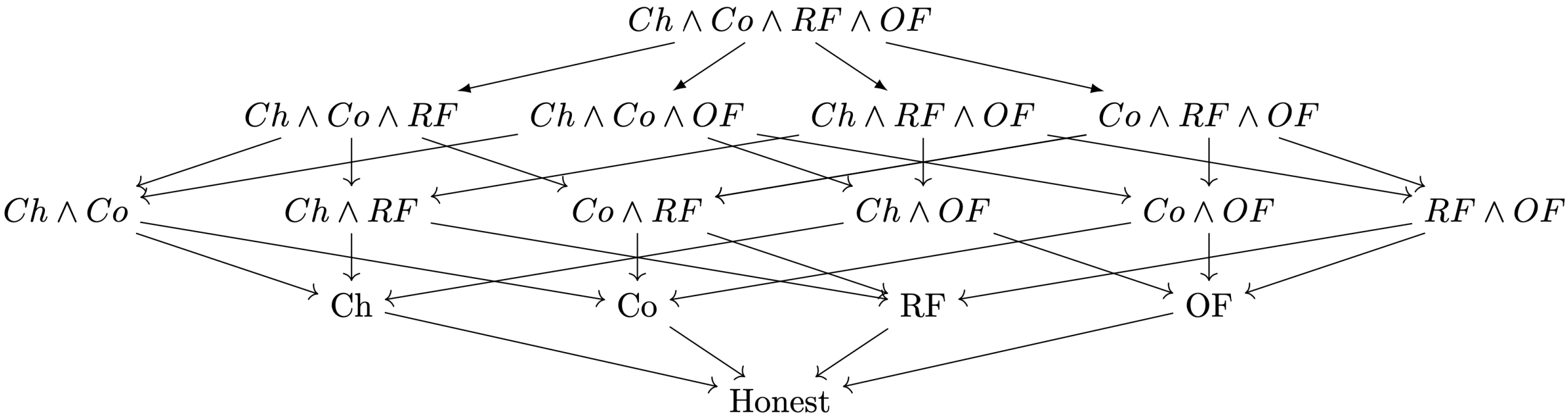
Honest
Chatty
Cocky
Rforger
Oforger



Lattice of human threats

What are the maximal threat model combinations (MTMC) for which the property holds?

Honest
Chatty
Cocky
Rforger
Oforger



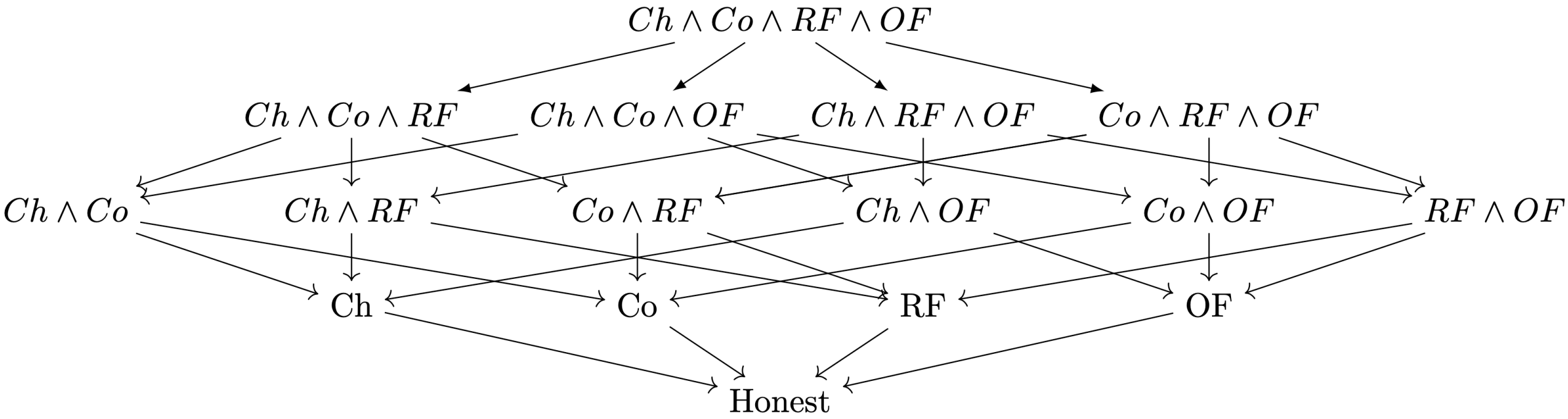
Lattice of human threats

What are the maximal threat model combinations (MTMC) for which the property holds?

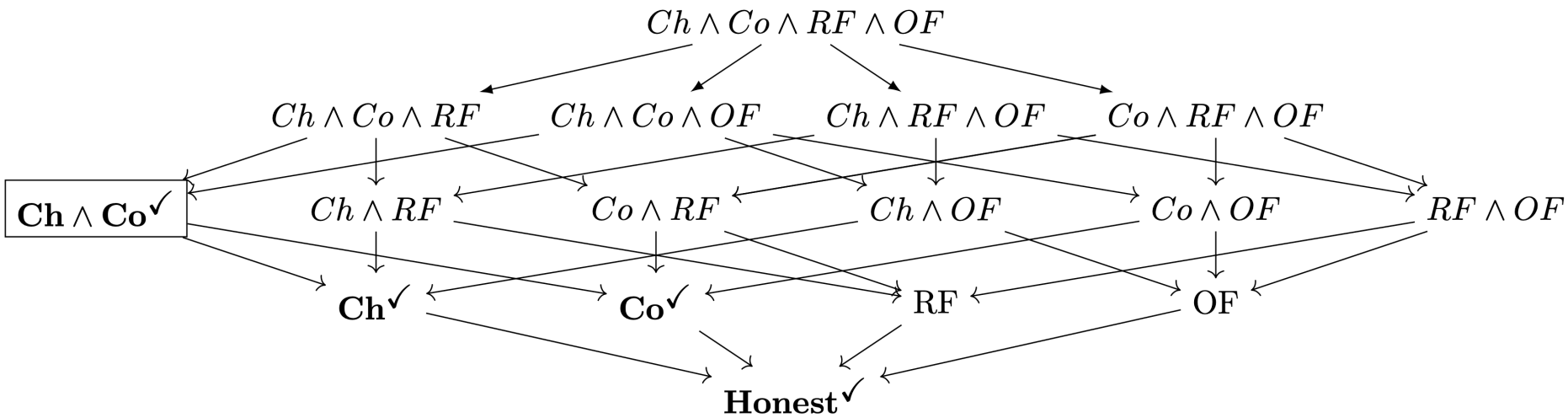
Honest
Chatty
Cocky
Rforger
Oforger

Problem: Finding MTMC can be time expensive!

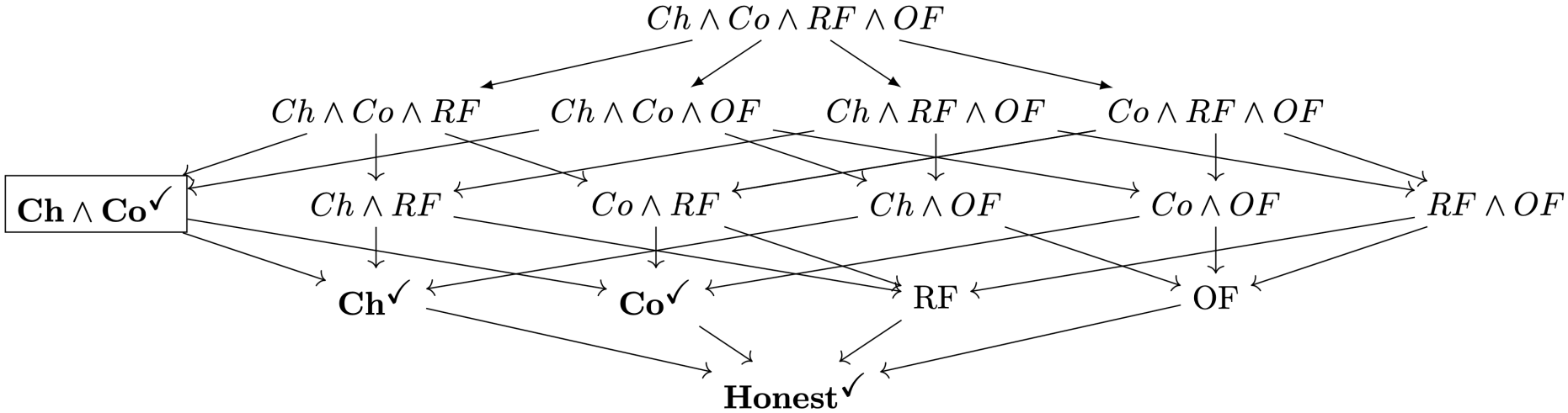
Worst case: $2^{\#\text{threats}}$ Tamarin analysis per property

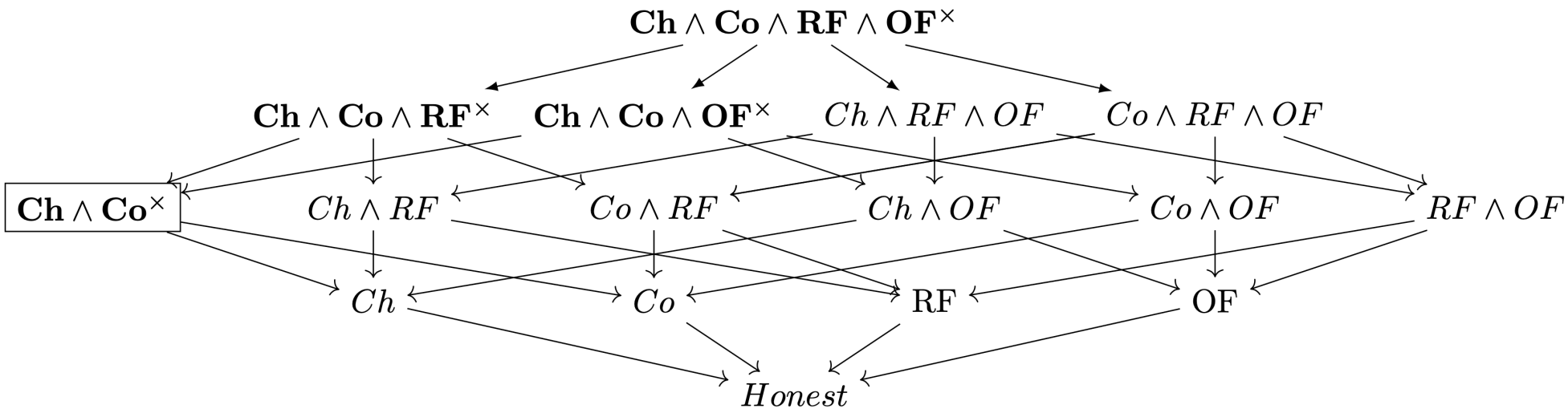


Lattice of human threats

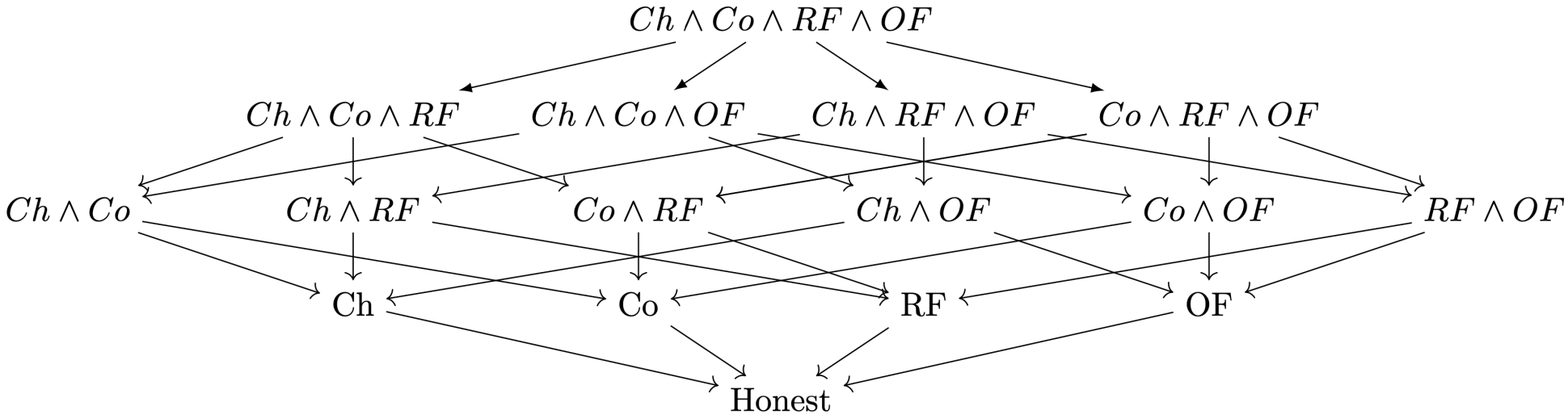


Lattice of human threats





Lattice of human threats



procedure `Greedy_check` (G) **:**

  $c \leftarrow$ `Max_edges` (G)

  if `L` $(c) \rightarrow \checkmark$ **then**

    `DFS` $(G, c, \checkmark, \downarrow)$

  else

    `DFS` $(G, c, \times, \uparrow)$

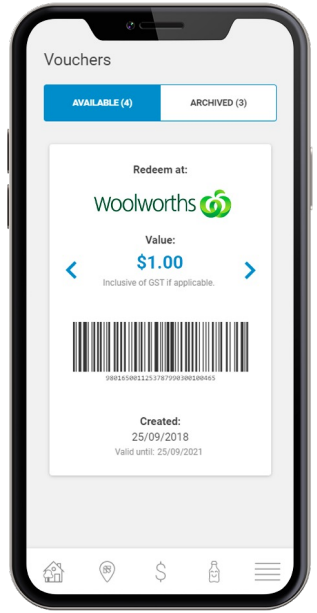
  `Greedy_check` $(G\ [C\text{-}C_l\ ])$

Results

	Kvickly & Coop		Netto	
	Result	*MTMC*	*Result*	*MTMC*
Cash for voucher	×	(Ch ∧ Co ∧ OF) , (RF ∧ OF)	✓	(Ch ∧ Co ∧ RF ∧ OF)
Cash for container	×	(Ch ∧ Co ∧ OF) , (RF ∧ OF)	✓	(Ch ∧ Co ∧ RF ∧ OF)
Cash for container customer	×	(Ch ∧ OF) , (RF ∧ OF)	×	(Ch ∧ OF) , (RF ∧ OF)
Cash for purchase	×	(Ch ∧ Co) , (RF ∧ OF)	×	(Ch ∧ RF ∧ Co) , (RF ∧ OF)
Cash for purchase customer	×	Ch , (RF ∧ OF)	×	Ch , (RF ∧ OF)

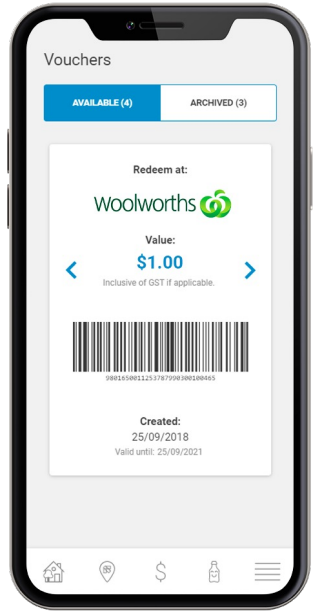
Fix

- Inspiration from *myTomraApp*, piloted in Australia
  - Cash out directly at the RVM



Fix

- Inspiration from *myTomraApp*, piloted in Australia
  - Cash out directly at the RVM



- Combination of NemID + e-boks + Storebox
- Receipt linked to the buyer as e-voucher
- NemID 2FA to protect against human threats

Conclusion

- Attempt to **understanding formally** human threats in STS
- **Lattice of threat models** makes sense when dealing with human threats
- Fixes against human threats require a **shifting to technical solutions**

- Just an attempt
  - A general set of human + physical + network threats
  - Encoding epistemic modal logic to Tamarin
  - More case studies
  - Consider privacy

‘‘under the Danish law it is not allowed to copy or make changes to vouchers or to encourage others to do so.”