A Labeled Logic for Analyzing Cyber-Forensics Evidence

Luca Viganò

Erisa Karafili, Matteo Cristani, Luca Viganò

"AF-Cyber: Logic-based Attribution and Forensics in Cyber Security"
Funded by the EU's Horizon 2020 under the Marie Skłodowska-Curie grant agreement No 746667.

Agenda

The Future is Interconnected

- *In 2020 there is an expectation of more than 20 billions of IoT devices connected* (McAfee labs)
- The growing of connectivity increases the security challenges
- *"Every minute, we are seeing about half a million attack attempts that are happening in Cyber Space"*(Fortinet)
- The cost of Cyber Crime Damage by 2021 will reach $6 Trillion (Cybersecurity Ventures)

The Problem

- Forensics investigations often produce an enormous amount of evidence
  - Pieces of evidence are produced/collected by various sources:
    - humans (e.g., another analyst) or
    - forensic tools such as intrusion detection system (IDS), traceback systems, malware analysis tools, and so on.

- The forensics investigator needs to
  - collect the evidence
  - check the sources of the evidence for evaluating their reliability
  - deal with enormous amount of pieces of evidence
  - analyse incomplete and/or conflicting evidence

A first example

- Erisa: which are the last two small teams to win the Serie A?

A first example

- Erisa: which are the last two small teams to win the Serie A?
- Matteo (born in Verona) and Luca (born in Genova) answer:

A first example

- Erisa: which are the last two small teams to win the Serie A?
- Matteo (born in Verona) and Luca (born in Genova) answer:

A first example

- Erisa: which are the last two small teams to win the Serie A?
- Matteo (born in Verona) and Luca (born in Genova) answer:

- When?

A first example

- Erisa: which are the last two small teams to win the Serie A?
- Matteo (born in Verona) and Luca (born in Genova) answer:

- When?

  There is some confusion about the dates (1984-85 and 1990-91), so what can Erisa conclude?

Data Breach of Democratic National Committee (DNC)

In Nov 2016, Wikileaks published private emails from the DNC.

Data Breach of Democratic National Committee (DNC)

In Nov 2016, Wikileaks published private emails from the DNC.

- Crowdstrike (a cyber-security company):
  - Attack occurred in March-April 2016
  - A successful spear phishing campaign using Bitly accounts to shorten malicious URLs

Data Breach of Democratic National Committee (DNC)

In Nov 2016, Wikileaks published private emails from the DNC.

- Crowdstrike (a cyber-security company):
  - Attack occurred in March-April 2016
  - A successful spear phishing campaign using Bitly accounts to shorten malicious URLs
- TheForensicator (an anonymous analyst):
  - Attack occurred the 5th of July 2016
  - Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016

Data Breach of Democratic National Committee (DNC)

In Nov 2016, Wikileaks published private emails from the DNC.

- Crowdstrike (a cyber-security company):
  - Attack occurred in March-April 2016
  - A successful spear phishing campaign using Bitly accounts to shorten malicious URLs
- TheForensicator (an anonymous analyst):
  - Attack occurred the 5th of July 2016
  - Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016
- FireEye (another cyber-security company):
  - It is possible to have a non physical speed transfer of 23MB/s.

Data Breach of Democratic National Committee (DNC)

In Nov 2016, Wikileaks published private emails from the DNC.

- Crowdstrike (a cyber-security company):
  - Attack occurred in March-April 2016
  - A successful spear phishing campaign using Bitly accounts to shorten malicious URLs
- TheForensicator (an anonymous analyst):
  - Attack occurred the 5th of July 2016
  - Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016
- FireEye (another cyber-security company):
  - It is possible to have a non physical speed transfer of 23MB/s.

What should an analyst conclude from these discording statements and pieces of evidence?

How can a decision be made?

Our Solution

Solution

Evidence Logic $\mathcal{EL}$ and its Rewriting Procedure represent the pieces of evidence, analyse and filter them by using the relations of trust between sources and reasonings

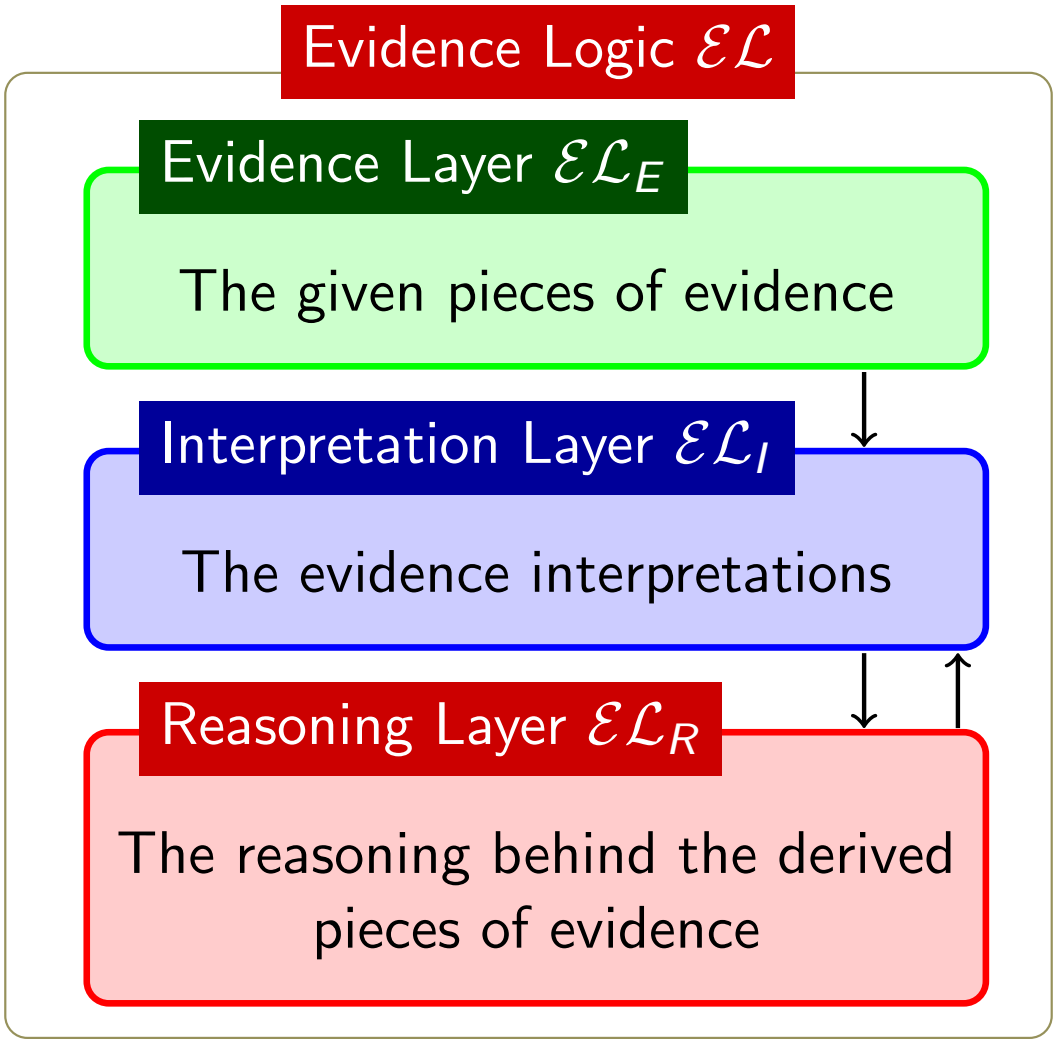
- Our solution filters the enormous amount of evidence
- Solves temporal and factual discordancies
- $\mathcal{EL}$ and the Rewriting Procedure are sound

Evidence Logic $\mathcal{EL}$

- **Evidence Logic** $\mathcal{EL}$ is based on Linear Temporal Logic and permits to represent:
  - the different pieces of evidence
  - the evidence source and sources relations of trust
  - the reasoning behind the derived pieces of evidence and their relations of trust

- In a nutshell:
  - **Evidence** represents information related to the attack, where a given (piece of) evidence usually represents an event, its occurrence and the source of the information of the occurrence of the event (another analyst, a cyber-forensics tool, etc.)
  - **Evidence interpretation** represents what the analyst thinks about the occurrence of an event e and about the occurrences of the events causing e

Evidence Logic Layers



$\mathcal{EL}_E$: Evidence

Definition

Given $t, t_1, \ldots t_n \in T$, $a, a_1, \ldots a_n \in Ag$, $r_1, r_2 \in \mathcal{R}$, $p \in Vars_S$ and $\phi, \phi_1, \ldots, \phi_n \in Lit$, the set ρ of formulas of $\mathcal{EL}_E$ is

$$\begin{aligned} \rho ::= \quad & a : (t : \phi) \mid \\ & a : (t : \phi)\ [a_1 : (t_1 : \phi_1) \mid \ldots \mid a_n : (t_n : \phi_n)]_r \mid \\ & a_1 \lhd_p a_2 \mid r_1 \prec r_2 \end{aligned}$$

$$Alice : (t : SourceAttack(A, IP_1)) \qquad Bob : (t : \neg SourceAttack(A, IP_1))$$
$$Bob \lhd_{SourceAttack} Alice$$

$$Charlie : (t : AttackOrigin(A, Area_1))\ [Alice : (t : SourceAttack(A, IP_1)) \mid Geoloc : (t : Geo(IP_1, Area_1))]_{r_1}$$

Simple Evidence and Derived Evidence

- The simple evidence expresses that the agent represented by the source label a thinks that the literal ϕ is true at the instant of time represented by the temporal label t

$$a : (t : \phi)$$

- The derived evidence expresses that a thinks that ϕ is true at instant of time t *because* of reasoning r, where a_1 thinks that ϕ_1 is true at t_1, ... and a_n thinks that ϕ_n is true at t_n

$$a : (t : \phi)\ [a_1 : (t_1 : \phi_1) \mid a_2 : (t_2 : \phi_2) \mid \ldots \mid a_n : (t_n : \phi_n)]_r$$

  - In other words, based on r, a thinks that ϕ is *caused* by $\phi_1, \cdots, \phi_n$ (with their respective time instants and agents).
  - The reasoning r of the derived evidence $a : (t : \phi)$ is composed of simple and/or derived pieces of evidence.
    We forbid cycles between derived pieces of evidence: if $a_i : (t_i : \phi_i)\ [\cdots \mid a_j : (t_j : \phi_j) \mid \ldots]_r$, then $a_j : (t_j : \phi_j)\ [\cdots \mid a_i : (t_i : \phi_i) \mid \ldots]_{r'}$ is not a wff.

Evidence

- FireEye (*FE*): it is possible to have a non physical speed transfer of 23MB/s.

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$\overbrace{FE}^{Source} : (\overbrace{t_2}^{Time} : \overbrace{NonPhysicalSpeedTrans(23MB/s)}^{Event})$$

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s)) \Big\} \rightarrow Simple\ Evidence$$

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

- Crowdstrike (CS): the attack occurred in March-April 2016, a successful spear phishing campaign using Bitly accounts to shorten malicious URLs.

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

- Crowdstrike (CS): the attack occurred in March-April 2016, a successful spear phishing campaign using Bitly accounts to shorten malicious URLs.

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

- Crowdstrike (CS): the attack occurred in March-April 2016, a successful spear phishing campaign using Bitly accounts to shorten malicious URLs.

$$\overbrace{CS}^{Source} : (\overbrace{t_1}^{Time} : \overbrace{Attack}^{Event}) \overbrace{[CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}}^{Simple/Derived\ Evidence\ used\ by\ r_1}$$

Evidence

- FireEye (FE): it is possible to have a non physical speed transfer of 23MB/s.

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s)) \Big\} \rightarrow Simple\ Evidence$$

- Crowdstrike (CS): the attack occurred in March-April 2016, a successful spear phishing campaign using Bitly accounts to shorten malicious URLs.

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1} \Big\} \rightarrow \begin{array}{l} Derived \\ Evidence \end{array}$$

Other Pieces of Evidence

- TheForensicator (TF): the attack occurred the 5th of July 2016. Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016.

Other Pieces of Evidence

- TheForensicator (TF): the attack occurred the 5th of July 2016. Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016.

$$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

Other Pieces of Evidence

- TheForensicator (TF): the attack occurred the 5th of July 2016. Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016.

$$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

- The analyst trusts more FireEye than TheForensicator for the speed of non physical data transfer

Other Pieces of Evidence

- TheForensicator (TF): the attack occurred the 5th of July 2016. Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016.

$$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

- The analyst trusts more FireEye than TheForensicator for the speed of non physical data transfer

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Other Pieces of Evidence

- TheForensicator (TF): the attack occurred the 5th of July 2016. Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016.

$$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

- The analyst trusts more FireEye than TheForensicator for the speed of non physical data transfer

$$TF \overbrace{\lhd_{NonPhysicalSpeedTrans(23MB/s)}}^{Trust\ \ Relation} FE$$

Other Pieces of Evidence

- TheForensicator (TF): the attack occurred the 5th of July 2016. Analysing the released metadata: physical transfer, as the created data were transferred on the speed of 23MB/s and the data were created the 5th of July 2016.

$$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

- The analyst trusts more FireEye than TheForensicator for the speed of non physical data transfer

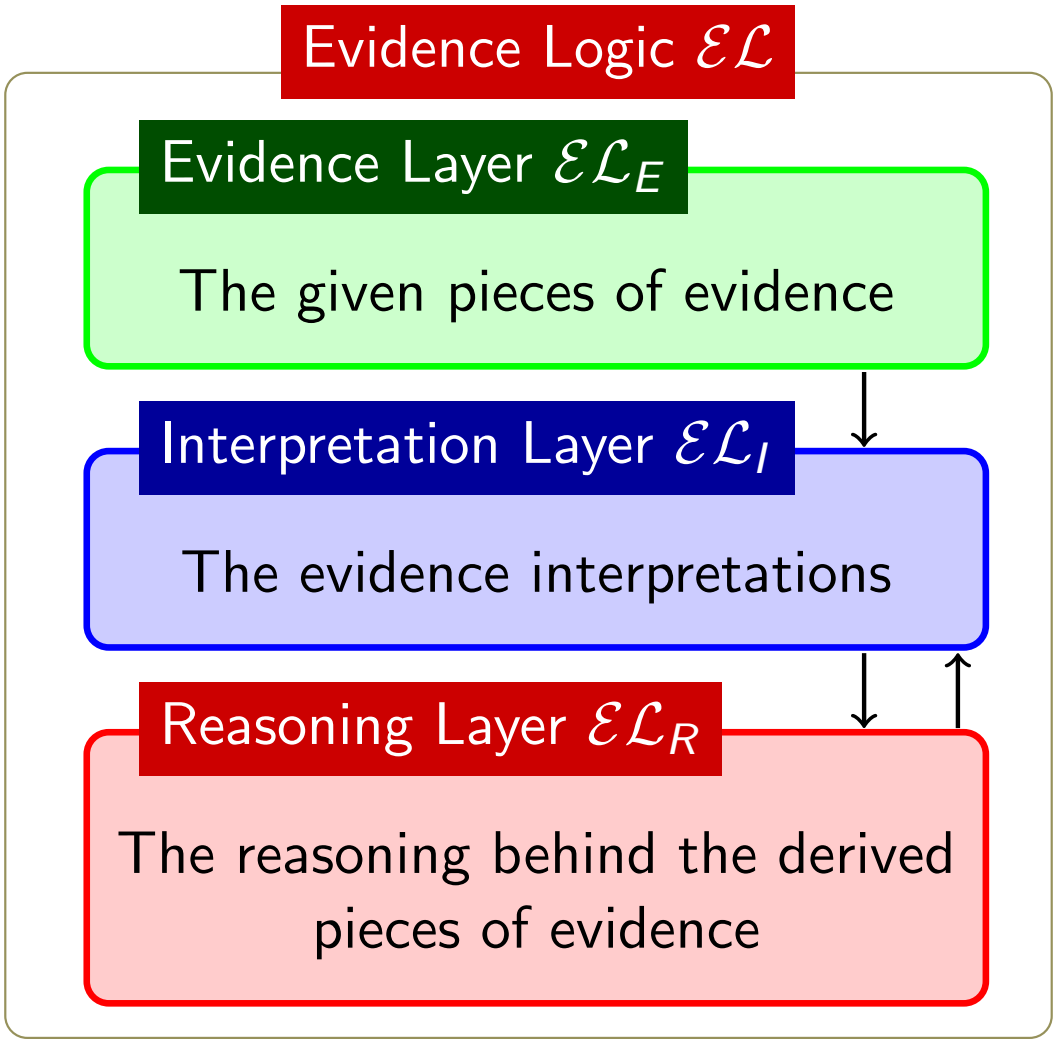
$$\left.\begin{array}{l} TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE \end{array}\right\} \rightarrow Relational\ Formula$$

Evidence Representation with $\mathcal{EL}_E$

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

Evidence Logic Layers



$\mathcal{EL}_I$: Evidence Interpretation

- *Evidence interpretation*: what analyst thinks is plausibly true.
- Second level $\mathcal{EL}_I$ of $\mathcal{EL}$ employs a simplified variant of *LTL*.
- $\mathcal{EL}_I$ inherits from $\mathcal{EL}_E$: temporal labels T, reasonings $\mathcal{R}$ and propositional variables *Vars* (and thus also literals *Lit*).

Definition

Given $t, t_1, \ldots t_n \in T$, $\phi, \phi_1, \ldots, \phi_n \in Lit$, $r \in \mathcal{R}$ and $\phi' \in Lit_D$, the set φ of formulas of $\mathcal{EL}_I$, called interpretations, is

$$\varphi ::= \; t : \phi \mid t_1 : \phi_1 \wedge t_2 : \phi_2 \wedge \ldots \wedge t_n : \phi_n \rightarrow_r t : \phi'$$

$t_1 : \phi_1 \wedge \ldots \wedge t_n : \phi_n \rightarrow_r t : \phi'$ means analyst thinks that ϕ' is true at t, based on r, if ϕ_i is true at t_i for all $i \in \{1, \ldots, n\}$.

- Interpretation expresses a positive event $t : p$ (occurrence of event) or a negative event $t : \neg p$ (non occurrence of event).
- Interpretations that express positive events represent *plausible pieces of evidence* and help analyst perform a correct analysis.

$\mathcal{EL}_I$: Evidence Interpretation

Definition

Given $t, t_1, \ldots t_n \in T$, $\phi, \phi_1, \ldots, \phi_n \in Lit$, $r \in \mathcal{R}$ and $\phi' \in Lit_D$, the set φ of formulas of $\mathcal{EL}_I$, called *interpretations*, is

$$\varphi ::= \; t : \phi \mid t_1 : \phi_1 \wedge t_2 : \phi_2 \wedge \ldots \wedge t_n : \phi_n \rightarrow_r t : \phi'$$

$t : SourceAttack(A, IP_1)$
$t : \neg SourceAttack(A, IP_1)$
$t : SourceAttack(A, IP_1) \wedge t : Geo(IP_1, Area_1) \rightarrow_{r_1} t : AttackOrigin(A, Area_1)$

Evidence Interpretation

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$\Downarrow$$

Evidence Interpretation

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$
$$\Downarrow$$
$$t_2 : NonPhysicalSpeedTrans(23MB/s)$$

Evidence Interpretation

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$\Downarrow$$

$$t_2 : NonPhysicalSpeedTrans(23MB/s) \Big\} \rightarrow Evidence\ \ Interpretation$$

Evidence Interpretation

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$
$$\Downarrow$$
$$t_2 : NonPhysicalSpeedTrans(23MB/s)$$

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$

Evidence Interpretation

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$
$$\Downarrow$$
$$t_2 : NonPhysicalSpeedTrans(23MB/s)$$

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$
$$\Downarrow$$
$$t_1 : SpPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack$$

Evidence Interpretation

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$
$$\Downarrow$$
$$t_2 : NonPhysicalSpeedTrans(23MB/s)$$

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$
$$\Downarrow$$
$$t_1 : SpPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack \Big\} \rightarrow \text{Evidence Interpretation}$$

Evidence Interpretation with $\mathcal{EL}_I$

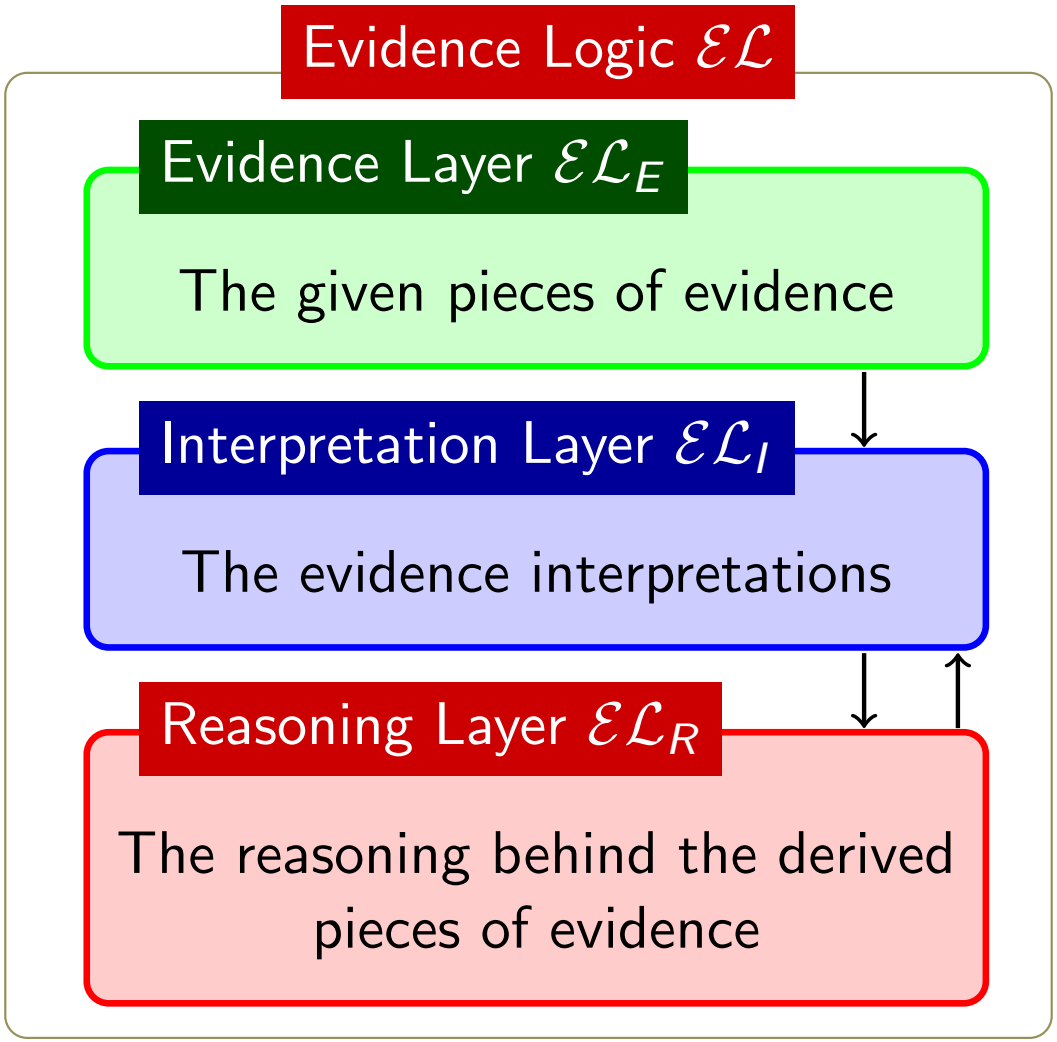
Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SpPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack$
$t_2 : NonPhysicalSpeedTrans(23MB/s)$

Evidence Logic Layers



Evidence Reasoning

- The third layer $\mathcal{EL}_R$ of $\mathcal{EL}$ is the *reasoning layer* and deals with the reasoning behind the derived evidence.
- Also $\mathcal{EL}_R$ uses LTL and inherits from $\mathcal{EL}_E$ temporal labels T, reasonings $\mathcal{R}$ and propositional variables *Vars*.

Definition

Given $t \in T$, $\phi \in Lit_D$ and $r, r_k, \ldots, r_l \in \mathcal{R}$, the set ψ of formulas of $\mathcal{EL}_R$ is

$$\psi ::= (t : \phi)_r \mid (t : \phi)_{r,r_k,\ldots,r_l}.$$

- The *reasoning* involves only derived pieces of evidence, which we can divide in two types (first special case of second).
- $(t : \phi)_{r,r_k,\cdots,r_l}$ composed of simple/derived pieces of evidence. The reasoning involves the one of agent stating the derived evidence, $a : (t : \phi)\ [a_1 : (t_1 : \phi_1) \mid \ldots \mid a_j : (t_j : \phi_j)]_r$, as well as all the reasonings involved in the derived pieces of evidence $\phi_i \in Lit$ for $i \in \{1, \ldots, j\}$ that are part of reasoning r.

$\mathcal{EL}_R$: Evidence Reasoning

Definition

Given $t \in T$, $\phi \in Lit_D$ and $r, r_k, \ldots, r_l \in \mathcal{R}$, the set ψ of formulas of $\mathcal{EL}_R$ is

$$\psi ::= (t : \phi)_r \mid (t : \phi)_{r, r_k, \ldots, r_l}.$$

$$t : AttackOrigin(A, Area_1)_{r_1}$$

Evidence Reasoning

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$

Evidence Reasoning

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$
$$\Downarrow$$
$$(t_1 : Attack)_{r_1}$$

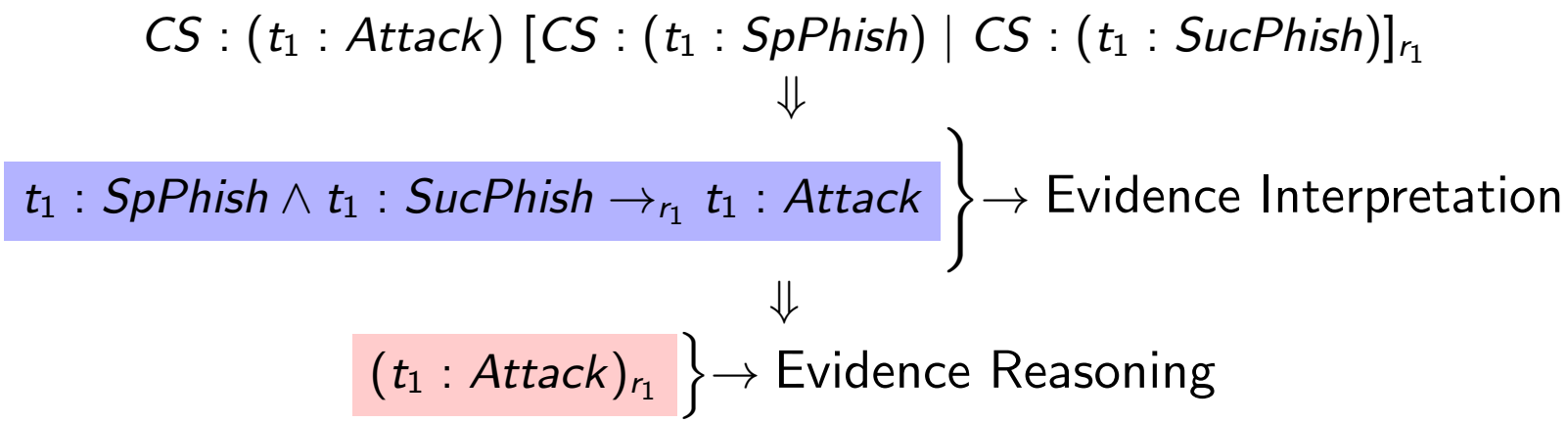
Evidence Reasoning

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$

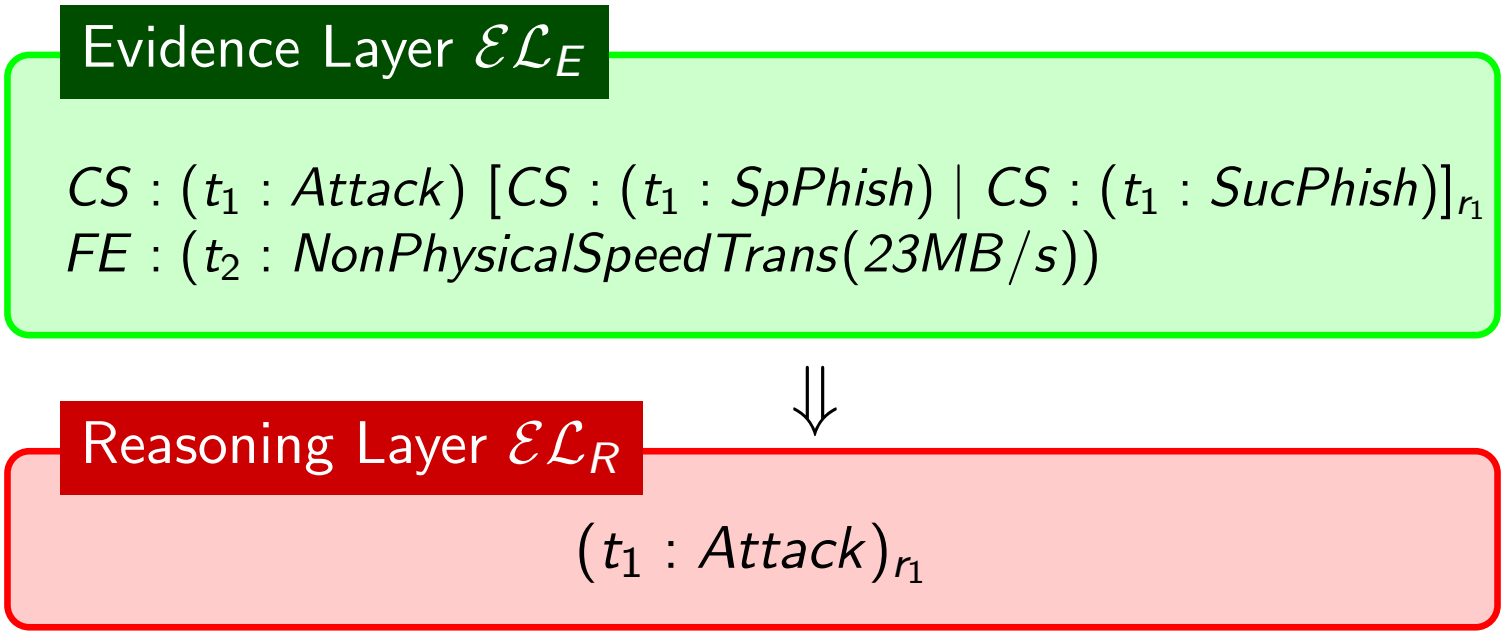
$$\Downarrow$$

$$(t_1 : Attack)_{r_1} \Big\} \rightarrow \text{Evidence Reasoning}$$

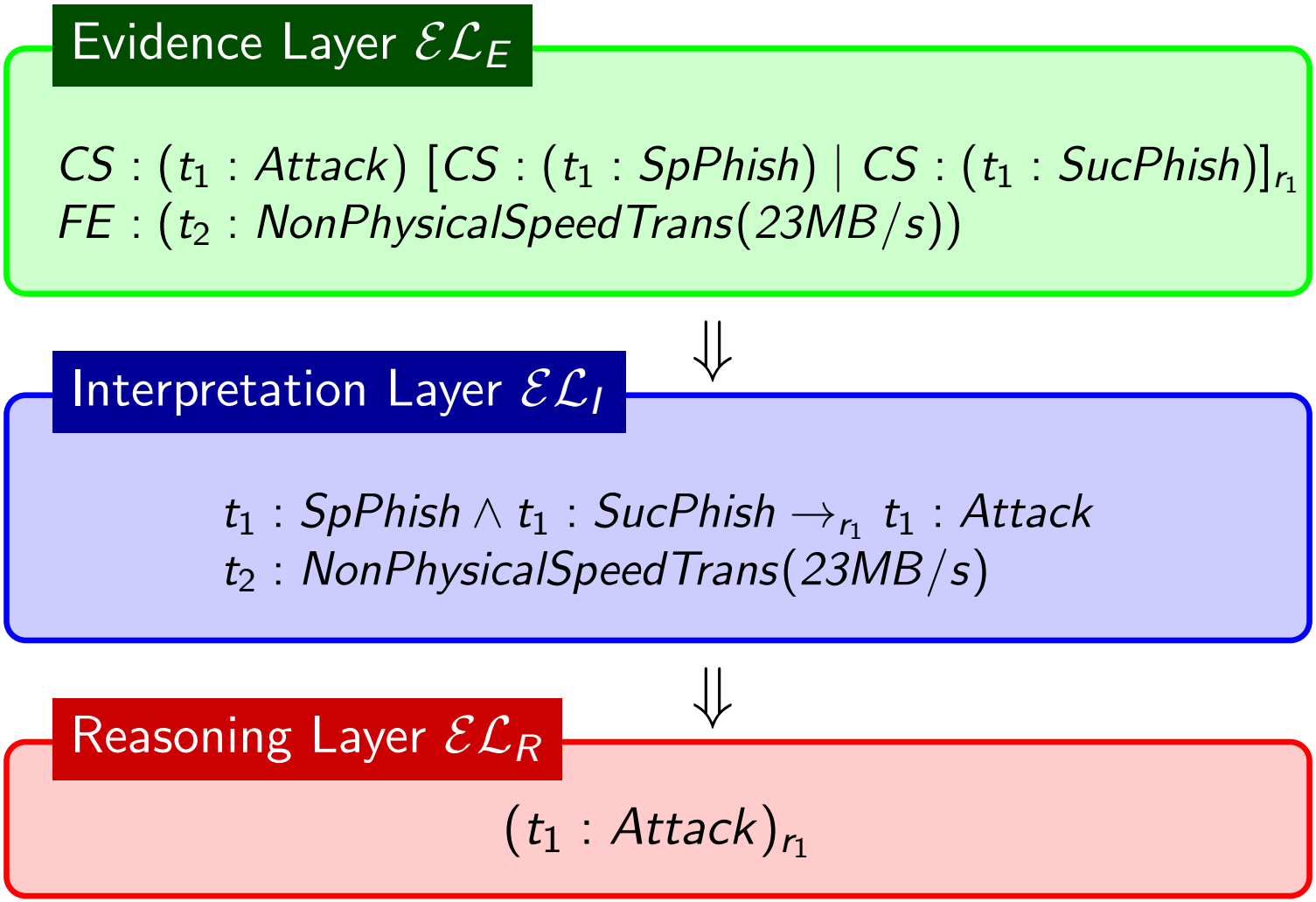
Evidence Reasoning



Evidence Reasoning with $\mathcal{EL}_R$



Evidence Reasoning with $\mathcal{EL}_R$



Semantics of $\mathcal{EL}$

Definition

The *plausible pieces of evidence* are a finite stream of temporal instants in which at every instant of time we may associate a finite number of occurrences or not occurrences of an event.

Definition

A model of the evidence language $\mathcal{EL}$ is a tuple

$$\mathfrak{M} = \{Ag^{\mathfrak{I}}, \mathcal{F}^{\mathfrak{I}}, \mathcal{PO}^{\mathfrak{I}}, \mathcal{TR}^{\mathfrak{I}}, Vars^{\mathfrak{I}}, \mathcal{R}^{\mathfrak{I}}, \mathfrak{I}\}$$

In order to avoid having clear contradictions in the models, we constrain the functions $Ag^{\mathfrak{I}}$ and $\mathcal{R}^{\mathfrak{I}}$ as follows:

- $(COND_1)$: If $a^{\mathfrak{I}}(t,p) = True$, then $a^{\mathfrak{I}}(t',p) = False$ for all $t' \neq t$.
- $(COND_2)$: If $(t,p)_{r^{\mathfrak{I}}} = True$, then $(t',p)_{r^{\mathfrak{I}}} = False$ for all $t' \neq t$.
- $(COND_3)$: Every $\lhd_p{}^{\mathfrak{I}}$ is an irreflexive and antisymmetric relation.
- $(COND_4)$: Every $\prec^{\mathfrak{I}}$ is an irreflexive and antisymmetric relation.

Rewriting System

The rewriting system gets as input the given pieces of evidence and gives as output a consistent set of pieces of evidence by

- rewriting pieces of evidence into interpretations and reasonings
- analysing the pieces of evidence
- resolving their discordances by eliminating the less trusted ones
- capturing the temporal and factual discordancies by using the trust relations

Types of Rules

- Insertion rules

$$\frac{a_1 : (t_1 : \phi) \quad a_2 : (t_2 : \phi)}{\mathcal{E} \cup \{a_1 : (t_2 : \neg\phi), a_2 : (t_1 : \neg\phi)\}} \mathcal{D}_1$$

- Elimination rules

$$\frac{a_2 \lhd_p a_1 \quad a_1 : (t : \phi) \quad a_2 : (t : \neg\phi)}{\mathcal{E} \setminus \{a_2 : (t : \neg\phi)\}} \mathcal{D}_2$$

- Closure rules

$$\frac{a : (t_1 : \phi) \quad a : (t_2 : \phi)}{\bot} \mathcal{C}_C$$

Rewriting Rules

Transformation rules

$$\frac{a : (t : \phi)}{\mathcal{E} \cup \{t : \phi\}}\ \mathcal{L}_1 \qquad \frac{(t : \phi)_{r,\cdots,r_n}}{\mathcal{E} \cup \{t : \phi\}}\ \mathcal{L}'_1$$

$$\frac{a : (t : \phi)\ [a_1 : (t_1 : \phi_1) \mid \cdots \mid a_n : (t_n : \phi_n)]_r}{\mathcal{E} \cup \{a_i : (t_i : \phi_i)\}_{\forall i \in \{1,\cdots,n\}\ \phi_i \in Lits} \cup \{t_1 : \phi_1 \wedge \cdots \wedge t_n : \phi_n \rightarrow_r t : \phi\}}\ \mathcal{L}_2$$

Rewriting Rules

Discordance resolutions rules

$$\frac{a_1 : (t_1 : \phi) \quad a_2 : (t_2 : \phi)}{\mathcal{E} \cup \{a_1 : (t_2 : \neg\phi), a_2 : (t_1 : \neg\phi)\}}\ \mathcal{D}_1 \qquad \frac{(t_1 : \phi)_{r_1} \quad (t_2 : \phi)_{r_2}}{\mathcal{E} \cup \{(t_2 : \neg\phi)_{r_1}, (t_1 : \neg\phi)_{r_2}\}}\ \mathcal{D}'_1$$

$$\frac{a_2 \lhd_p a_1 \quad a_1 : (t : \phi) \quad a_2 : (t : \neg\phi)}{\mathcal{E} \setminus \{a_2 : (t : \neg\phi)\}}\ \mathcal{D}_2 \qquad \frac{r_2 \prec r_1 \quad (t : \phi)_{r_1} \quad (t : \neg\phi)_{r_2}}{\mathcal{E} \setminus \{(t : \neg\phi)_{r_2}\}}\ \mathcal{D}'_2$$

Rewriting Rules

Transformation rules

$$\frac{a : (t : \phi)}{\mathcal{E} \cup \{t : \phi\}}\ \mathcal{L}_1 \qquad \frac{(t : \phi)_{r,\cdots,r_n}}{\mathcal{E} \cup \{t : \phi\}}\ \mathcal{L}'_1$$

$$\frac{a : (t : \phi)\ [a_1 : (t_1 : \phi_1) \mid \cdots \mid a_n : (t_n : \phi_n)]_r}{\mathcal{E} \cup \{a_i : (t_i : \phi_i)\}_{\forall i \in \{1,\cdots,n\}\ \phi_i \in Lit_S} \cup \{t_1 : \phi_1 \wedge \cdots \wedge t_n : \phi_n \rightarrow_r t : \phi\}}\ \mathcal{L}_2$$

Discordance resolutions rules

$$\frac{a_1 : (t_1 : \phi) \quad a_2 : (t_2 : \phi)}{\mathcal{E} \cup \{a_1 : (t_2 : \neg\phi), a_2 : (t_1 : \neg\phi)\}}\ \mathcal{D}_1 \qquad \frac{(t_1 : \phi)_{r_1} \quad (t_2 : \phi)_{r_2}}{\mathcal{E} \cup \{(t_2 : \neg\phi)_{r_1}, (t_1 : \neg\phi)_{r_2}\}}\ \mathcal{D}'_1$$

$$\frac{a_2 \lhd_p a_1 \quad a_1 : (t : \phi) \quad a_2 : (t : \neg\phi)}{\mathcal{E} \setminus \{a_2 : (t : \neg\phi)\}}\ \mathcal{D}_2 \qquad \frac{r_2 \prec r_1 \quad (t : \phi)_{r_1} \quad (t : \neg\phi)_{r_2}}{\mathcal{E} \setminus \{(t : \neg\phi)_{r_2}\}}\ \mathcal{D}'_2$$

Algorithm

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply $\textsc{Trans}\lhd$,$\textsc{Trans}\prec$ rules **do** Apply $\textsc{Trans}\lhd$, $\textsc{Trans}\prec$ rules **end while**
2: **while** We can apply $\textsc{Trans}\lhd$, $\textsc{Trans}\prec$ rules **do**
3: Apply $\textsc{Trans}\lhd$ and $\textsc{Trans}\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**

Rewriting Procedure

Evidence Layer $\mathcal{EL}_E$

$$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$$
$$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$
$$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$
$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$
$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Rewriting Procedure

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

- Apply rule $\mathcal{L}_2$

Transformation Rule Application

$$\frac{CS : (t_1 : Attack)\ [CS : (t_1 : SPhish) \mid CS : (t_1 : SucPhish)]_{r_1}}{\mathcal{E} \cup \{CS : (t_1 : SPhish), CS : (t_1 : SucPhish)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack\}}\ \mathcal{L}_2$$

Transformation Rule Application

$$\frac{TF : (t_2 : Attack)\ [(TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}}{\mathcal{E} \cup \{TF : (t_2 : MetaC)\} \cup \{t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack\}}\ \mathcal{L}_2$$

Transformation Rule Application

$$\frac{TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}}{\mathcal{E} \cup \{TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))\} \cup \{t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}}\ \mathcal{L}_2$$

Result of rule $\mathcal{L}_2$ application

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$
$CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : MetaC),$
$TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$

Result of rule $\mathcal{L}_2$ application and next step

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$
$CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : MetaC),$
$TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

⇓

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$

- Apply rule $\mathcal{D}_2$

Elimination Rule $\mathcal{D}_2$

$$\frac{TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE \quad FE : (t_2 : NonPhysicalSpeedTrans(23MB/s)) \quad TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))}{\mathcal{E} \setminus \{TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))\}}\ \mathcal{D}_2$$

Result of rule $\mathcal{D}_2$ application

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$
$CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : MetaC),$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$

Result of rule $\mathcal{D}_2$ application and next step

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$
$CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : MetaC),$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

$\Downarrow$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$

- Apply rule $\mathcal{L}_1$

Transformation Rules

$$\frac{FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))}{\mathcal{E} \cup \{t_2 : NonPhysicalSpeedTrans(23MB/s)\}}\ \mathcal{L}_1$$

$$\frac{CS : (t_1 : SPhish)}{\mathcal{E} \cup \{t_1 : SPhish\}}\ \mathcal{L}_1 \qquad \frac{CS : (t_1 : SucPhish)}{\mathcal{E} \cup \{t_1 : SucPhish\}}\ \mathcal{L}_1$$

$$\frac{TF : (t_2 : MetaC)}{\mathcal{E} \cup \{t_2 : MetaC\}}\ \mathcal{L}_1$$

Transformation Rules

$$\frac{FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))}{\mathcal{E} \cup \{t_2 : NonPhysicalSpeedTrans(23MB/s)\}}\ \mathcal{L}_1$$

$$\frac{CS : (t_1 : SPhish)}{\mathcal{E} \cup \{t_1 : SPhish\}}\ \mathcal{L}_1 \qquad \frac{CS : (t_1 : SucPhish)}{\mathcal{E} \cup \{t_1 : SucPhish\}}\ \mathcal{L}_1$$

$$\frac{TF : (t_2 : MetaC)}{\mathcal{E} \cup \{t_2 : MetaC\}}\ \mathcal{L}_1$$

Result of rule $\mathcal{L}_1$ application

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$
$t_2 : NonPhysicalSpeedTrans(23MB/s)$
$t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC$

Result of rule $\mathcal{L}_1$ application and next step

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$
$t_2 : NonPhysicalSpeedTrans(23MB/s),$
$t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC$

- Apply rule $(\rightarrow)$

Derivation of Derived Evidence

$$\frac{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack \quad t_1 : SPhish \quad t_1 : SucPhish}{\mathcal{E} \cup \{(t_1 : Attack)_{r_1}\}} \ (\rightarrow)$$

Result of rule ($\rightarrow$) application

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

$\Downarrow$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$
$t_2 : NonPhysicalSpeedTrans(23MB/s),$
$t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC$

$\Downarrow$

Reasoning Layer $\mathcal{EL}_R$

$(t_1 : Attack)_{r_1}$

Result of rule $(\rightarrow)$ application and next step

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

$\Downarrow$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$
$t_2 : NonPhysicalSpeedTrans(23MB/s),$
$t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC$

$\Downarrow$

Reasoning Layer $\mathcal{EL}_R$

$(t_1 : Attack)_{r_1}$

- Apply rule $(\mathcal{L}'_1)$

Application of rule $\mathcal{L}'_1$

$$\frac{(t_1 : Attack)_{r_1}}{\mathcal{E} \cup \{(t_1 : Attack)\}} \mathcal{L}'_1$$

Result of the rewriting procedure

Evidence Layer $\mathcal{EL}_E$

$CS : (t_1 : Attack)\ [CS : (t_1 : SpPhish) \mid CS : (t_1 : SucPhish)]_{r_1}$
$TF : (t_2 : Attack)\ [TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$
$TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$
$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$
$t_2 : NonPhysicalSpeedTrans(23MB/s),$
$t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC$
$t_1 : Attack$

Reasoning Layer $\mathcal{EL}_R$

$(t_1 : Attack)_{r_1}$

Result of the rewriting procedure

- The forensics analyst has as result the following consistent set of pieces of evidence:

Interpretation Layer $\mathcal{EL}_I$

$t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,$
$t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,$
$t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA$
$t_2 : NonPhysicalSpeedTrans(23MB/s),$
$t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC$
$t_1 : Attack$

- $\mathcal{EL}$ Logic allows us to conclude that the *Attack* occurred at the instant of time t_1 (March-April 2016)

Conclusions

- We presented a formal representation for the pieces of evidence
- Our $\mathcal{EL}$ Logic captures the evidence source, reasoning and their level of trust
- We introduced a rewriting procedure that given the pieces of evidence:
  - Captures and solves factual and temporal discordancies
  - Gives a consistent set of pieces of evidence filtered using the relations of trust

Future Work

- Implementation and testing of the framework
- Enrichment with a reputation/belief revision process
- Integration of the framework with a trust reinforcement system
- Use Bayesian belief networks
- Work with probabilities for the pieces of evidence
- Incorporate within an Attribution Process

5 Algorithm Application

Algorithm Application

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply TRANS$\lhd$,TRANS $\prec$ rules **do** Apply TRANS$\lhd$, TRANS $\prec$ rules **end while**
2: **while** We can apply TRANS$\lhd$, TRANS $\prec$ rules **do**
3: Apply TRANS$\lhd$ and TRANS $\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Algorithm Application

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply TRANS$\lhd$,TRANS $\prec$ rules **do** Apply TRANS$\lhd$, TRANS $\prec$ rules **end while**
2: **while** We can apply TRANS$\lhd$, TRANS $\prec$ rules **do**
3: Apply TRANS$\lhd$ and TRANS $\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Transformation Rule Application

$$\frac{CS : (t_1 : Attack)\ [CS : (t_1 : SPhish) \mid CS : (t_1 : SucPhish)]_{r_1}}{\mathcal{E} \cup \{CS : (t_1 : SPhish), CS : (t_1 : SucPhish)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack\}}\ \mathcal{L}_2$$

$$\frac{TF : (t_2 : Attack)\ [(TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}}{\mathcal{E} \cup \{TF : (t_2 : MetaC)\} \cup \{t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack\}}\ \mathcal{L}_2$$

$$\frac{TF : (t_2 : PhysA)\ [TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}}{\mathcal{E} \cup \{TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))\} \cup \{t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}}\ \mathcal{L}_2$$

Algorithm Application II

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply TRANS$\lhd$,TRANS $\prec$ rules **do** Apply TRANS$\lhd$, TRANS $\prec$ rules **end while**
2: **while** We can apply TRANS$\lhd$, TRANS $\prec$ rules **do**
3: Apply TRANS$\lhd$ and TRANS $\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$\mathcal{E} \cup \{CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s)),\ TF : (t_2 : MetaC)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhis \rightarrow_{r_1} t_1 : Attack,\ t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,\ t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$$

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Algorithm Application II

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply TRANS$\lhd$,TRANS $\prec$ rules **do** Apply TRANS$\lhd$, TRANS $\prec$ rules **end while**
2: **while** We can apply TRANS$\lhd$, TRANS $\prec$ rules **do**
3: Apply TRANS$\lhd$ and TRANS $\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$\mathcal{E} \cup \{CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s)),\ TF : (t_2 : MetaC)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhis \rightarrow_{r_1} t_1 : Attack,\ t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,\ t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$$

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Elimination Rule $\mathcal{D}_2$

$$\frac{TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE \quad FE : (t_2 : NonPhysicalSpeedTrans(23MB/s)) \quad TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))}{\mathcal{E} \setminus \{TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))\}}\ \mathcal{D}_2$$

Algorithm Application III

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply $\text{TRANS}\lhd$,$\text{TRANS}\prec$ rules **do** Apply $\text{TRANS}\lhd$, $\text{TRANS}\prec$ rules **end while**
2: **while** We can apply $\text{TRANS}\lhd$, $\text{TRANS}\prec$ rules **do**
3: Apply $\text{TRANS}\lhd$ and $\text{TRANS}\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$\mathcal{E} \cup \{CS : (t_1 : SPhish),\ CS : (t_1 : SucPhish),\ TF : (t_2 : MetaC)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,\ t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,\ t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$$

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Transformation Rule

$$\frac{FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))}{\mathcal{E} \cup \{t_2 : NonPhysicalSpeedTrans(23MB/s)\}}\ \mathcal{L}_1$$

$$\frac{CS : (t_1 : SPhish)}{\mathcal{E} \cup \{t_1 : SPhish\}}\ \mathcal{L}_1 \qquad \frac{CS : (t_1 : SucPhish)}{\mathcal{E} \cup \{t_1 : SucPhish\}}\ \mathcal{L}_1$$

$$\frac{TF : (t_2 : MetaC)}{\mathcal{E} \cup \{t_2 : MetaC\}}\ \mathcal{L}_1$$

Algorithm Application IV

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply $\textsc{Trans}\lhd$,$\textsc{Trans}\prec$ rules **do** Apply $\textsc{Trans}\lhd$, $\textsc{Trans}\prec$ rules **end while**
2: **while** We can apply $\textsc{Trans}\lhd$, $\textsc{Trans}\prec$ rules **do**
3: Apply $\textsc{Trans}\lhd$ and $\textsc{Trans}\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\bot$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$\mathcal{E} \cup \{t_1 : SPhish,\ t_1 : SucPhish, t_2 : MetaC, t_2 : NonPhysicalSpeedTrans(23MB/s)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack, t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack, t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$$

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Algorithm Application IV

Algorithm 1 Algorithm for the Rewriting Procedure

1: **while** We can apply TRANS$\lhd$,TRANS $\prec$ rules **do** Apply TRANS$\lhd$, TRANS $\prec$ rules **end while**
2: **while** We can apply TRANS$\lhd$, TRANS $\prec$ rules **do**
3: Apply TRANS$\lhd$ and TRANS $\prec$ rules
4: **end while**
5: Apply $\mathcal{C}_T$ and $\mathcal{C}'_T$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
6: **while** We can apply $\mathcal{L}_2$ rule **do** Apply $\mathcal{L}_2$ rule **end while**
7: **while** We can apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **do** Apply $\mathcal{D}_1$, $\mathcal{D}_2$ rules **end while**
8: Apply $\mathcal{C}_C$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
9: **while** We can apply $\mathcal{L}_1$ rule **do** Apply $\mathcal{L}_1$ rule **end while**
10: **while** We can apply $(\rightarrow)$ rule **do** Apply $(\rightarrow)$ rule **end while**
11: **while** We can apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **do** Apply $\mathcal{D}'_1$, $\mathcal{D}'_2$ rules **end while**
12: **while** We can apply $(\rightarrow')$ rule **do** Apply $(\rightarrow')$ rule **end while**
13: **while** We can apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **do** Apply $\mathcal{D}''_1$, $\mathcal{D}''_2$ rules **end while**
14: Apply $\mathcal{C}'_C$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**
15: **while** We can apply $\mathcal{L}'_1$ rule **do** Apply $\mathcal{L}'_1$ rule **end while**
16: Apply $\mathcal{C}_P$; **if** we have $\perp$, **then** We do not have a model. Exit! **endif**

Pieces of Evidence

$$\mathcal{E} \cup \{t_1 : SPhish,\ t_1 : SucPhish,\ t_2 : MetaC,\ t_2 : NonPhysicalSpeedTrans(23MB/s)\} \cup \{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack,\ t_2 : MetaC \wedge t_2 : PhysA \rightarrow_{r_2} t_2 : Attack,\ t_2 : \neg NonPhysicalSpeedTrans(23MB/s) \rightarrow_{r_3} t_2 : PhysA\}$$

$$CS : (t_1 : Attack)[CS : (t_1 : SpPhish) \mid CS : (t_1 : (SucPhish)]_{r_1}$$

$$TF : (t_2 : Attack)[TF : (t_2 : MetaC) \mid TF : (t_2 : PhysA)]_{r_2}$$

$$TF : (t_2 : PhysA)[TF : (t_2 : \neg NonPhysicalSpeedTrans(23MB/s))]_{r_3}$$

$$FE : (t_2 : NonPhysicalSpeedTrans(23MB/s))$$

$$TF \lhd_{NonPhysicalSpeedTrans(23MB/s)} FE$$

Derivation of Derived Evidence

$$\frac{t_1 : SPhish \wedge t_1 : SucPhish \rightarrow_{r_1} t_1 : Attack \quad t_1 : SPhish \quad t_1 : SucPhish}{\mathcal{E} \cup \{(t_1 : Attack)_{r_1}\}} (\rightarrow)$$

$$\Downarrow$$

$$\frac{(t_1 : Attack)_{r_1}}{\mathcal{E} \cup \{(t_1 : Attack)\}} \mathcal{L}'_1$$