

Towards an integrated formal analysis for security and trust

Fabio Martinelli

Institute of Informatics and Telematics

National Research Council of Italy

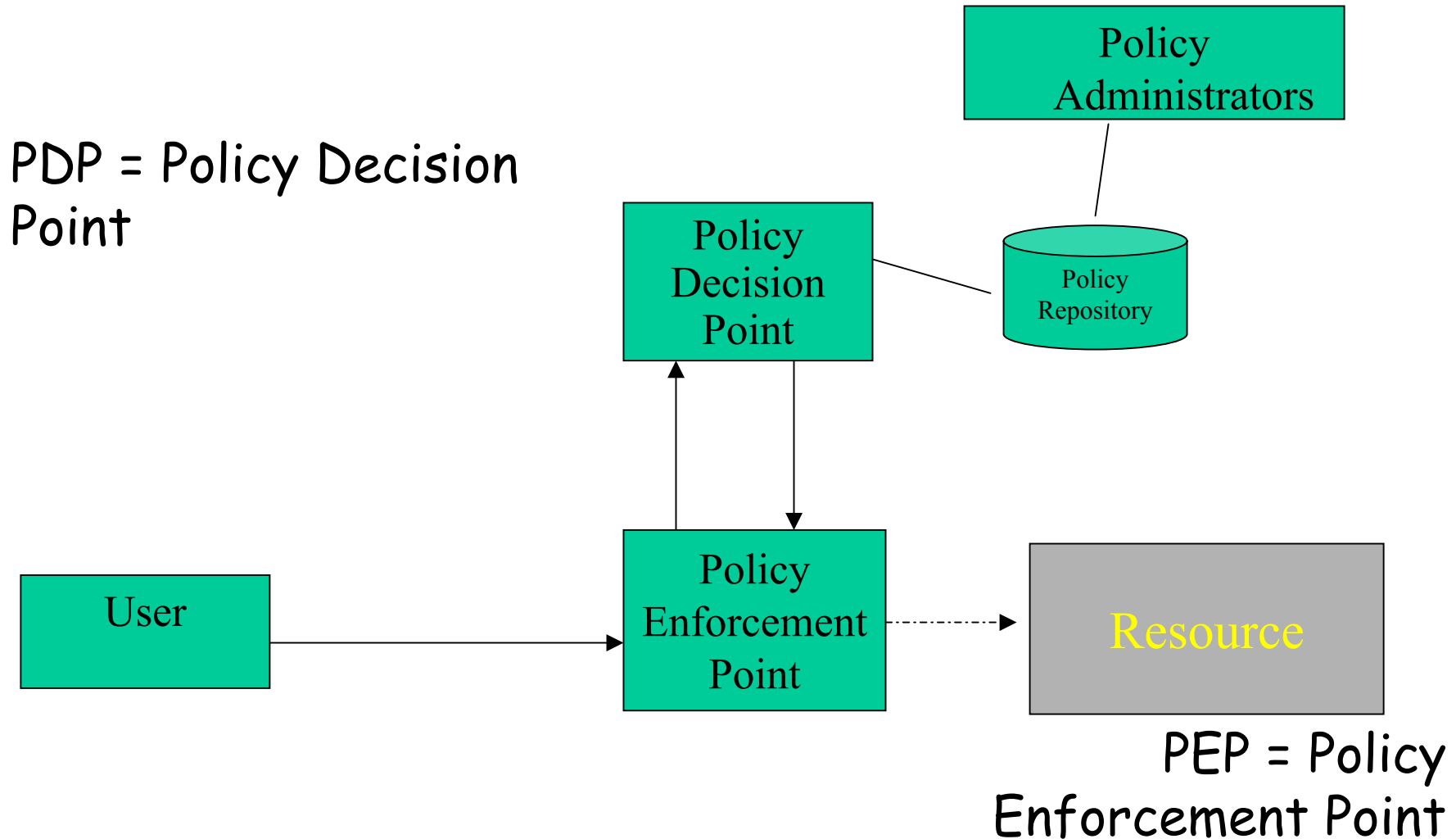
(IIT-CNR)

Pisa - Italy

Security protocols and access control

- Security protocols are usually analyzed with different techniques w.r.t. access control
 - Security protocols
 - Computational proof methods
 - Formal language/logic methods
 - Access control
 - Access matrix/Graph analysis
 - Logic: first order, datalog, etc..

A (simple) AAA scenario



Credentials-based access control

- Security protocols use credentials
 - Analysis usually does not consider the steps when one acquires such credentials
 - Security protocols produce credentials
 - Current analysis methods deal with credentials in the form of cryptographic messages
- Forms of access control use credentials
 - Credential based-access control
 - For authentication $\{\text{principal, role}\}_{\text{issuer}}$
 - For authorization $\{\text{role, permission}\}_{\text{issuer}}$

Principals \longleftrightarrow Roles \longleftrightarrow Permissions

CryptoCCS [Martinelli, ICTCS'98]

- CCS-like process algebra with inference rules:
 - $a.P$ action (send/receive)
 - $P|P$ parallel composition of processes
 - $[m_1 \dots m_n \mid - x]P$ inference rule
 - ...

- Inference rules :
$$\frac{\text{premises}}{\text{conclusion}}$$

$$\frac{m \quad k}{E(m, k)} \text{ (encryption)}$$

$$\frac{E(m, k)}{m} \quad k \text{ (decryption)}$$

Languages RT_0 (Role-based Trust Management) [Li et. al 2002-]

- A family of languages for reasoning about trust relationships in distributed environments
 - A, B, C, D, ... entities
 - r roles/attributes
- Rules:
 - $A.r \leftarrow D$ means D has role r for A
 - $A.r \leftarrow B.r_1$ means if C has role r_1 for B then C has role r for A
 - $A.r \leftarrow A.r_1.r_2$, means if B has role r_1 for A and if C has role r_2 for B then C has role r for A
 - $A.r \leftarrow A_1.r_1 \& A_2.r_2$ if B has role r_1 for A_1 & R_2 for A_2 then B has role r for A

RT₀ and inference rules

$$A.r \leftarrow D$$

$$\{D, r\}_A$$

$$A.r \leftarrow B.r_1$$

$$\frac{\{y, r_1\}_B}{\{y, r\}_A}$$

link

$$A.r \leftarrow A.r_1.r_2$$

$$\frac{\{y, r_2\}_t \quad \{t, r_1\}_A}{\{y, r\}_A}$$

$$A.r \leftarrow A_1.r_2 \& A_2.r_2$$

$$\frac{\{y, r_1\}_{A_1} \quad \{y, r_2\}_{A_2}}{\{y, r\}_A}$$

- Projects:

- Model-based Design/Verification for Web Services (MbDV4WS) – 2004/2005 - funded by CSP
 - Modeling of security/trust aspects through process algebras
- Trusted e-services for Dynamic Coalitions – 2004/2005 - funded by CNR
 - Web/GRID services
 - Mobile ad hoc networks (MANETs)
 - Multi-agents Systems (MAS)

- Events:

- 2nd International Workshop on Formal Aspects in Security&Trust FAST2004 – Toulouse France 26-27 August 2004
 - Affiliated with 18th IFIP World Computer Congress (WCC04)
 - Sponsored by IFIP WG 1.7
 - Deadline: 18 June 2004
 - Special issue on International Journal of Information Security (IJIS)