Argumentation-Based Security for Social Good

Erisa Karafili

Imperial College London

April 25, 2018

Erisa Karafili, Antonis C. Kakas, Nikolaos I. Spanoudakis, Emil C. Lupu

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

Agenda

1. Introduction
2. Secure Data Sharing with Argumentation
3. Attribution Problem in Cyber Attacks
4. Conclusions

Imperial College London

1. Introduction
2. Secure Data Sharing with Argumentation
3. Attribution Problem in Cyber Attacks
4. Conclusions

Introduction to the Solution

- Two important problems in "social context"
- They can both be seen as decision making problems
- Argumentation reasoning solves problems under partial, conflicting and context dependent knowledge
- Our solution captures different types of conflicts
- We introduce a conflict resolution procedure via priorities between rules

1 Introduction

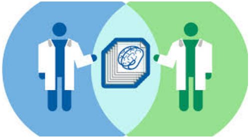
2 Secure Data Sharing with Argumentation

3 Attribution Problem in Cyber Attacks

4 Conclusions

Data Sharing

- Data services are increasing in popularity
- They enable service optimisation and personalisation
- The necessity to protect and ensure the security properties of the data



Imperial College London

Data Sharing Agreements

- Different entities are involved during the sharing of data
- A data sharing agreement is made between the involved entities
  - Data security requirements
  - User preferences
  - Business rules
  - Legislation rules

Challenges:

- Difficult to represent these agreements
- The agreements are applied to the same data in different contextual environment
- The rules of the agreements can create conflicts or not be efficient

Secure Data Sharing with Argumentation

Solution

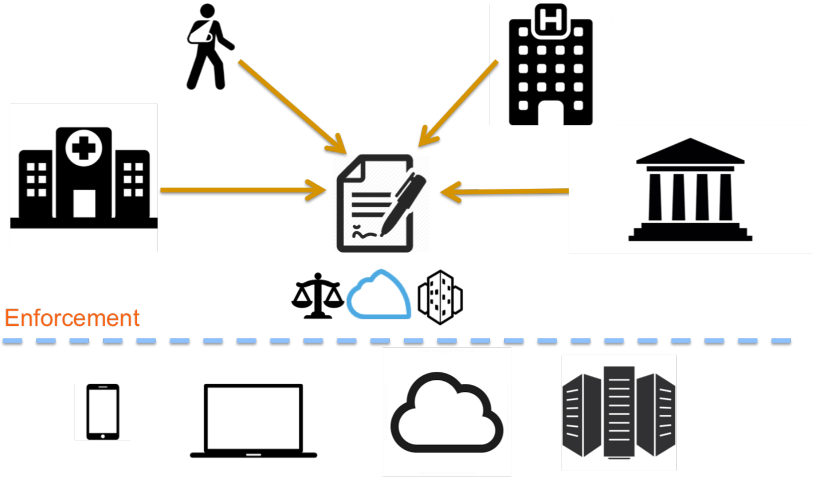
A technique based on a policy language and argumentation reasoning for representing and analysing data sharing agreements

Contributions:

- Representation of the rules through arguments
- Efficiency and consistency analysis
- Solve the conflicts by introducing priorities between rules
- An automated decision process decides how and who can access/share/use the data
- The decision process is made using the GorgiasB tool[1]

[1] http://gorgiasb.tuc.gr/

An E-Health Example: Coco Cloud



http://www.coco-cloud.eu/

DSAs Rules and their Representation

DSAs Rules and their Representation

Some of the rules included in the DSAs:

(1) The patient can access her/his data

$Access(Data, Patient, Permitted) \leftarrow Owner(Patient, Data)$

DSAs Rules and their Representation

Some of the rules included in the DSAs:

(1) The patient can access her/his data

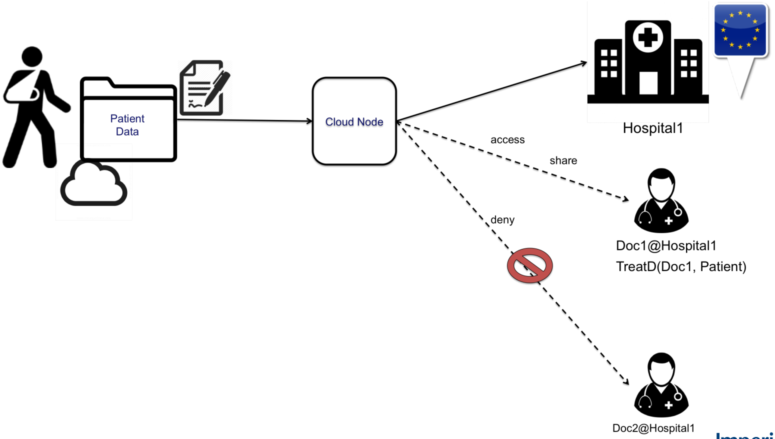
(2) The treating doctor can access the patient's data, when s/he is inside the hospital and during her/his shift

$$
\begin{aligned}
Access(Data, Doctor, Permitted) \leftarrow \quad & TreatD(Doctor, Patient) \wedge \\
& Owner(Patient, Data) \wedge \\
& shift(D) \wedge hospP(H, L_2) \wedge \\
& position(Doctor, L_1) \wedge \\
& same(L_1, L_2)
\end{aligned}
$$

Imperial College London

DSAs Rules and their Representation

(2) The treating doctor can access the patient's data, when s/he is inside the hospital and during her/his shift



DSAs Rules and their Representation

Some of the rules included in the DSAs:

(1) The patient can access her/his data

(2) The treating doctor can access the patient's data, when s/he is inside the hospital and during her/his shift

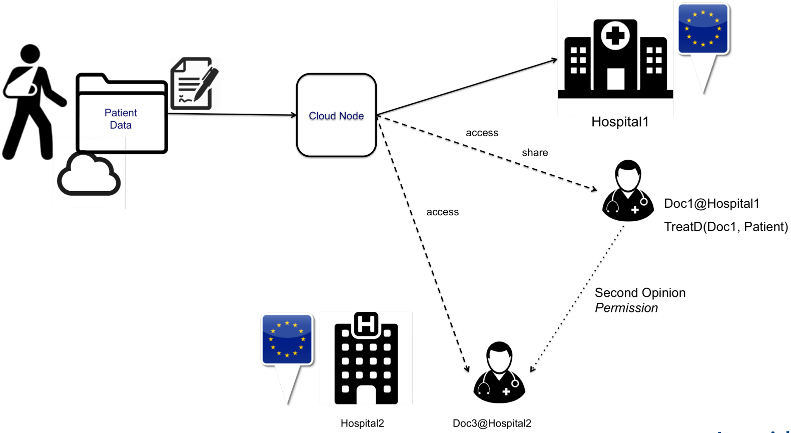
(3) The data can be shared inside the EU/EEA, e.g., a second opinion

$$\begin{aligned} Access(Data, Doctor, Permitted) \leftarrow \quad & Owner(Patient, Data) \wedge \\ & TDoc(D_1, Patient) \wedge \\ & SecondOp(D_1, Doctor) \wedge \\ & Work(Doctor, H) \wedge EU^*(H) \end{aligned}$$

Imperial College London

DSAs Rules and their Representation

(3) The data can be shared inside the EU/EEA, e.g., a second opinion



Imperial College London

DSAs Rules and their Representation

Some of the rules included in the DSAs:

(1) The patient can access her/his data

(2) The treating doctor can access the patient's data, when s/he is inside the hospital and during her/his shift

(3) The data can be shared inside the EU/EEA, e.g., a second opinion

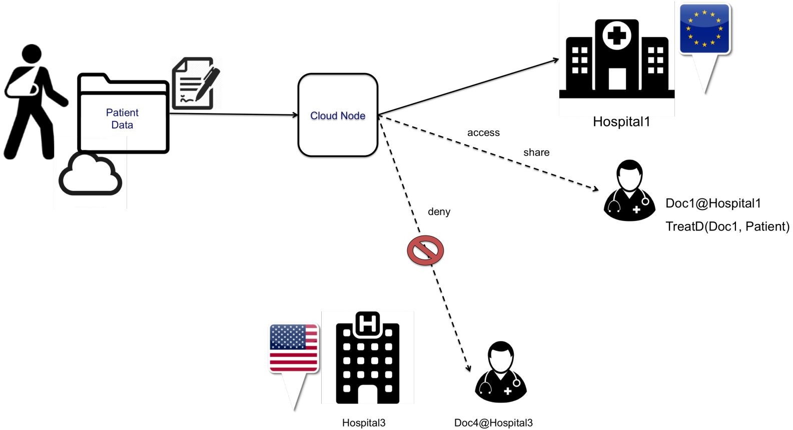
(4) The data cannot be shared outside EU or EEA

$$\begin{aligned} Access(Data, Doctor, Denied) \leftarrow \; & Owner(Patient, Data) \wedge \\ & Work(Doctor, H) \wedge \\ & not \;\; EU^{*}(H) \end{aligned}$$

Imperial College London

DSAs Rules and their Representation

(4) The data cannot be shared outside EU or EEA



Imperial College London

Conflicting Rules

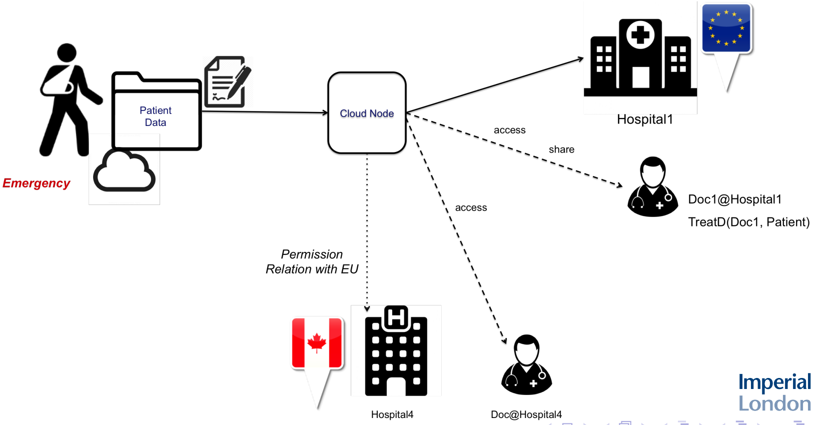
(5) In case, the patient is in an emergency not in an EU/EEA country, then part of his data can be shared with an entity of that country, if that country has legal agreements for cross borders flow of information with EU

$$\begin{aligned} Access(Data, Doctor, Permitted) \leftarrow \; & Emergency(Patient, H) \wedge \\ & Owner(Patient, Data) \wedge \\ & Work(Doctor, H) \wedge \\ & \textbf{not } EU^{*}(H) \wedge Agreement(H) \end{aligned}$$

Imperial College London

Conflicting Rules

(5) In case, the patient is in an emergency not in an EU/EEA country, then part of his data can be shared with an entity of that country, if that country has legal agreements for cross borders flow of information with EU



Conflicting Rules

(5) In case, the patient is in an emergency not in an EU/EEA country, then part of his data can be shared with an entity of that country, if that country has legal agreements for cross borders flow of information with EU

$$\begin{aligned} Access(Data, Doctor, Permitted) \leftarrow\ & Emergency(Patient, H) \wedge \\ & Owner(Patient, Data) \wedge \\ & Work(Doctor, H) \wedge \\ & \textbf{not } EU^{*}(H) \wedge Agreement(H) \end{aligned}$$

- The introduced policy analysis is able to find the conflict between rules (4) and (5)
- The argumentation based decision process solves this conflict by introducing a priority between the rules

$$(5) > (4)$$

Imperial College London

1. Introduction

2. Secure Data Sharing with Argumentation

3. **Attribution Problem in Cyber Attacks**

4. Conclusions

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 minutes, 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)

Imperial College London

The Attribution Problem

Attribution in cyber attacks is the process of assigning an action to a particular actor/entity/country

Problem

Given evidence of an attack, decide who did/performed/instigated the attack

- Forensics helps in the attribution process
- The evidence is incomplete and/or conflicting

Solution

A methodology based on argumentation reasoning and social science techniques

Imperial College London

Attribution in Cyber Attacks

- We propose a methodology based on Adbuctive and Argumentation reasoning
- The attribution reasoner is based on logical rules
- The knowledge based is structured through a Social Science model (Q-model)
- Implementing *physical* as well as *social attribution*

Imperial College London

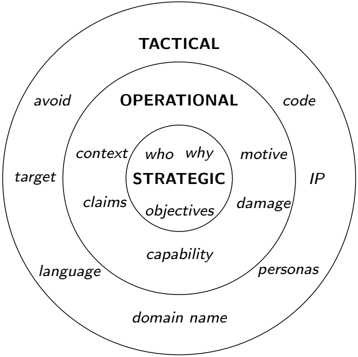
Attribution through Argumentation

- Pieces of evidence are represented as facts and defeasible knowledge
- The rules are defined as arguments for certain conclusions
- Hierarchies are introduced between arguments
- The reasoner decides the winning argument
- The reasoner is implemented using tools for preference-based argumentation
- An explanation is provided for the given attribution

Imperial College London

Attribution with Argumentation and Social Science

- The evidence is categorised and analysed following a social science approach
- The reasoner can answer if a given entity performed the attack



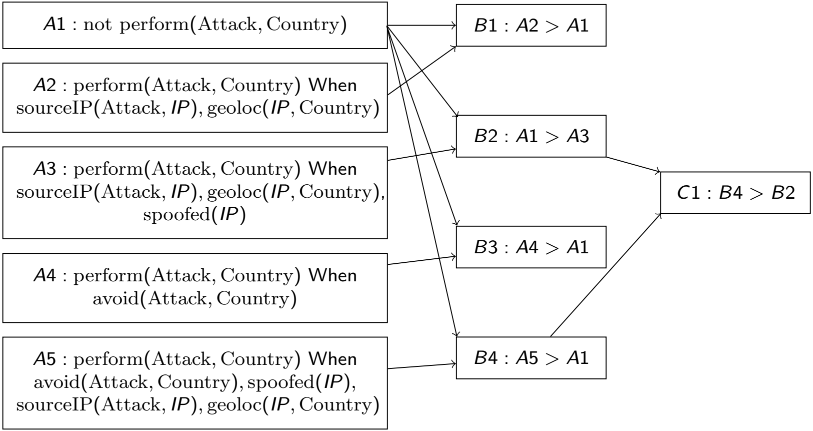
An example of Attribution in Cyber Attack

- HIDS logs check: SSH brute force/dictionary attack
- Firewalls logs check: IP's sources of the attack
  - Geolocation of the IP's

- IP's spoofed, that country did not performed the attack
- The attack is designed to avoid a certain country, then that country performed the attack

Imperial College London

Decision Diagram for the Attribution example



$A1 : \text{not perform}(\text{Attack}, \text{Country})$

$A2 : \text{perform}(\text{Attack}, \text{Country})$ When $\text{sourceIP}(\text{Attack}, IP), \text{geoloc}(IP, \text{Country})$

$A3 : \text{perform}(\text{Attack}, \text{Country})$ When $\text{sourceIP}(\text{Attack}, IP), \text{geoloc}(IP, \text{Country}), \text{spoofed}(IP)$

$A4 : \text{perform}(\text{Attack}, \text{Country})$ When $\text{avoid}(\text{Attack}, \text{Country})$

$A5 : \text{perform}(\text{Attack}, \text{Country})$ When $\text{avoid}(\text{Attack}, \text{Country}), \text{spoofed}(IP), \text{sourceIP}(\text{Attack}, IP), \text{geoloc}(IP, \text{Country})$

$B1 : A2 > A1$

$B2 : A1 > A3$

$B3 : A4 > A1$

$B4 : A5 > A1$

$C1 : B4 > B2$

Further Reasoning Rules and Priorities

Consider complex examples of attacks, where social attribution is involved

- Language(Attack, Country)
- Motive(Attack, Country)
- Capable(Attack, Country)
- Target(Attack, Country)

1 Introduction

2 Secure Data Sharing with Argumentation

3 Attribution Problem in Cyber Attacks

4 Conclusions

Imperial College
London

Conclusions

- We presented a solution for
  - Regulatory data sharing
  - Cyber attack attribution
- The solution is based on argumentation reasoning
- Decision making mechanism under incomplete, conflicting and context dependent information

Ongoing and Future Work

Ongoing Work:

- Collect and categorise the various pieces of evidence
- Extract the reasoning rules applied in various use cases
- Construct and enrich the reasoner
- Extend the attribution solution to guide the analysts during evidence collection/analysis

Future Work:

- Quantitative arguments strength
- Construct a Logical Framework for Attribution
- Work on human cognitive reasoning for the social evidence
- Fully automate the conflict resolution process

Imperial College London

Questions?

e.karafili@imperial.ac.uk

http://www.imperial.ac.uk/people/e.karafili

http://rissgroup.org/

RISS

Imperial College
London

References

1. Erisa Karafili, Antonis C. Kakas, Nikolaos I. Spanoudakis, Emil C. Lupu “Argumentation-based Security for Social Good” in *AAAI 2017 Fall Symposium Series*, 164-170, 2017.
2. Erisa Karafili, Emil C. Lupu “Enabling Data Sharing in Contextual Environments: Policy Representation and Analysis” in SACMAT 2017, 231-238, 2017.
3. Erisa Karafili, Konstantina Spanaki, Emil C. Lupu “An argumentation reasoning approach for data processing” in *Journal of Computers in Industry*, Elsevier, Volume 94, 52-61, 2018.
4. Thomas Rid, Ben Buchanan “Attributing cyber attacks” in *Journal of Strategic Studies*, 38(1-2):4–37, 2015.

Imperial College London