# ABAC AND THE EVOLUTION OF ACCESS CONTROL MODEL

I-Security Seminar
ITS Surabaya, Sept 2014

Co Founder of BelajarMikrotik.Com

Founder of ForumMikrotik.Com

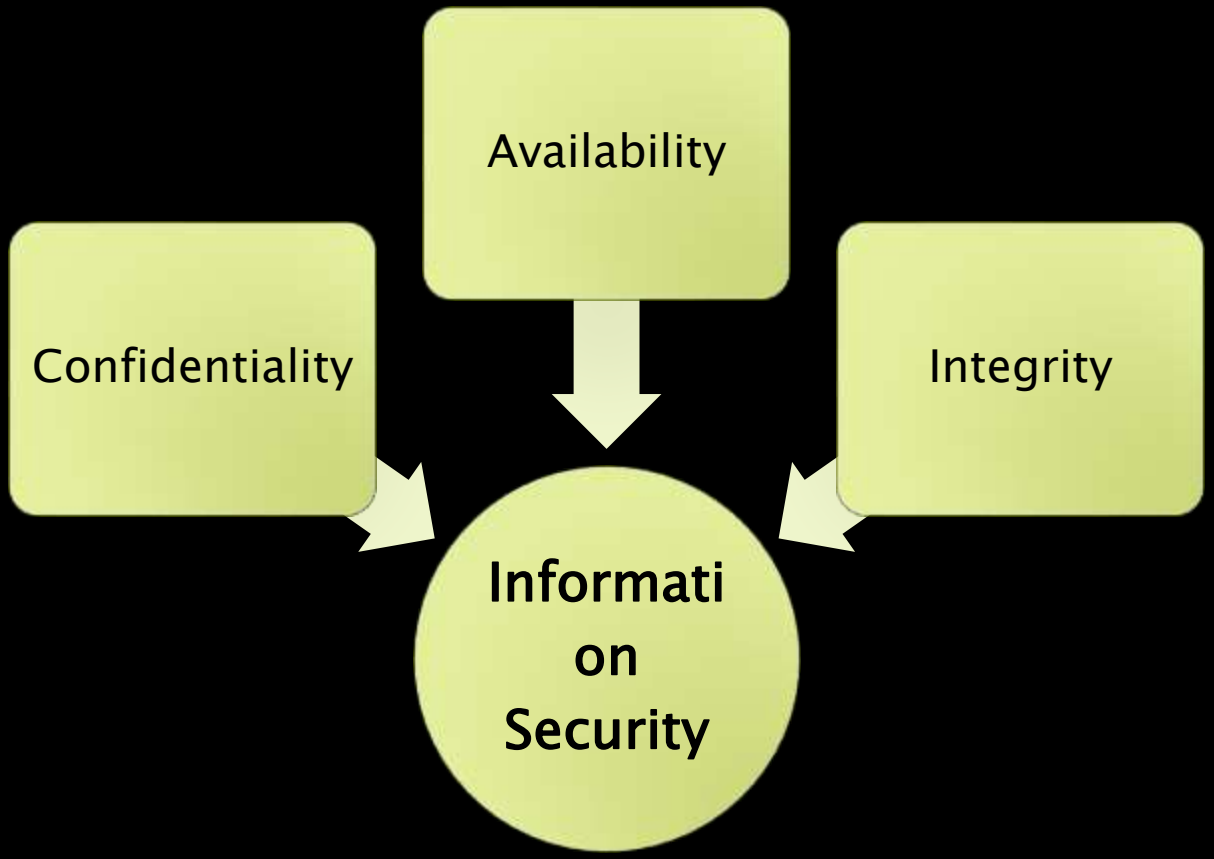
Trainer and Lecturer for Project Management and Information Security Classes

ICT Manager of Services at PT. Bayan Resources Tb

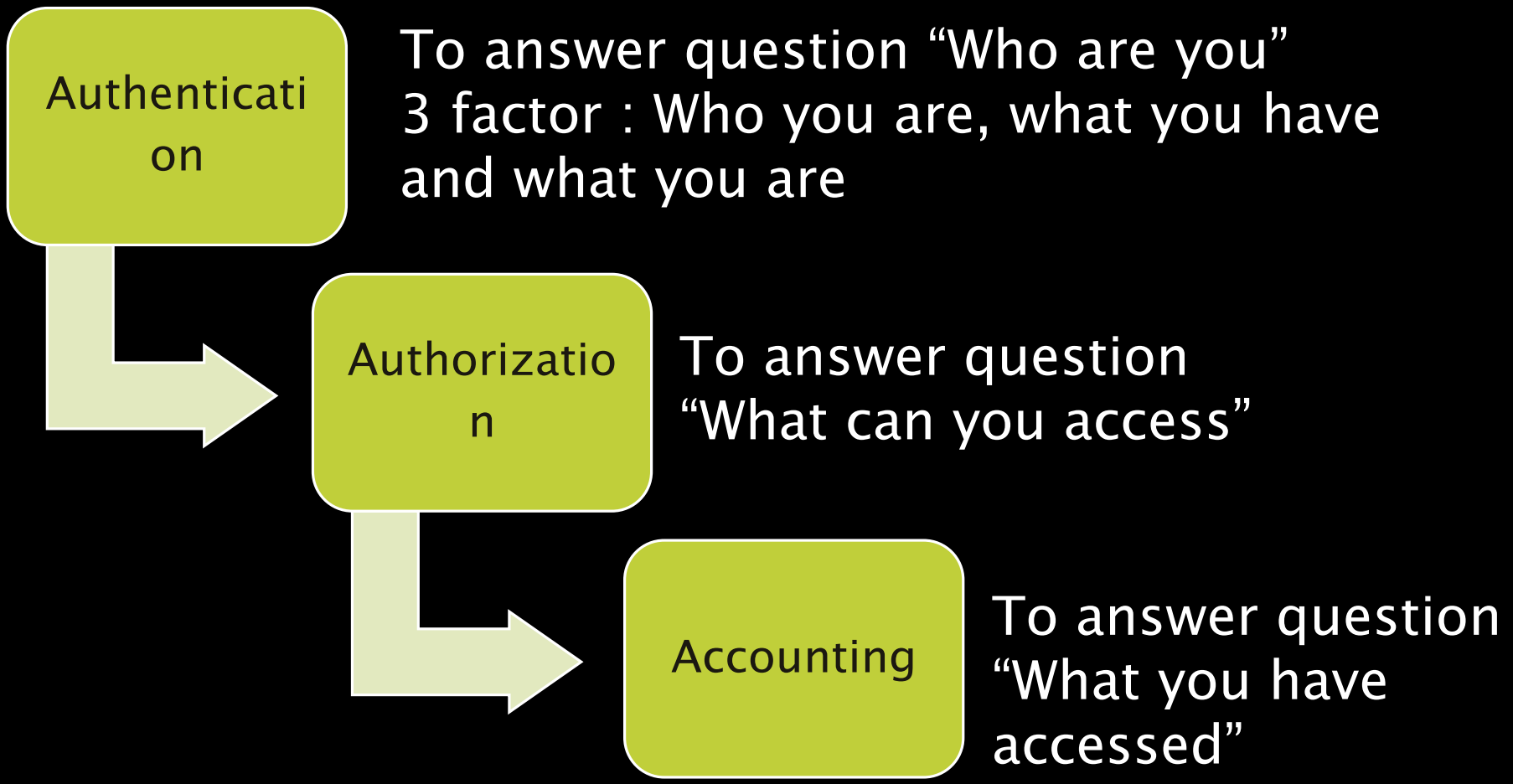
AKBAR AZWIR, MM, PMP, CISSP

belajar MikroTik
www.belajarmikrotik.com

# INFORMATION SECURITY



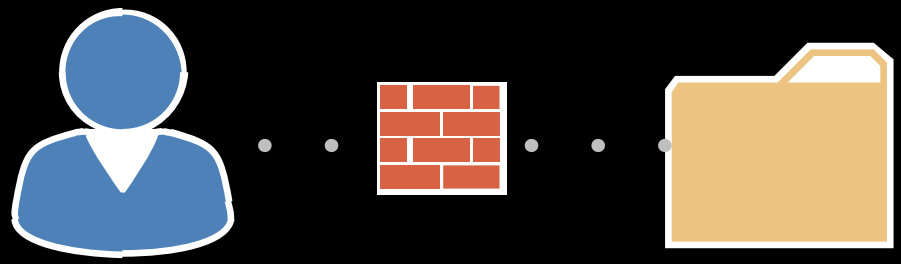
# AAA


Authenticati
on
To answer question “Who are you”
3 factor : Who you are, what you have and what you are
Authorizatio
n
To answer question
“What can you access”
Accounting
To answer question
“What you have accessed”

# Let’s talk about Access Con

# ACCESS CONTROL MECHANISM

*"The logical component that serves to receive the access request from the subject, to decide, and to enforce the access decision."*



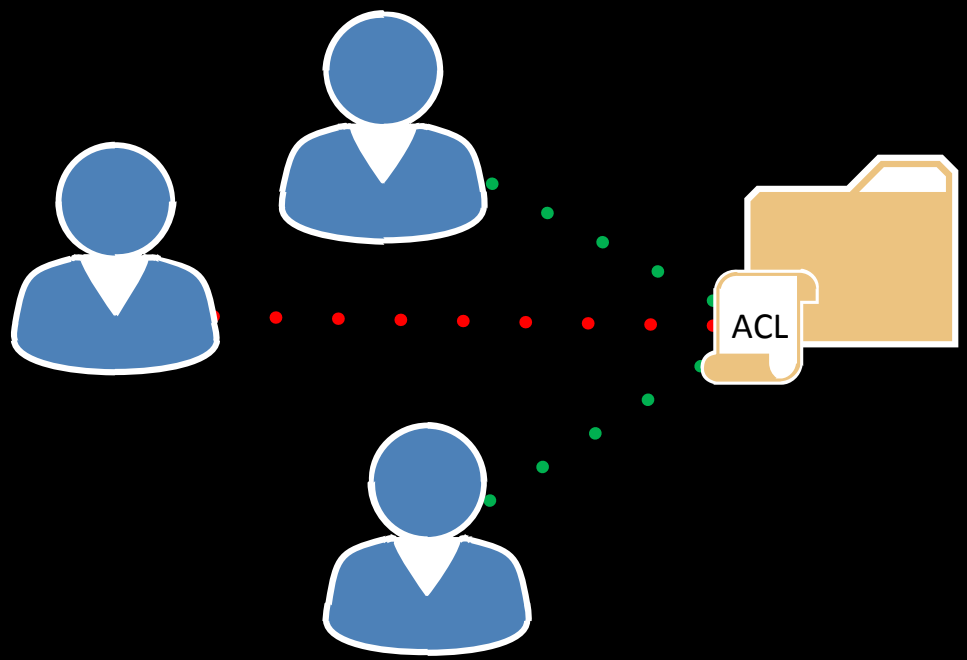
# ACCESS CONTROL MODEL

*"Framework that dictates how Subjects Access Object."*

– CISSP AIO Exam Guide, 6th Edition

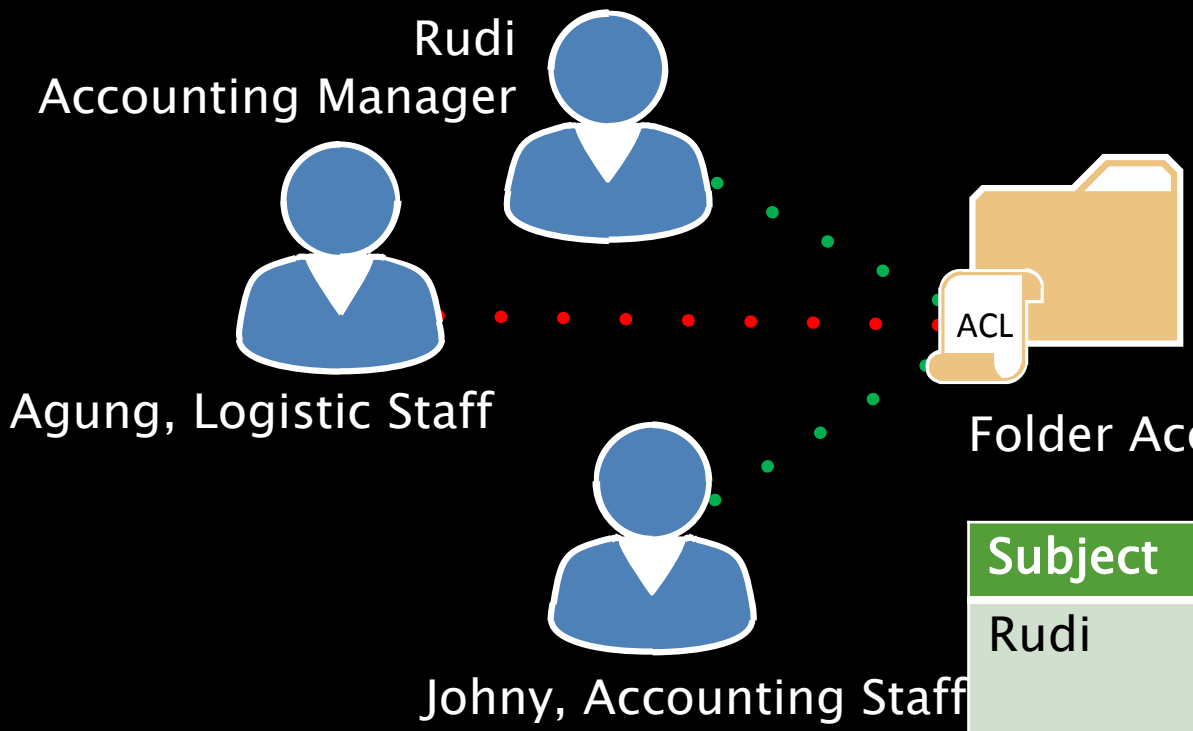

# ACCESS CONTROL MODEL

# DISCRETIONARY ACCESS CONTROL (DAC)




- Decentralized
- Owner Discretion, usually via administrator
- Enforce through ACL
- Identity Based
- Permission rule attached to the Object

# DISCRETIONARY ACCESS CONTROL (DAC)



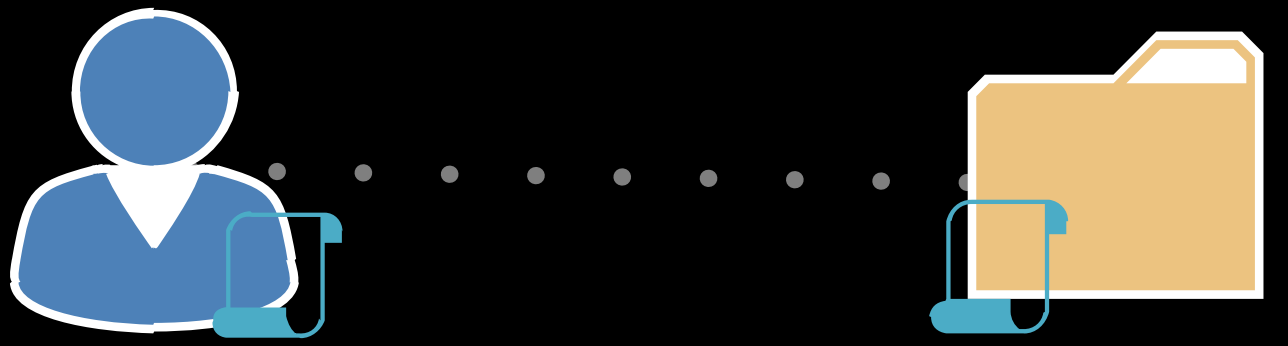

| Subject | Permission |
|---|---|
| Rudi | Full Control |
| Johny | R W D C |

# DISCRETIONARY ACCESS CONTROL (DAC)

| Pros | Cons |
| --- | --- |
| • Easy to implement<br>• Great Flexibility<br>• Built-in in most OS | • Doesn't scale well<br>• Possibility of ACL Explosion<br>• Prone for mistakes |


# ACCESS CONTROL MODEL

# MANDATORY ACCESS CONTROL (MAC)

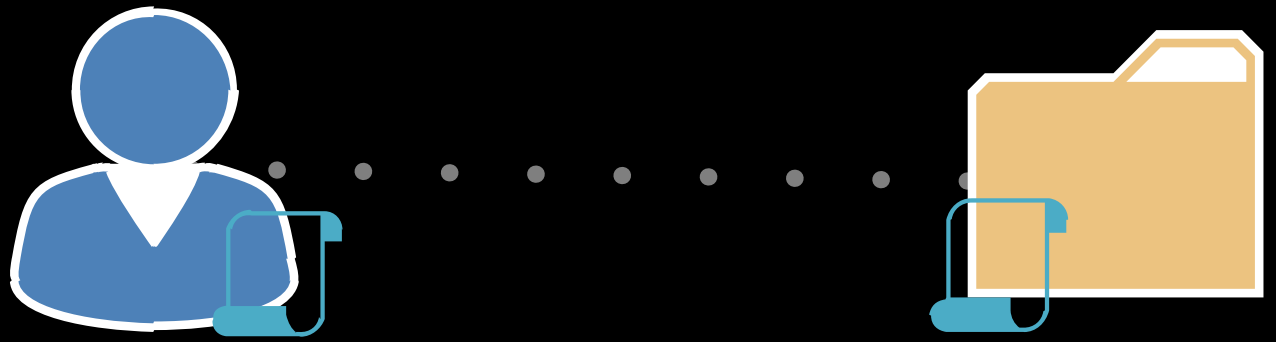


Subject with Clearance

Object with Classification

- Centralized
- Access Control enforced with Clearance and Classification
- Only Subject with Clearance the same or above from Object Classification can Access the Object

# MANDATORY ACCESS CONTROL (MAC)



Ken Watanabe, Intelligent Analysis
Clearance Level 2

Project Pegasus
Data Classification Top Secret

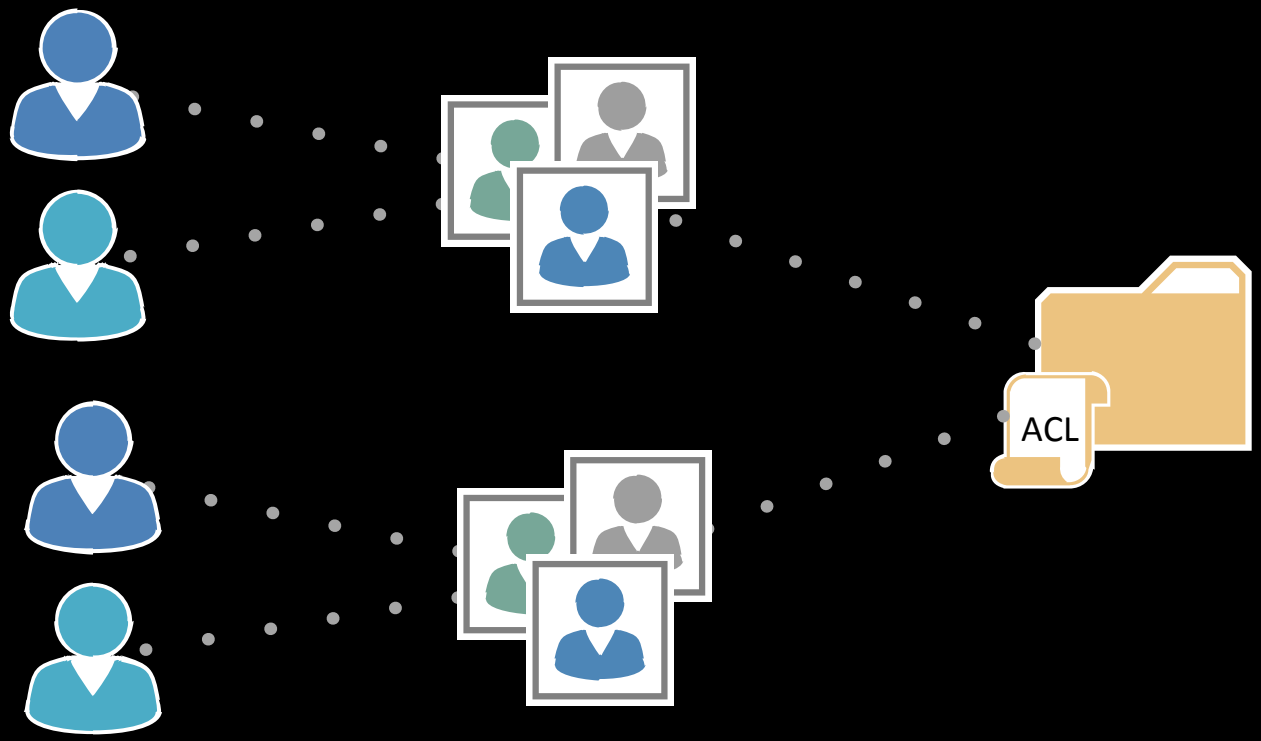
| Clearance Level | Classification |
|---|---|
| Level 5 | Top Secret, Secret, Classified, UnClassified |
| Level 4 | Secret, Classified, UnClassified |
| Level 3 | Classified, UnClassified |
| Level 2 | UnClassified |

# MANDATORY ACCESS CONTROL (MAC)

| Pros | Cons |
| --- | --- |
| • Most Secure<br>• Easy to scale | • Not Flexible<br>• Limited user functionality<br>• High admin overhead<br>• Expensive |


# ACCESS CONTROL MODEL

# ROLE BASED ACCESS CONTROL (RBAC)

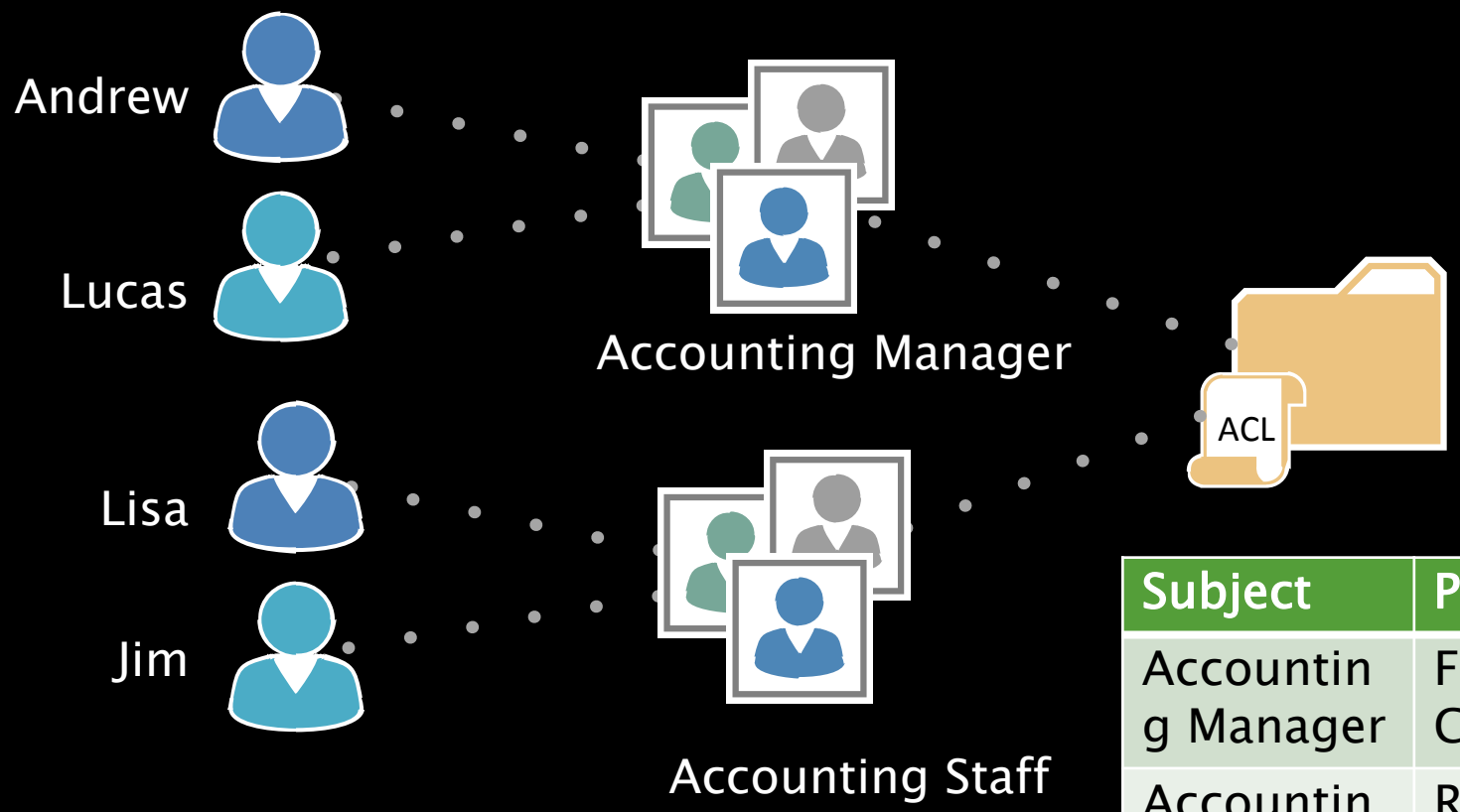



Subject Assigned to Role

Role

Object with ACL for Role

# ROLE BASED ACCESS CONTROL (RBAC)




| Subject | Permission |
|---|---|
| Accounting Manager | Full Control |
| Accounting Staff | R W D C |

# ROLE BASED ACCESS CONTROL (RBAC)

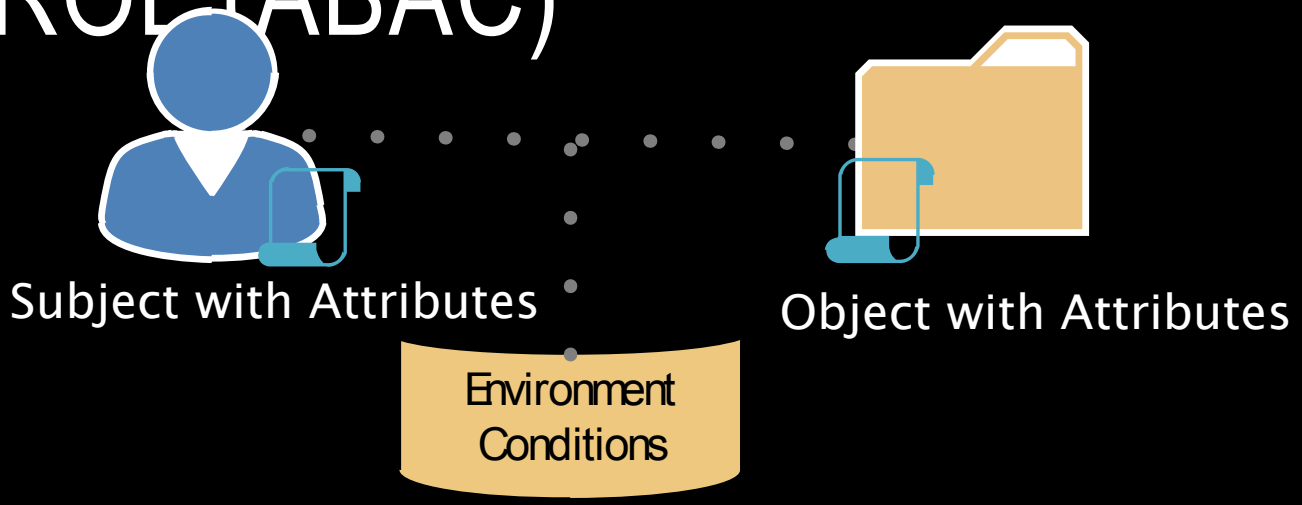
- Centralized and Decentralized at once
- Subject access permission are enforced through Role membership
- Role permissions are enforced through Object's ACL
- Subject can be a member of more than one role

# ROLE BASED ACCESS CONTROL (RBAC)

| Pros | Cons |
| --- | --- |
| • Scalable to some degree<br>• Great for organizations with high turn over | • Roles needs provisioning and maintenance<br>• Possibility of Role explosion<br>• Unable to accommodate real-time context |

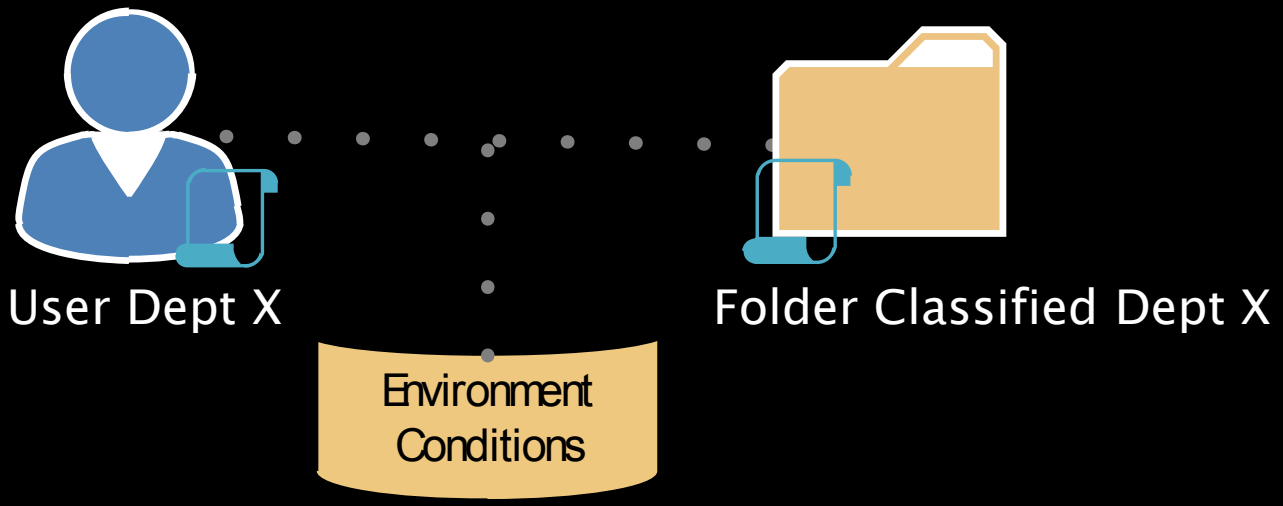

# ACCESS CONTROL MODEL

# ATTRIBUTE BASED ACCESS CONTROL (ABAC)




- Centralized
- Access Control enforced by taking Subject Attributes, Object Attributes, and Environment Context and compare them to the Policy
- Policy written using human readable language that easily understood, XACML (eXtensible Access Control

# ATTRIBUTE BASED ACCESS CONTROL (ABAC)




- Ex 1 : User can only access their Dept Folder from their own Office location at Working Hour only
- Ex 2 : Certain Folders can only be accessed from Specific Workstations if the bandwidth

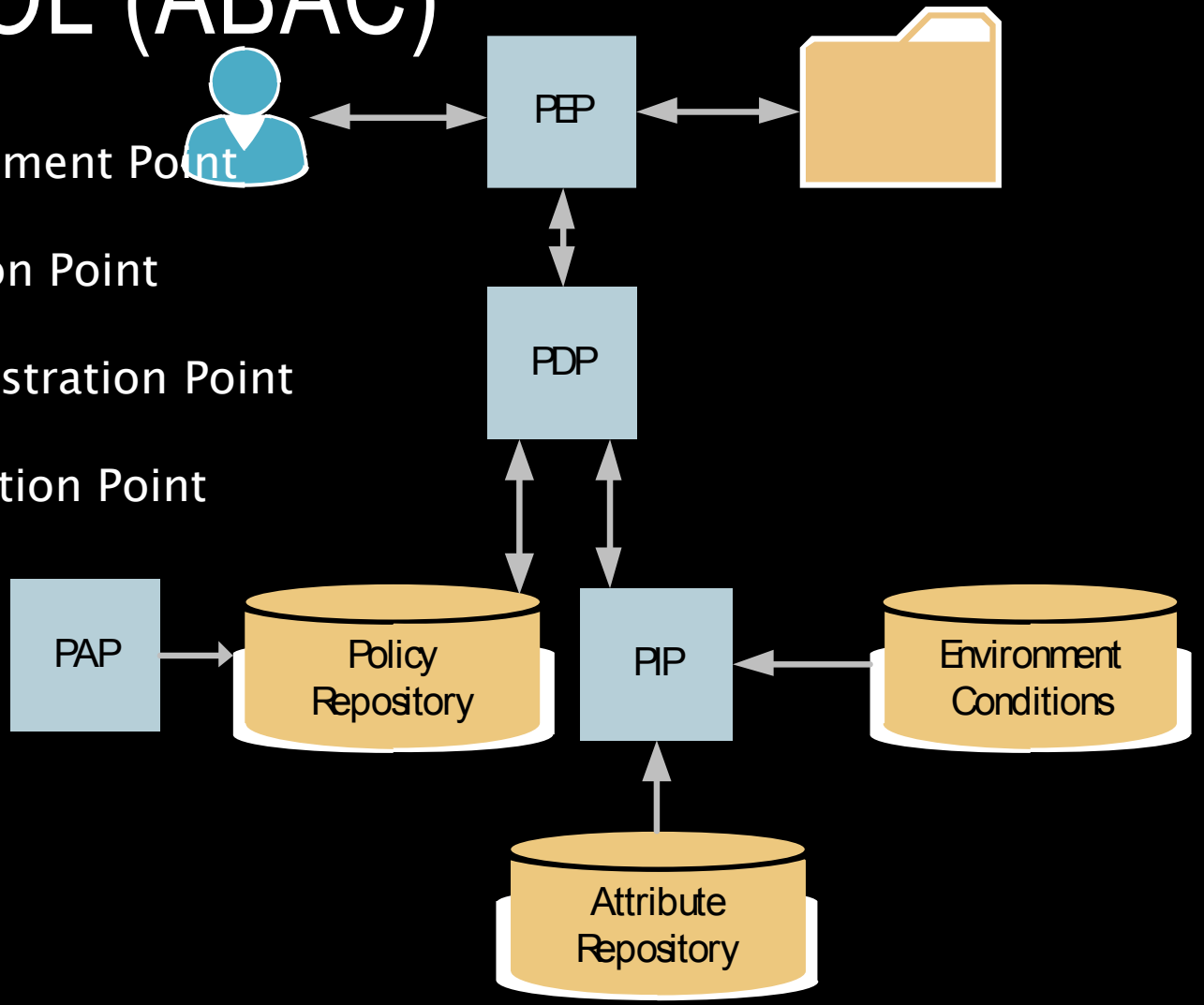
# ATTRIBUTE BASED ACCESS CONTROL (ABAC)

PEP : Policy Enforcement Point

PDP : Policy Decision Point

PAP : Policy Administration Point

PIP : Policy Information Point



# ATTRIBUTE BASED ACCESS CONTROL (ABAC)

| Pros | Cons |
| --- | --- |
| • Scalable<br>• Real time Context aware<br>• Segregation of Duty, different people can manage different Subject and Object Attributes and Policy | • It's new<br>• Requires socialization and convincing<br>• Organization change required to manage Attributes |

# ATTRIBUTE BASED ACCESS CONTROL (ABAC)

- ABAC is still in it's early stage
- Gartner predicts that by 2020 70% of business will use ABAC

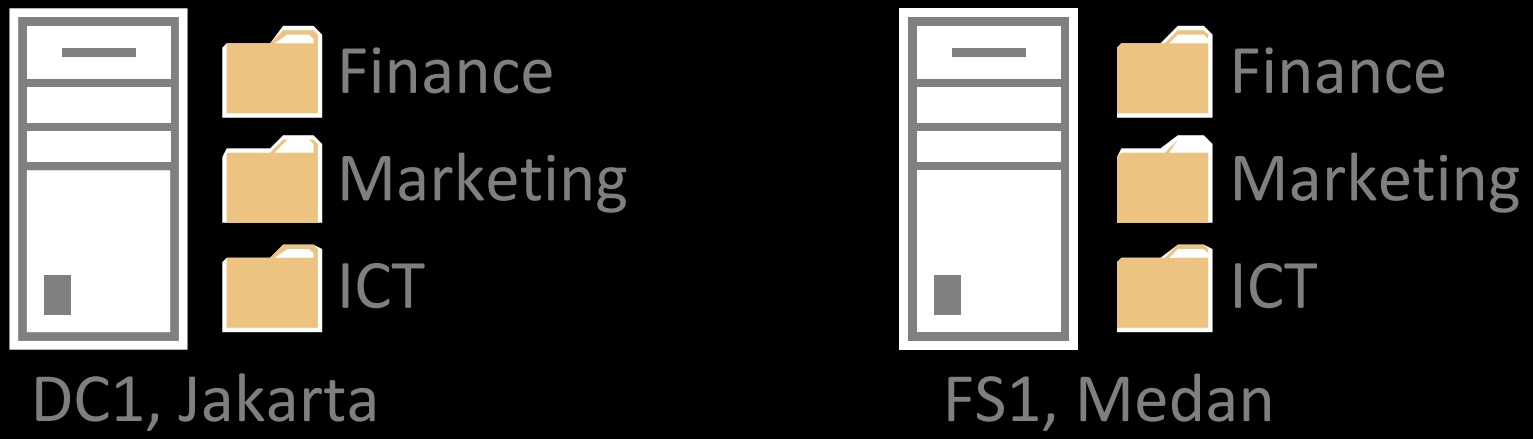
# ATTRIBUTE BASED ACCESS CONTROL (ABAC)

- Microsoft Windows Server 2012 Claim Based Access Control or Dynamic Access Control is Microsoft implementation of ABAC
- Fedora 3.3 FESL (Fedora Security Layer) using XACML to implement ABAC
- 3rd party auth service companies such as Axiomatics and Avatier offer ABAC implementation to OS and Applications and or Databases

# ATTRIBUTE BASED ACCESS CONTROL (ABAC)

- Open source ABAC projects such as :
  - http://abac.deterlab.net
  - OpenAZ, http://www.openliberty.org

# DAC SIMPLE DEMONSTRATION




| User | Attribute – Department | Attribute – st (State) |
|---|---|---|
| Andi.Michael | Finance | Jakarta |
| Bayu. Achmad | Finance | Medan |
| Ken. Surahyo | Marketing | Jakartq |
| David.Lim | Marketing | Medan |
| Zeru.Halim | Information | Jakarta |

# CONCLUSION

- The current information system ecosystem require a flexible yet secure access control and that's what ABAC is trying to answer
- As Gartner predicts, by 2020, 70% of business will use ABAC for authorization. Let's familiarize early
- There is still a lot of study required as there is no standard implementation of ABAC, therefor there is still a lot of involvement that we can offer to the Information System world

# Thank You

# Q & A

ABAC AND THE EVOLUTION OF ACCESS CONTROL MODEL

I-Security Seminar
ITS Surabaya, Sept 2014