

► **Towards a Security Reference Architecture  
for Big Data**

Julio Moreno, Manuel A. Serrano,  
Eduardo Fernández-Medina, Eduardo B. Fernandez

University of Castilla-La Mancha  
Escuela Superior de Informática  
Ciudad Real




Real Madrid vs Barcelona • Analysing the strengths and weaknesses

# Big Data of "El Clasico": Real Madrid vulnerable down the middle, Barcelona down the right

Lorenzo Lara | Madrid

22/12/2017 | 17:06 CEST   

 En Español



• 38 unforgettable images from past Clasicos

A game decided by some of the most memorable moments Spanish football can produce, **El Clasico** comes around again on Saturday afternoon with both

3



4





### Objectives

- Data analysis ✓
- Manage huge amount of data ✓



### Objectives

- Data analysis ✓
- Manage huge amount of data ✓
- Near real-time processing ✓





### Objectives

- Data analysis ✓
- Manage huge amount of data ✓
- Near real-time processing ✓
- Manage unstructured and semi-structured data ✓

9



### Objectives

- Data analysis ✓
- Manage huge amount of data ✓
- Near real-time processing ✓
- Manage unstructured and semi-structured data ✓

... and **security?** ✗

10



11



12



**Loss of  
Reputation**



**Financial  
Penalties**

13



**Standards and Methodologies**

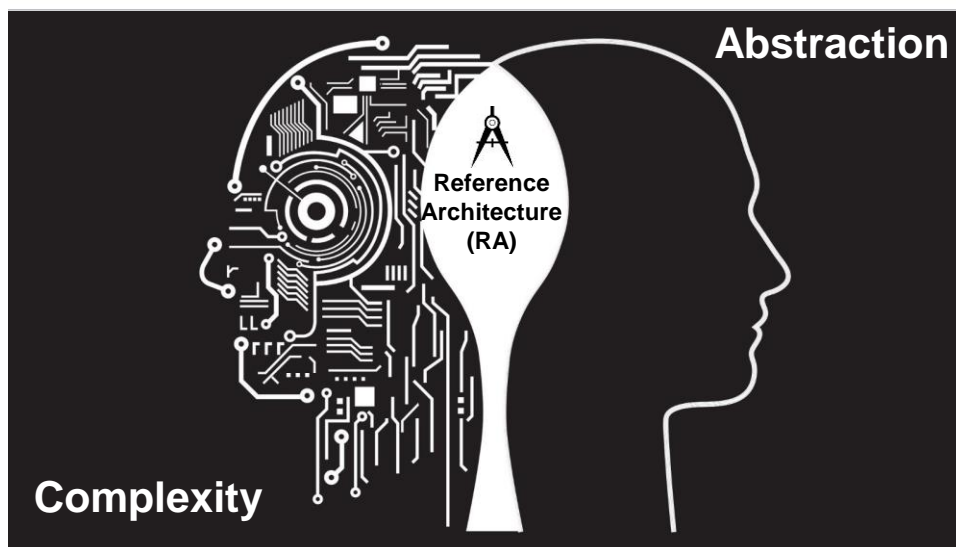
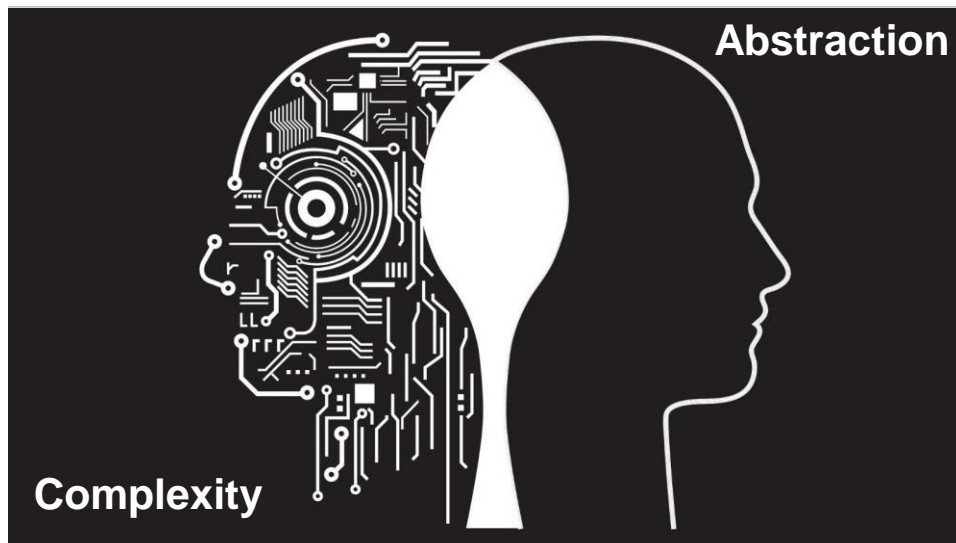


**Loss of  
Reputation**

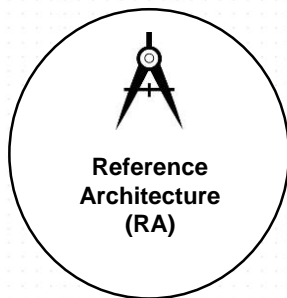


**Financial  
Penalties**

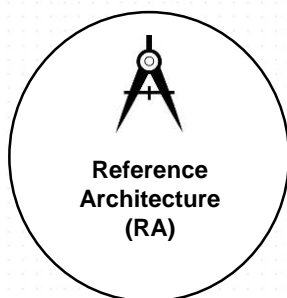
14





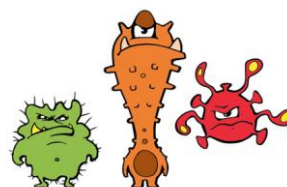
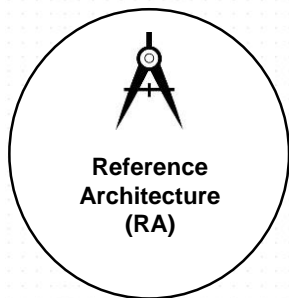


17



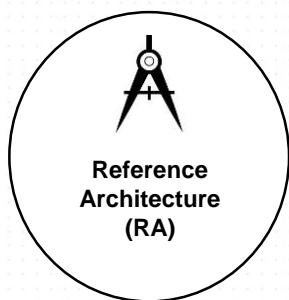
- An abstract SW architecture based on one or more domains

18

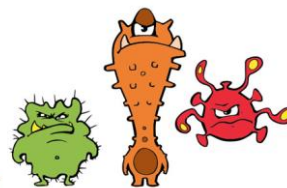


Threats

19



Security  
Pattern

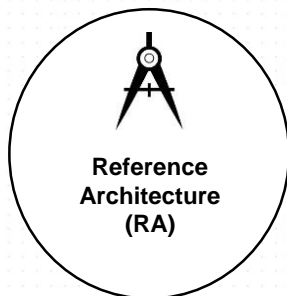


Threats

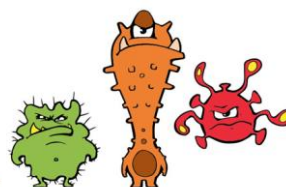
20



### Security Reference Architecture (SRA)



Security  
Pattern

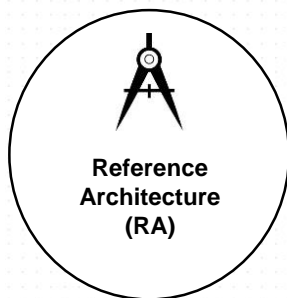


Threats

21



### Security Reference Architecture (SRA)



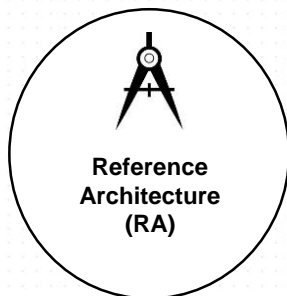
Security  
Pattern

- Facilitates the **definition** and **implementation** of security requirements

22



### Security Reference Architecture (SRA)



Security  
Pattern

- Facilitates the **definition** and **implementation** of security requirements
- Allows a **better understanding** of concepts like security policies or vulnerabilities

23



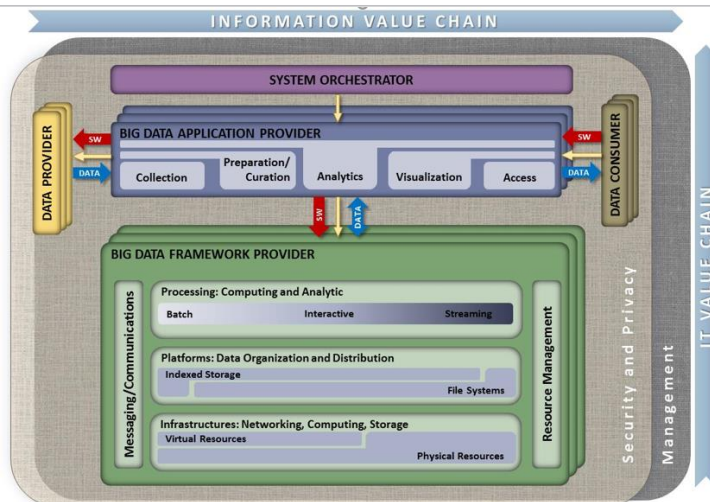
### SRA for Big Data

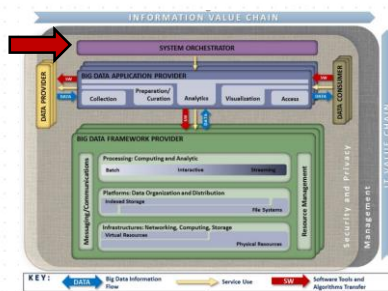


24



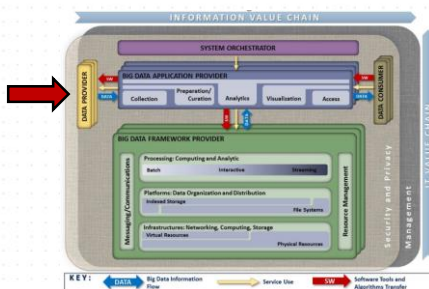
NIST Big Data Reference Architecture (NBDRA)





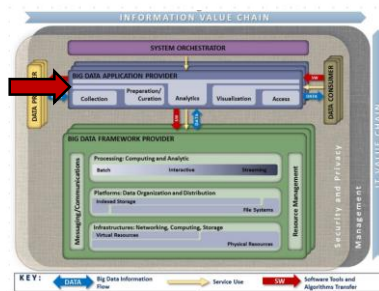
- Defining and integrating the required **data application activities** into the ecosystem
- **Configuring and managing** the other components of the Big Data architecture
- **Monitoring** the system and requirements

27



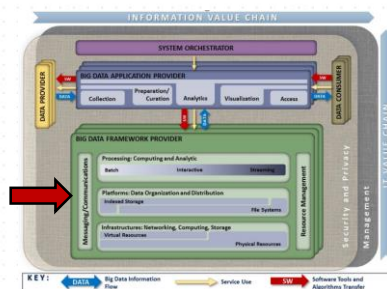
- Introduces new data that **feeds** into the Big Data ecosystem
- It creates an **abstraction of the data sources**
- It has a collection of **interfaces** that acts like gates

28



- Provides a **set of services** along data life cycle to meet the requirements
- Purpose: to **encapsulate** the business logic and functionality to be executed by the architecture
- Divided in **activities**: collection, preparation, analysis, visualization, and access.

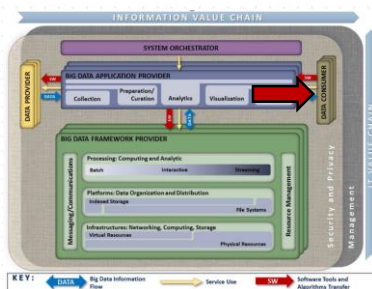
29



- The implementation of the **Big Data logic**
- **Support** the activities of the BDAP
- Also provides the **support services** for the system, like communications.

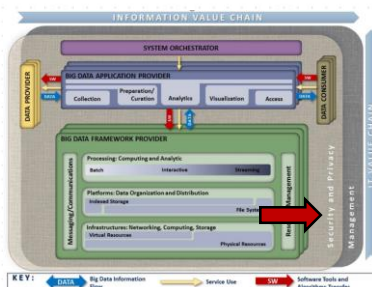
30





- Similar to Data Provider
- The interaction could include **interactive visualization or creating reports** by using business intelligence functions

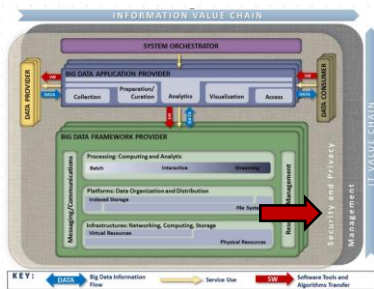
31



- NIST proposal **cannot be considered** as a SRA, but it recognizes the importance of security
- The representation in **blocks** is not expressive enough. It provides little emphasis on how the subcomponents are **connected**
- It can be difficult to **design and implement** a Big Data ecosystem

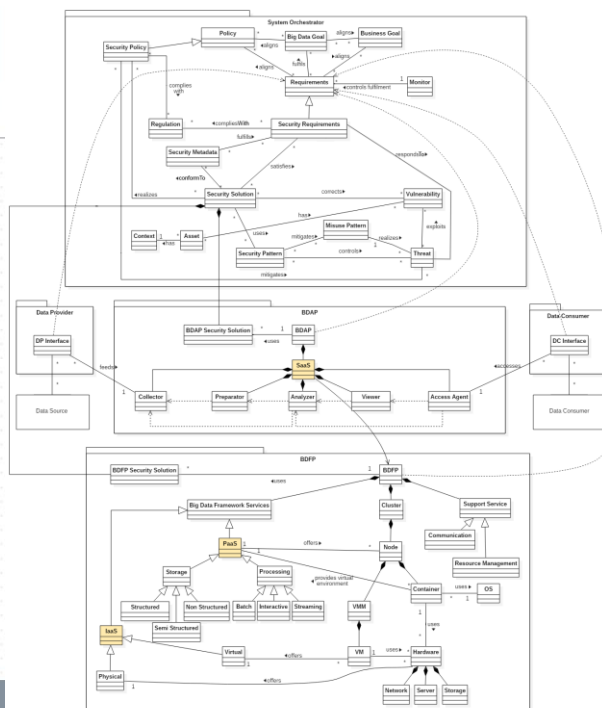
32

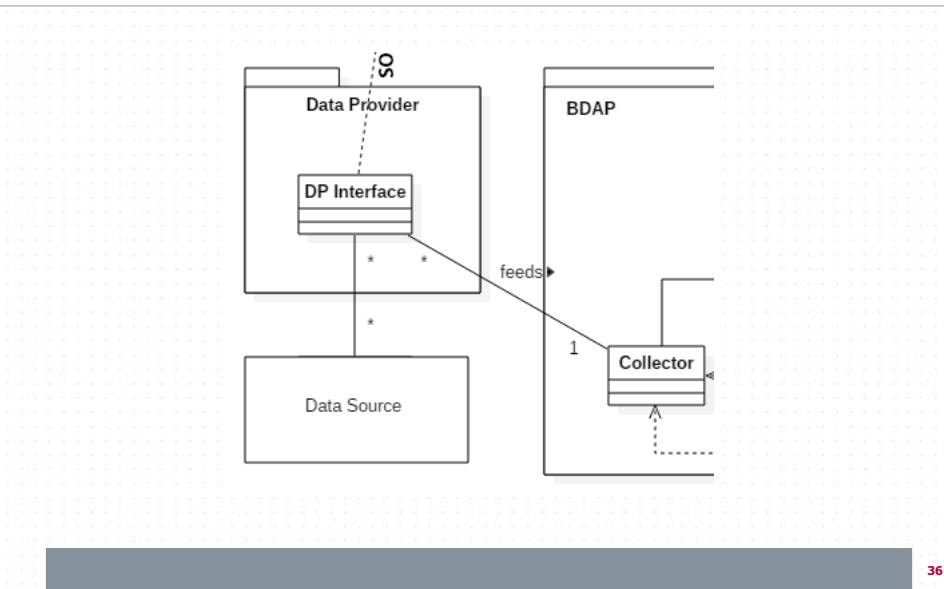
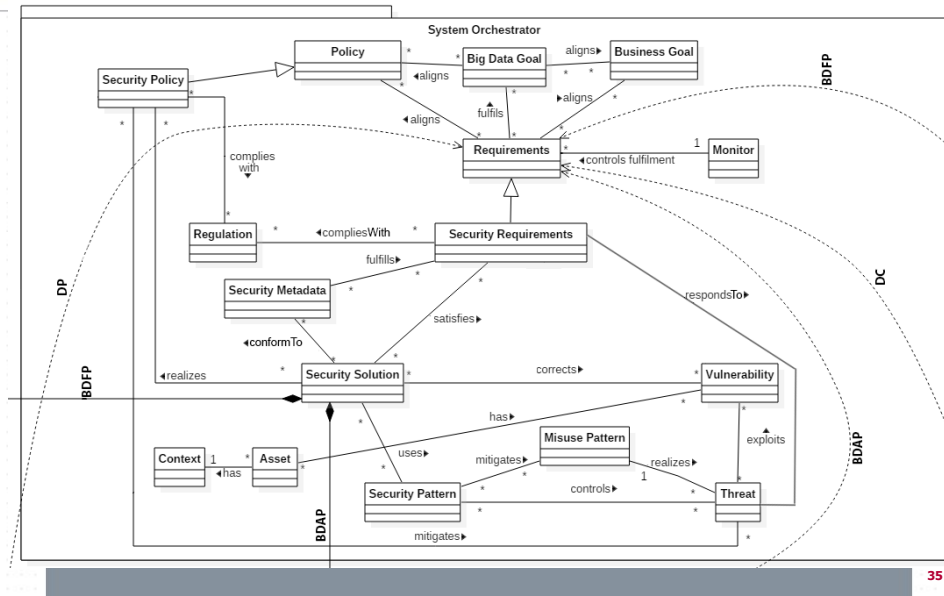


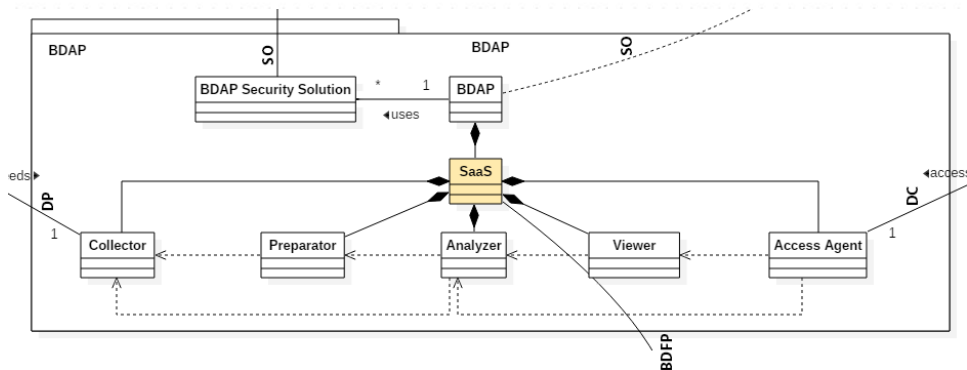


- NIST proposal **cannot be considered** as a SRA, but it recognizes the importance of security
- The representation in **blocks** is not expressive enough. It provides little emphasis on how the subcomponents are **connected**
- It can be difficult to **design and implement** a Big Data ecosystem

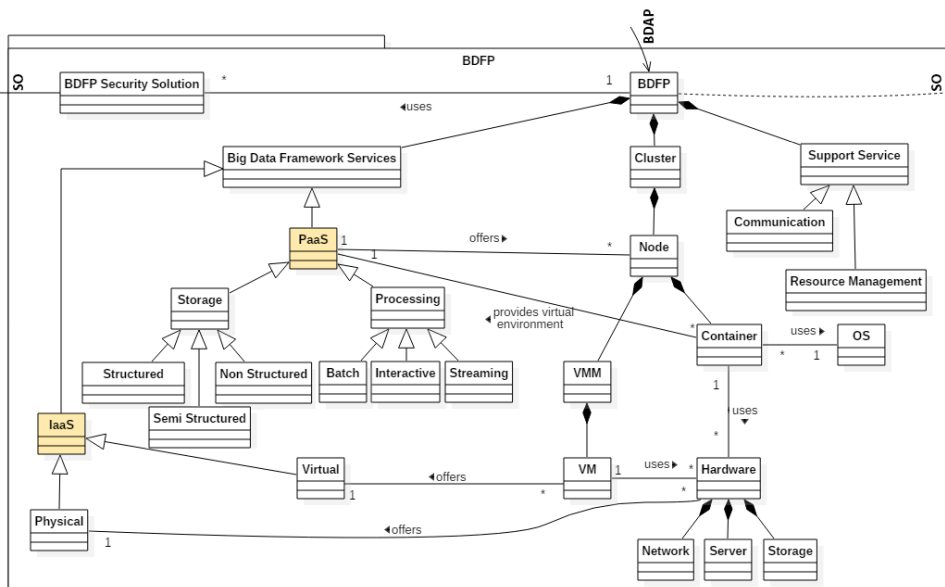
**Security Reference Architecture for Big Data (SRA)**

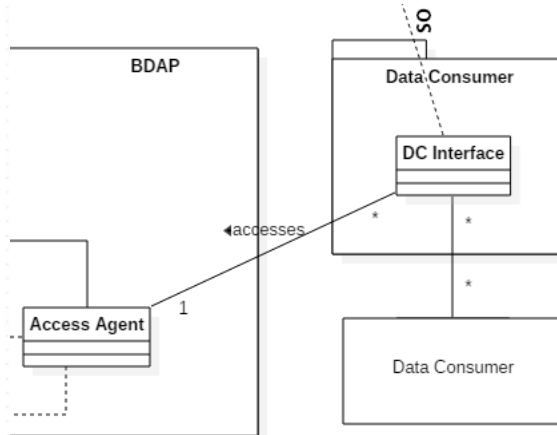






37





Security  
Pattern



**Security  
Pattern**



**Data  
Modification**



**Authentication\***

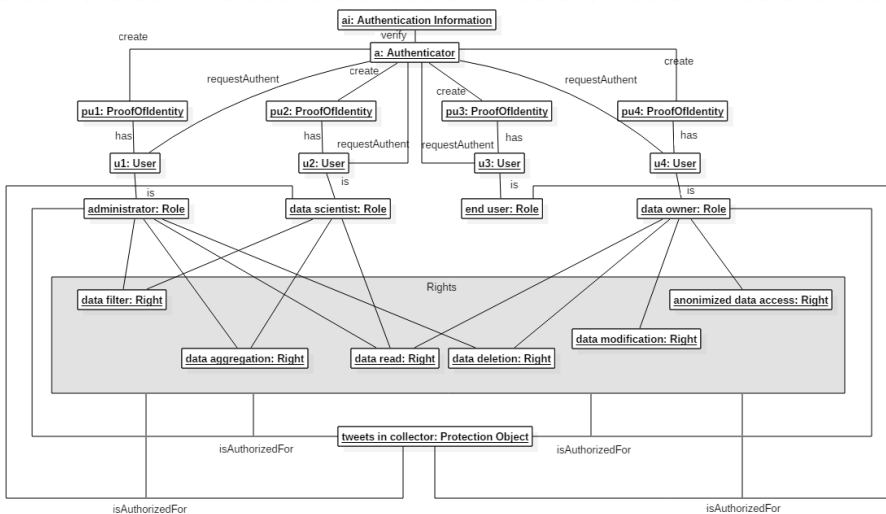
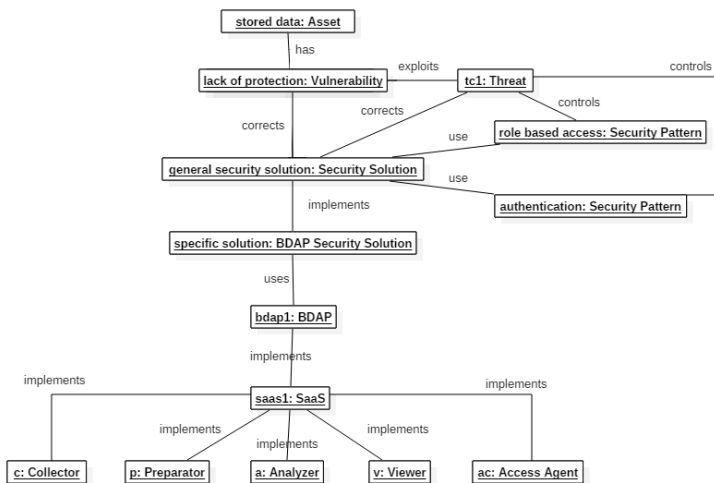


**Role-based  
Access Control\***



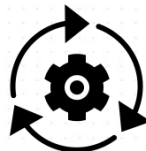
**Data  
Modification**

*\*Defined in: Eduardo B. Fernandez. 2013. Security patterns in practice: designing secure architectures using software patterns. John Wiley & Sons.*





UML diagrams



Facilitate secure  
implementation



Ease the  
application of  
security patterns

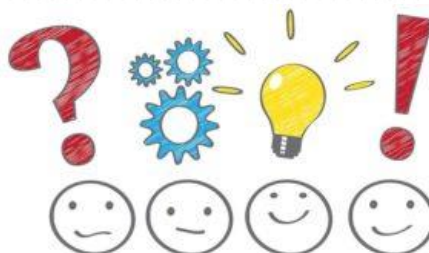


Identify  
threats



Creation and  
adaptation of  
security patterns





- Contact

[Julio.Moreno@uclm.es](mailto:Julio.Moreno@uclm.es)

[Manuel.Serrano@uclm.es](mailto:Manuel.Serrano@uclm.es)

[Eduardo.FdezMedina@uclm.es](mailto:Eduardo.FdezMedina@uclm.es)

[Fernande@fau.edu](mailto:Fernande@fau.edu)

47



RA	Pro- posal	Requirements concern	Security con- cern	Connection between compo- nents	Abstraction level
NIST		Medium	High	Low	High
Demchenko		Medium	Low	Medium	Medium
Klein		Low	Medium	Medium	Low
Pääkkönen and Pakkala		Medium	Low	High	Medium
SRA	Pro- posal	High	High	High	Medium

Comparison between RAs