INFO 310

Fall 2016

Week 3 – Lecture 2

HOUSEKEEPING

- Attendance
- Administrativa
- Security In The News

Lab I Recap

- What worked, what didn't?
- Still missing 4 submissions…
- Questions?

Authentication, Identity, & Access Management

Definitions

- **Identity:** Who someone is (or claims to be).
- **Username:** A unique sequence of characters used to identify a user account
- **User Account:** A collection of attributes, usually including user identity information
- **Password:** A sequence of characters used to prove control over a specific username
- **Access:** The ability to enter or use a resource
- **Authentication:** The act of verifying a username's access eligibility
- **Authorization** : The process of giving a username permission to access a resource, to do something.

Authentication vs. Authorization

- Localized
  - /etc/passwd & /etc/shadow
  - SAM
- Centralized
  - LDAP (Lightweight Directory Access Protocol)
    - SASL (Simple Authentication and Security Layer)
  - AD (Active Directory)
  - Kerberos*
  - RADIUS (Remote Authentication Dial-In User Service)
  - Also: EAP, HIP, MSCHAP, NTLM, PAP, PEAP, TACACS

Access Control Models

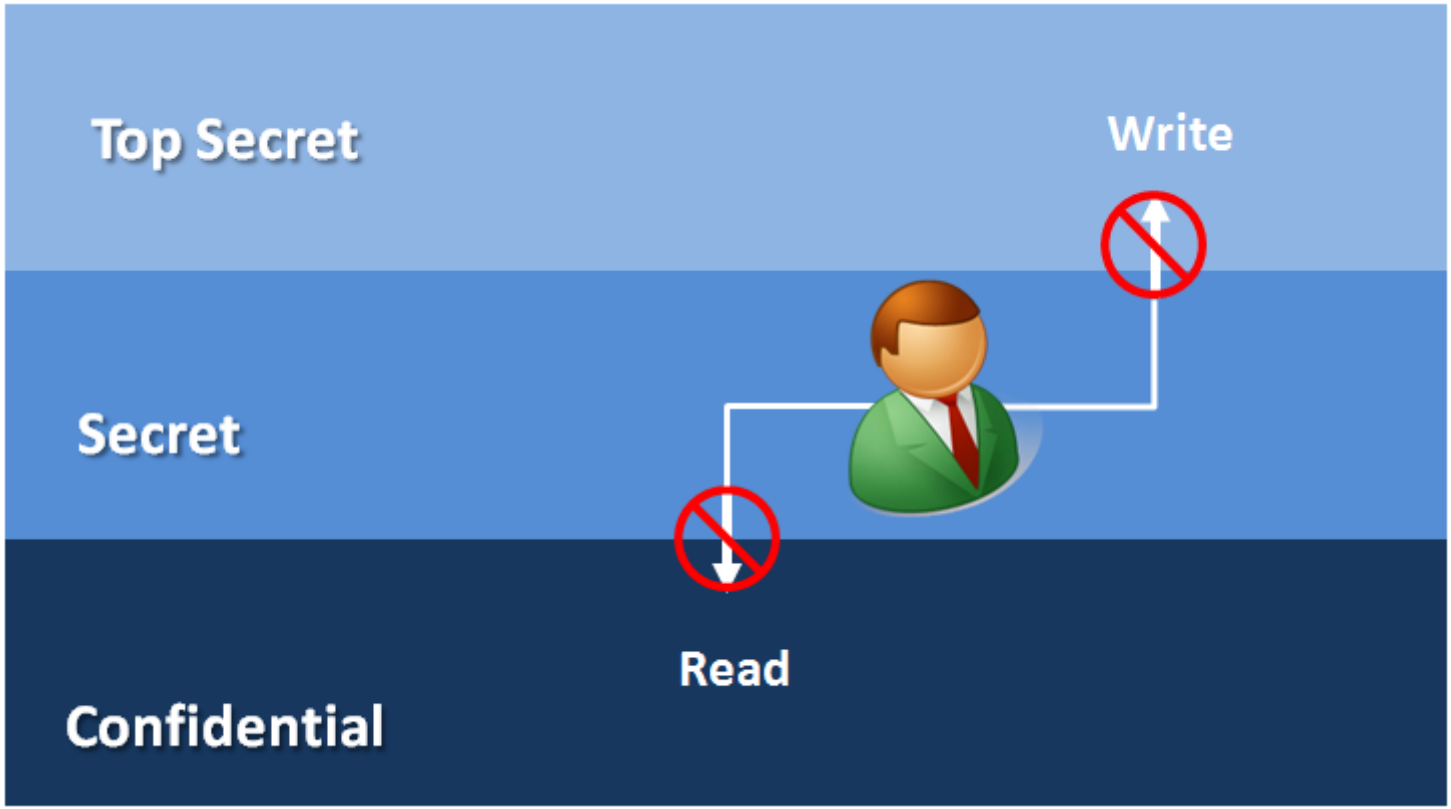
- Mandatory Access Controls (MAC)
  - Common Models:
    - Biba Integrity Model (BIM)
    - Bell-LaPadula (BLP)
- Role Based Access Controls (RBAC)
  - Rules Based Access Controls (RB-RBAC)
    - Access Control List (ACL)
- Attribute Based Access Controls (ABAC)

- Discretionary Access Controls (DAC)

Bell-LaPadula (BLP) Model

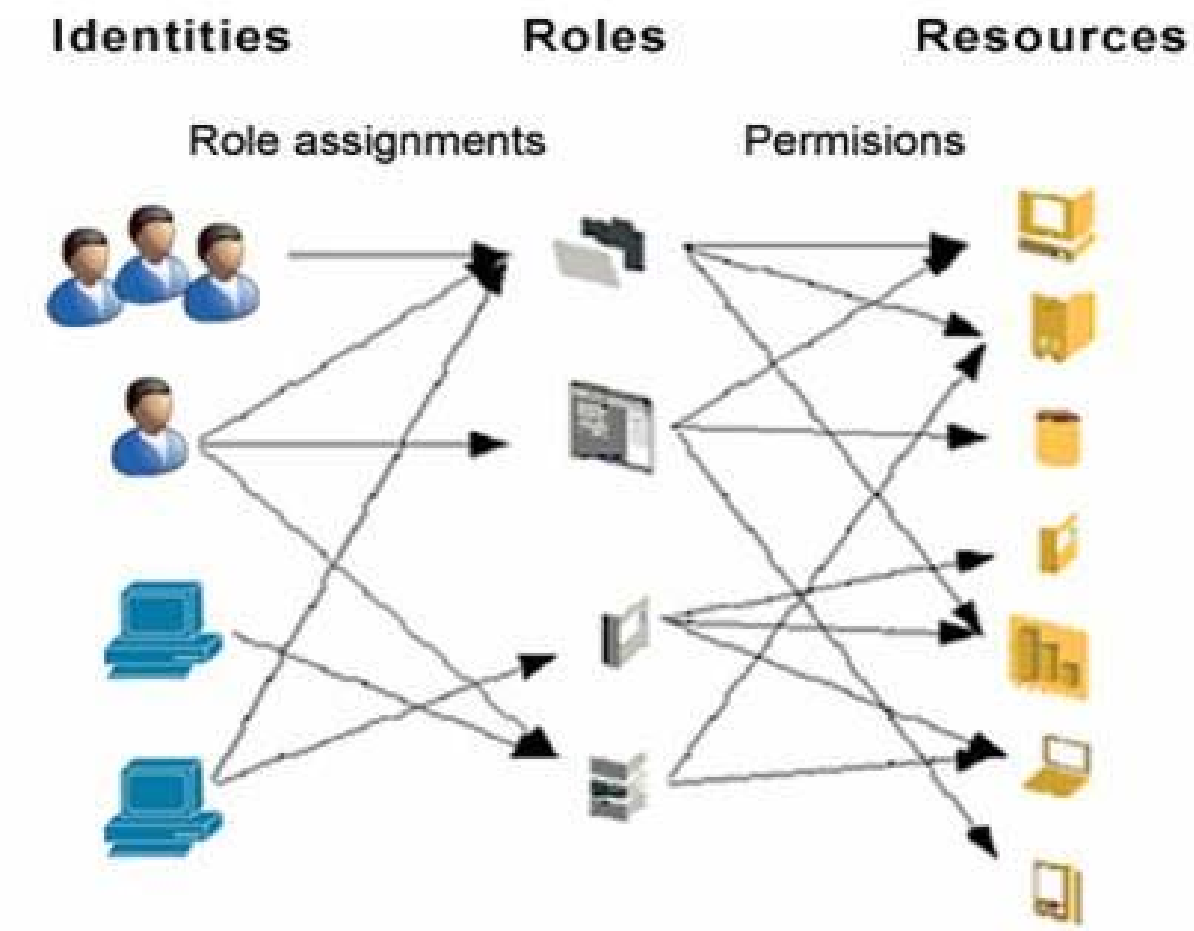
“No read up / No write down”
“Write up / Read down”

Biba Model

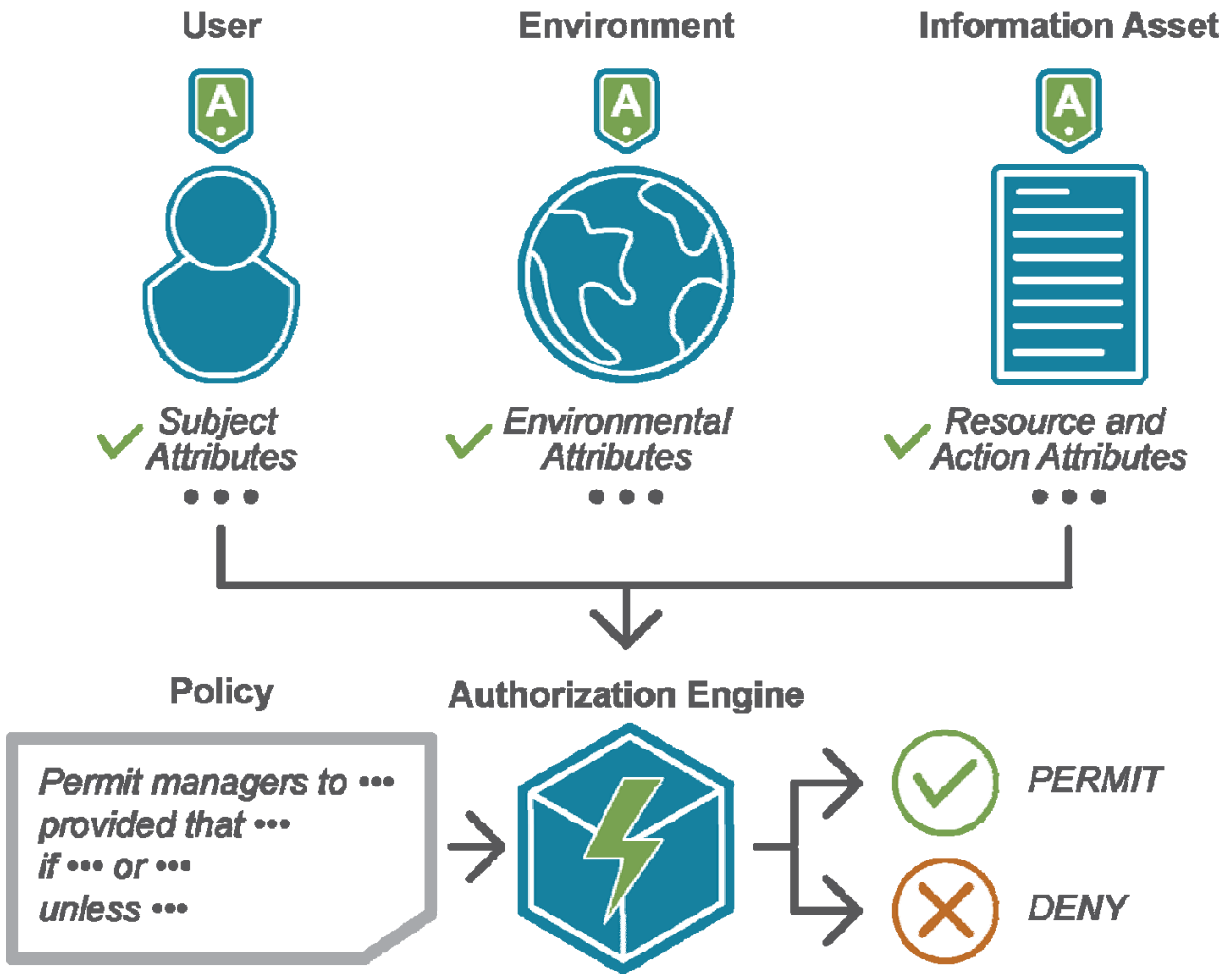


“No read down / No write up”
“Read up / Write down”

Role Based Access Control (RBAC)

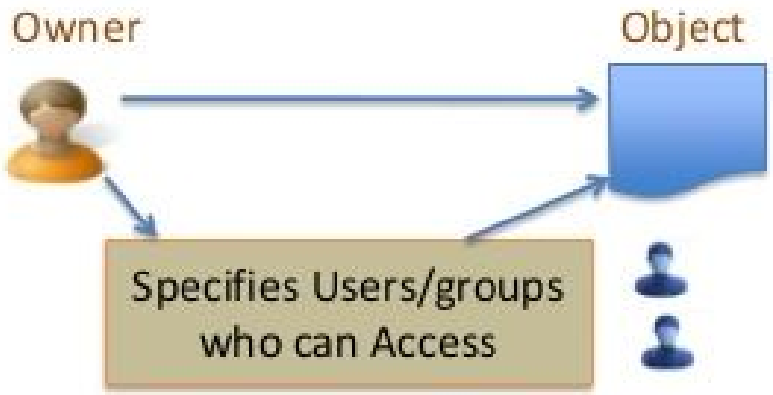


ABAC


User
Environment
Information Asset
Subject Attributes
Environmental Attributes
Resource and Action Attributes
Policy
Authorization Engine
Permit managers to •••
provided that •••
if ••• or •••
unless •••
PERMIT
DENY

DAC

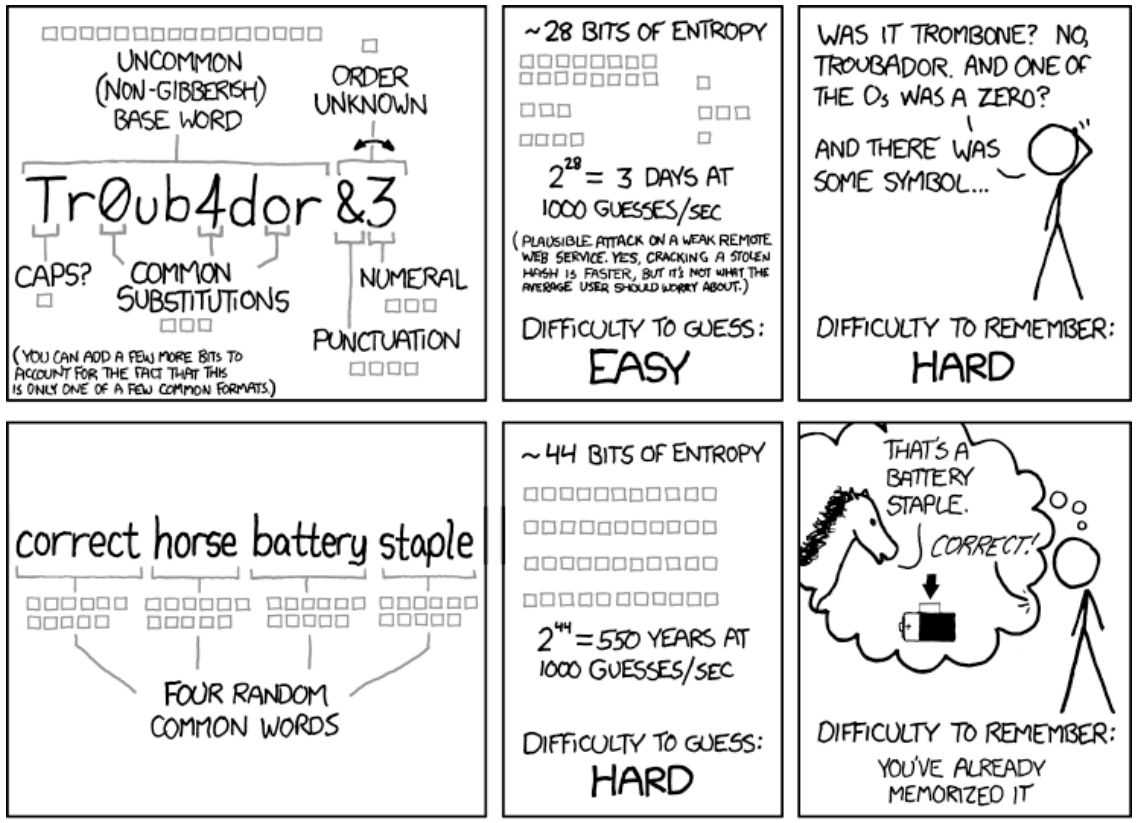
- Discretionary – Document owner has the authority to control access of the document.
- A system that enables the document owner to specify set of Users with access to a set of documents



Passwords

- Why passwords?
- Password vs. Pass Phrase
- Password Entropy
- Password Attacks
  - Brute Forcing
  - Dictionary Attacks
  - Hash Attacks
  - Phishing
  - Reset / Forgot Attacks
    - A word about secret questions…
- What makes a “good” / strong password?

https://xkcd.com/936/



(https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength)

Other types of authentication

- OTP (one time passwords)
- Public keys
- Pattern Based
- Out-of-band
- Challenge & Response

2-Factor / Multi-Factor

- Transmitted out of band
- Soft Token
  - Google Authenticator
  - Symantec VIP
  - FaceBook App
  - …
- Hard Token
  - RSA SecurID
  - EnTrust
  - YubiKey
  - …
- Secret Answers (not really…)
- Biometrics

Biometrics

- OK as a 2nd or 3rd factor…
  - Fingerprints
  - Palm scans
  - Retina Scans
  - Iris Scans
  - Facial Recognition
- Not so much as a 1st factor!

(this page intentionally left blank)