

A Policy Based Architecture for NSA RAdAC Model

Dr. A. Rahim Choudhary

703-234-6961, Rahim.Choudhary@SI-INTL.com

6th IEEE IA Workshop, USMA, Westpoint

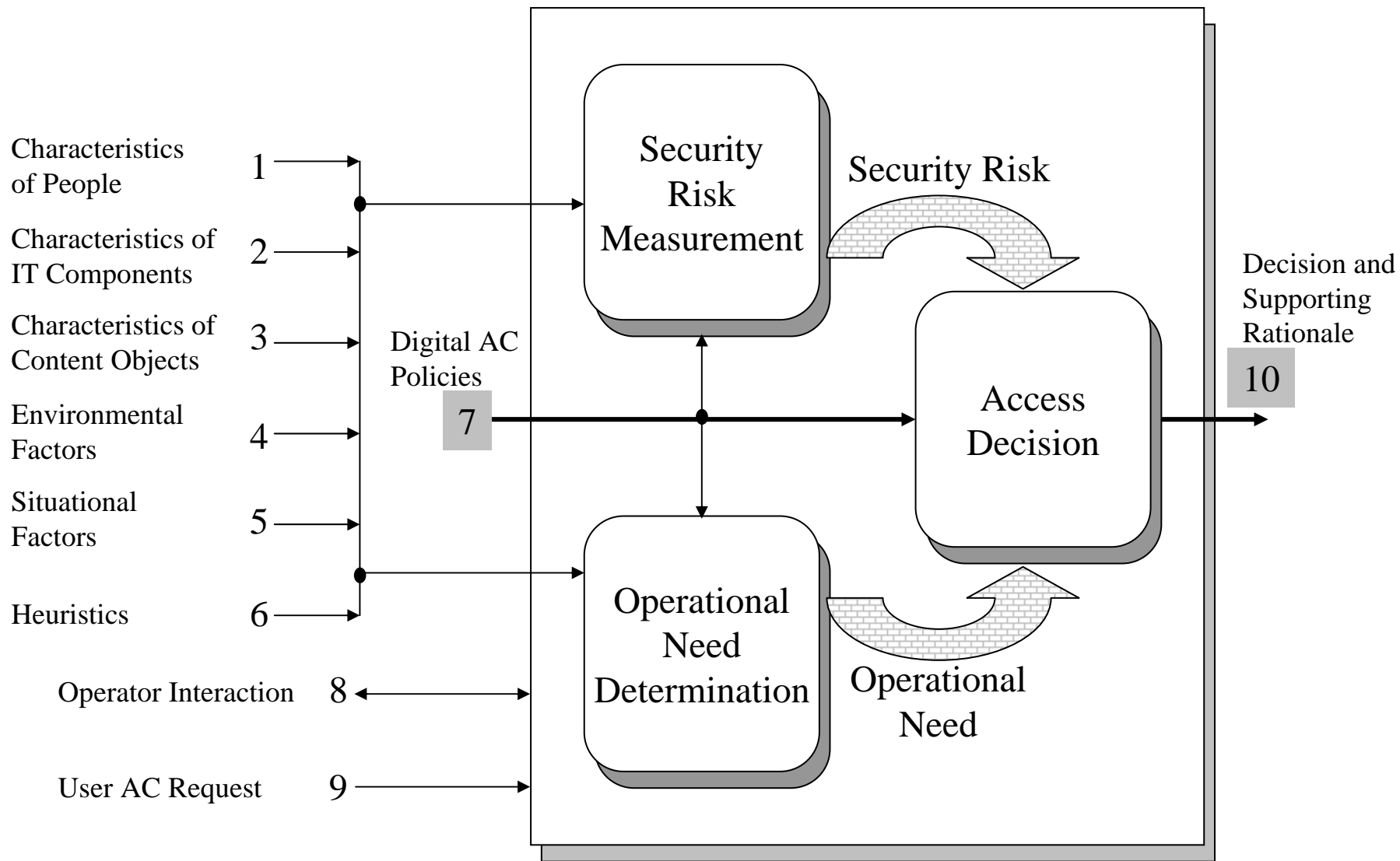
June 16, 2005

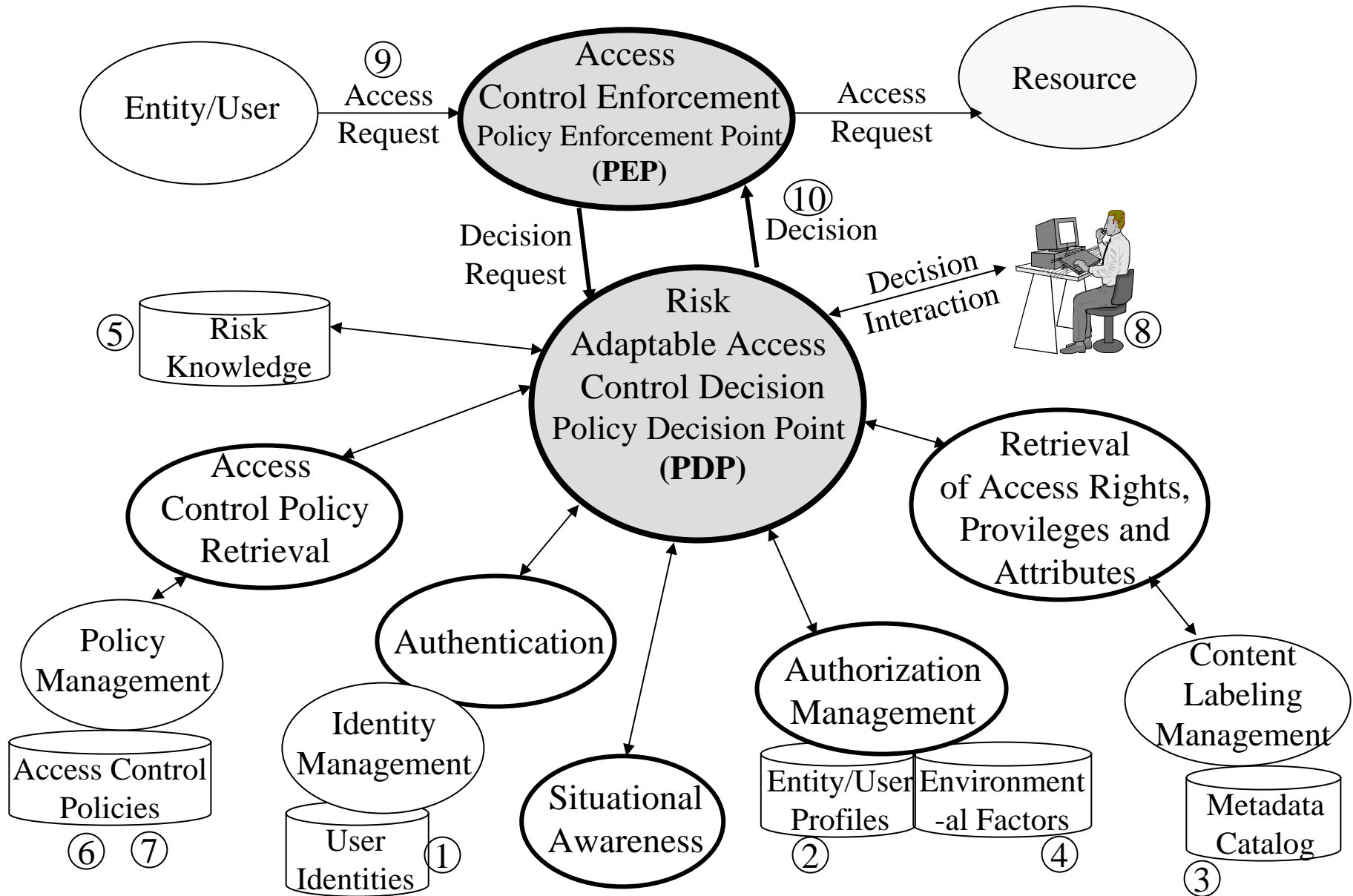
Agenda

- Introduction
 - RAdAC and Policy Based Management (PBM)
- NSA RAdAC Model
 - An Exposition
- My Policy-Based Architecture for RAdAC
 - A First Detailed Look

RAdAC and PBM

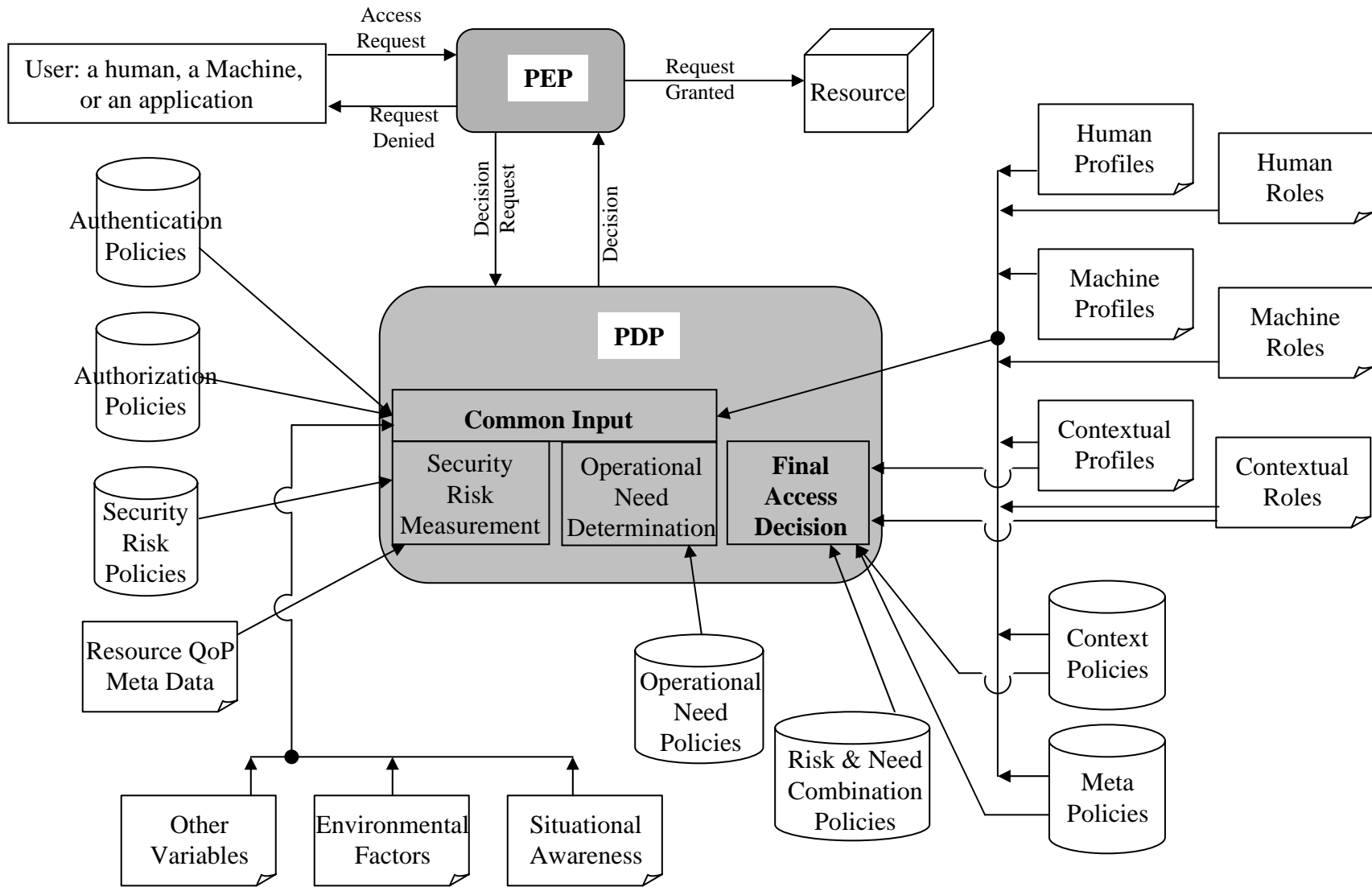
- The new model attempts to make a transition from a 'need to know' mindset of the cold war era to today's 'need to share' reality.
 - Distributed Policy Based Access Control supports this 'need to share'
- Security risk and operational need as part of each access control decision
 - Dynamic policy-based management of access control
 - Dynamic policy management





Policy Based Architecture for RAdAC

- Introduced a detailed set of ‘types’ of policies needed for RAdAC.
- Used these different types in an architecture
 - Security Risk Measurement
 - Operational Need Measurement
 - Combine the two into a unique actionable Policy Decision
 - Common Set
- Infrastructure needed to support a distributed implementation of Policy Based RAdAC.
 - 7 minimal PBM infrastructure functions; 9 different type of policies; 7 different types of information bases



Conclusion

- We have accomplished two things in this paper.
 - (1) Presented a dynamic policy based architecture for a distributed implementation of RAdAC model.
 - Identified and described seven different types of policies and ten different information bases
 - (2) Described the infrastructure within which such a model will live.
 - This infrastructure is needed for supporting any distributed policy based architecture for RAdAC, as well as for the dynamic management of policies themselves.
 - We have introduced and described eight different functions, which are minimally expected in such an infrastructure.