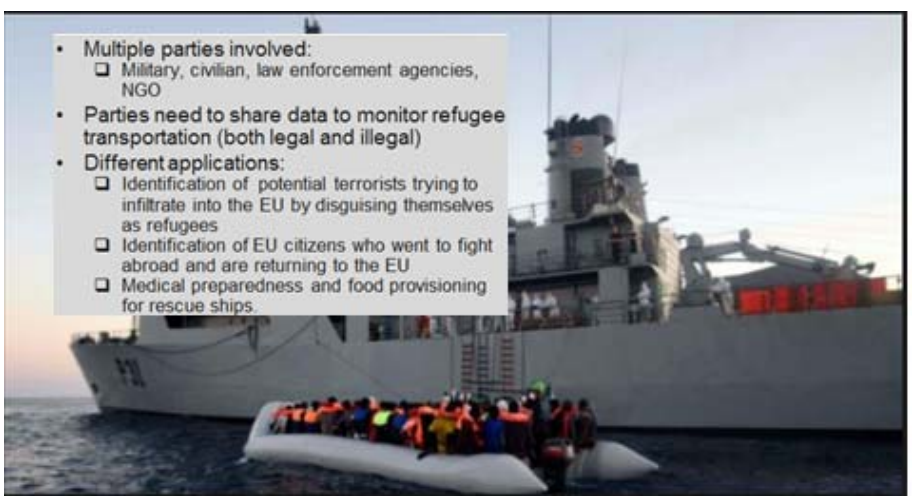
A Policy System for Control of Data Fusion Processes and Derived Data

Elisa Bertino (Purdue University), **Dinesh Verma** (IBM TJ Watson Research Ctr.), **Seraphin Calo** (IBM TJ Watson Research Ctr.)

The use of datasets for fusion processes must be governed by policy systems to ensure data security and privacy

Scenario

Rescue and Transportation Operations Across the Mediterranean Sea



Requirements

1) Data fusion may be constrained based on the content of the data; that is, whether a dataset (portion of a dataset) may be provided for a fusion task to a given subject depends on the content of the dataset (portion of it).

2) Data fusion may be executed only by subjects with specific roles an attributes.

3) Data fusion may have to be privacy-preserving with respect to its input.

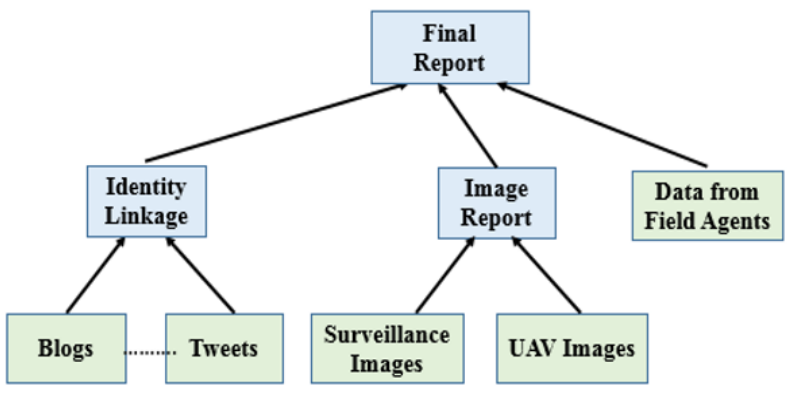
4) Results of data fusion may be made available to subjects based on their roles and attributes.

5) Data fusion may be constrained based on the source of data.

6) Data provided as input to fusion steps may have to be aggregated and sanitized.

Fusion Processes

Represented as trees



Policy Model

- **Three Domains:**
  - *Access Control Policies* (Basic, SoD, BoD)
  - *Fusion Policies* (data separation, pre-processing)
  - *Derived Data Control Policies*
- **Applicability Scope:** global, local
- **Support for Exceptions:** strong, weak
- **Attribute-based:** it uses
  - *Roles* to characterize the subjects
  - *Types* to characterize the protected resources
  - Attributes for roles and types are defined by *metadata templates*

Access Control Policies Informal Grammar

Definition. (**Basic access control policy**). An access control policy P is an expression of the form:

P = < **weak** | **strong**, Scp, S, D, A>
Scp = **global** | **local** {i_1 [i_2,…, i_n]}
S = r [{pr}]
D = ot [{d_pr}]
pr = $attr$ ϕ v | pr ∧ pr | pr ∨ pr | ¬pr
d_pr = pr | c_cnd
A = **read** | **write** | **execute** ◊

A policy specifying that analysts from an EU country can read the passenger list:
< **strong**, **local**{*i*}, analyst {country ∈ {EU}}, pass_list, **read** >

A policy specifying that analysts from country *A* can only read the list of passengers who are citizens of *A*:
< **strong**, **local**{*i*}, analyst {country = A },
pass_list {Select * From pass_list Where citizenship = A}, **read** >.

Fusion Policies Informal Grammar

Definition. (**Fusion policy**). A fusion policy P is an expression of the form:

P = < **weak** | **strong**, Scp, DS | SN | **mc** {is_i, D,D} | E(is_i) >
Scp = **global** | **local** {i_1 [i_2,…… i_n]}
DS = {D, D}
SN = **anom** | **diffpriv** | **encr** (D)
D = ot [{d_pr}]
d_pr = pr | c_cnd
pr = $attr$ ϕ v | pr ∧ pr | pr ∨ pr | ¬pr
E = **trustenv** | **enclave** ◊

A policy specifying that the fusion must be executed according to a multi-party protocol:
< **strong**, **local**{*i*}, **mc** {*is*, pass_list {Select * From pass_list Where citizenship = A}, fighter_list} >

Policy Enforcement Challenges

- to automatically determine the technologies to use based on the policies and which fusion tasks must be executed on which platform/environment
- to ensure that policies do not conflict and their enforcement is feasible

Distributed Analytics and Information Science International Technology Alliance
Annual Fall Meeting, September 2018