CSCV4022-Cloud Security

Faculty name: G Nagarajan

Introduction

- **Cloud computing** is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.
- The term is generally used to describe data centers available to many users over the Internet
- Clouds may be limited to a single organization (enterprise clouds), or be available to many organizations (public cloud).

Cloud providers typically use a "pay-as-you-go" model,

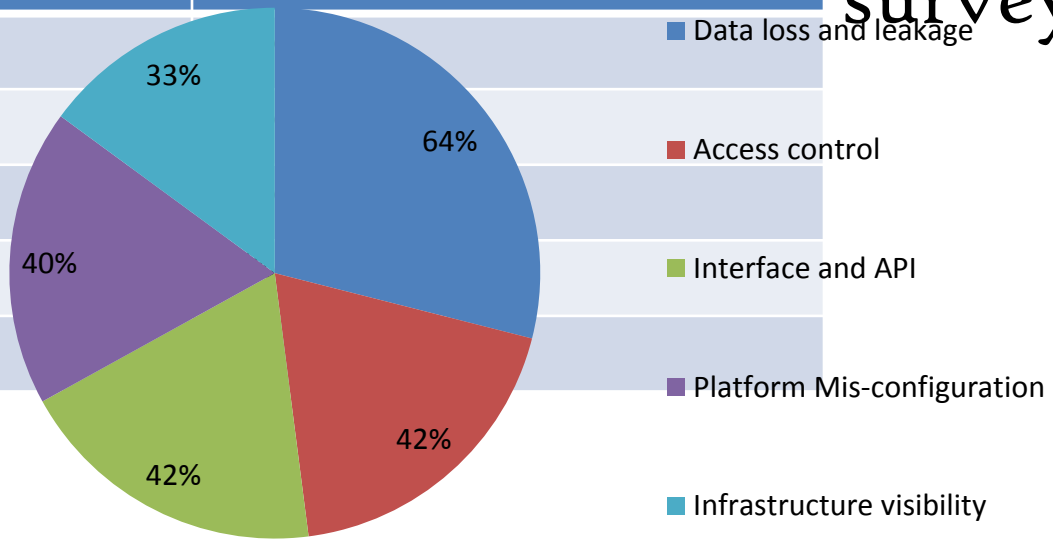
What is Cloud Security

- Cloud security—also called cloud computing security—refers to the discipline and practice of protecting cloud computing environments, applications, data, and information.
- Cloud security entails securing cloud environments against unauthorized use/access, distributed denial of service (DDOS) attacks, hackers, malware, and other risks.
- While cloud security applies to security for cloud environments, the related term, cloud-based security, refers to the software as a service (SaaS) delivery model of security services, which are hosted in the cloud rather than deployed via on-premise hardware or software.

Why Cloud Security?

- Information Security Community – CloudSecurity Insiders 2020 survey.

Security Controversy	Percentage of security issues
Data loss and leakage	64%
Access control	42%
Insecure Interface and API	42%
Platform Mis-configuration	40%
Infrastructure visibility	33%



News on Computer /Network

2019 Data Breach Hall of Shame: These were the biggest data breaches of the year

- Adobe left 7.5 million Creative Cloud customer records on an unsecure database.
- Every month, another company was asking its customers to change their passwords and report any damage. Cloud-based storage companies like Amazon Web Services and ElasticSearch repeatedly saw their names surface in stories of negligent companies in the fields of health care, hospitality, government.

2019 News on India Today

- Personal data of 267 million Facebook users was exposed online on a database. The database had been exposed for nearly two weeks before it was discovered by the researchers.
- This database can be used to conduct SMS and phishing scams.

Cloud Storage Security Challenges

Data privacy

Because your data is stored elsewhere, it might be impossible to know just how closed off it is. How can you be sure no one can access it when you don't maintain the servers.

Lack of control

If something affects your storage provider, like outages or malware infections, that will directly impact access to your data. You'll have to rely on the provider to fix the issues.

Data leakage

Data leakage can cause serious problems since it could expose business-critical or private data to external sources. Even if you take steps to prevent anyone in your enterprise from leaking data, your storage provider might accidentally expose your data to the wrong person.

Cloud security primary goals:

- **Confidentiality** – Makes information available to only authorized users.
- **Data Integrity** – Ensures that information has not been manipulated.
- **Authentication** – Confirms the authenticity of information or the identity of a user.
- **Non-repudiation** – Prevents a user from denying prior commitments or actions.

Confidentiality

- **Confidentiality** refers to the prevention of the unauthorized access of the data and hence making sure that only the user who has the permission can access the data.
- Data must be encrypted before it is outsourced, to protect it from malicious internal or external attacks.

Integrity

Protect the data from the unauthorized insert, update, or delete. The data owner and authorized users should be able to recognize if the data is corrupted or incomplete, and receive the most recent updated version of the data, which guarantees accuracy and consistency of data.

Authentication

- Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.
- **Authentication service has two variants: Message authentication:** identifies the originator of the message without any regard router or system that has sent the message. **Entity authentication:** is assurance that data has been received from a specific entity say a particular website.

Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party. Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data.

For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Availability

The data in the cloud servers should be accessible to its users. Major threats to availability are denial of service (DOS) attacks, natural disasters, and equipment failures at the service provider's end.

Access control:

The outsourced data should be accessed only by authorized users.

Access Control

- The outsourced data should be accessed only by authorized users.
- To effectively protect your data, your organization's access control policy must address these (and other) questions. What follows is a guide to the basics of access control: What it is, why it's important, which organizations need it the most, and the challenges security professionals can face.

What is access control?

In the fields of physical security and information security, **access control** (**AC**) is the selective restriction of access to a place or other resource while access management describes the process.

- At a high level, access control is a selective restriction of access to data. It consists of two main components: authentication and authorization
- Cloud Computing is an emerging technology that provides online storage of data and access to services.

Access Control is a method that allows access to the cloud services. Access Control methods include 1)

1)Mandatory Access Control (MAC),

2)Discretionary Access Control (DAC) and

2) Role Based Access Control (RBAC).

- The Access Control models, however, are not fully secure and efficient.
- There are limitations in terms of performance , reliability and security.
- In a research compare the existing models and propose methods for overcoming the issues that exist.

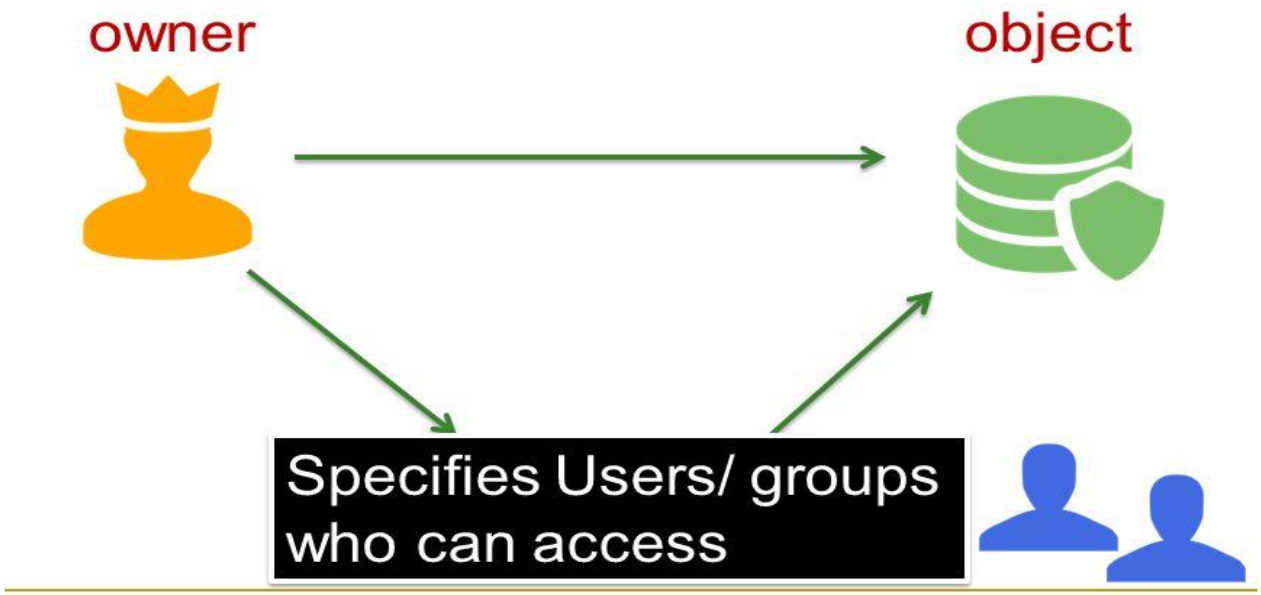
1) Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator.

MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users.

Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password.

DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

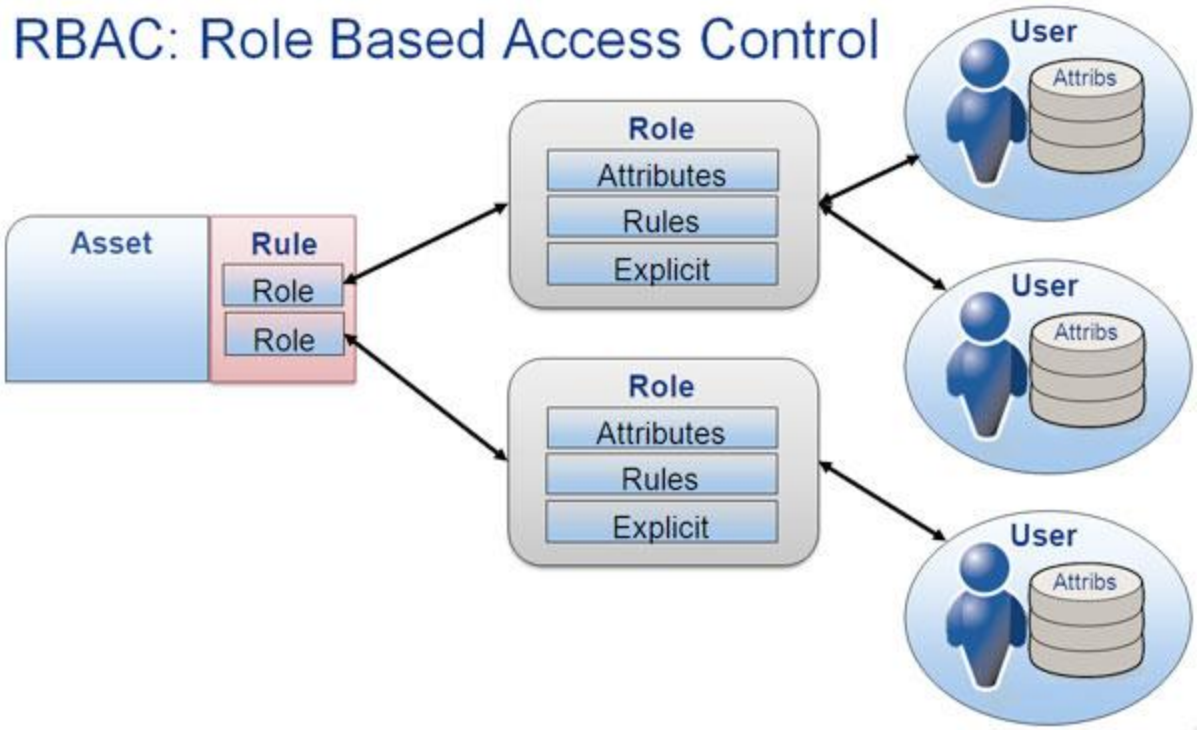
Discretionary Access Control (DAC)

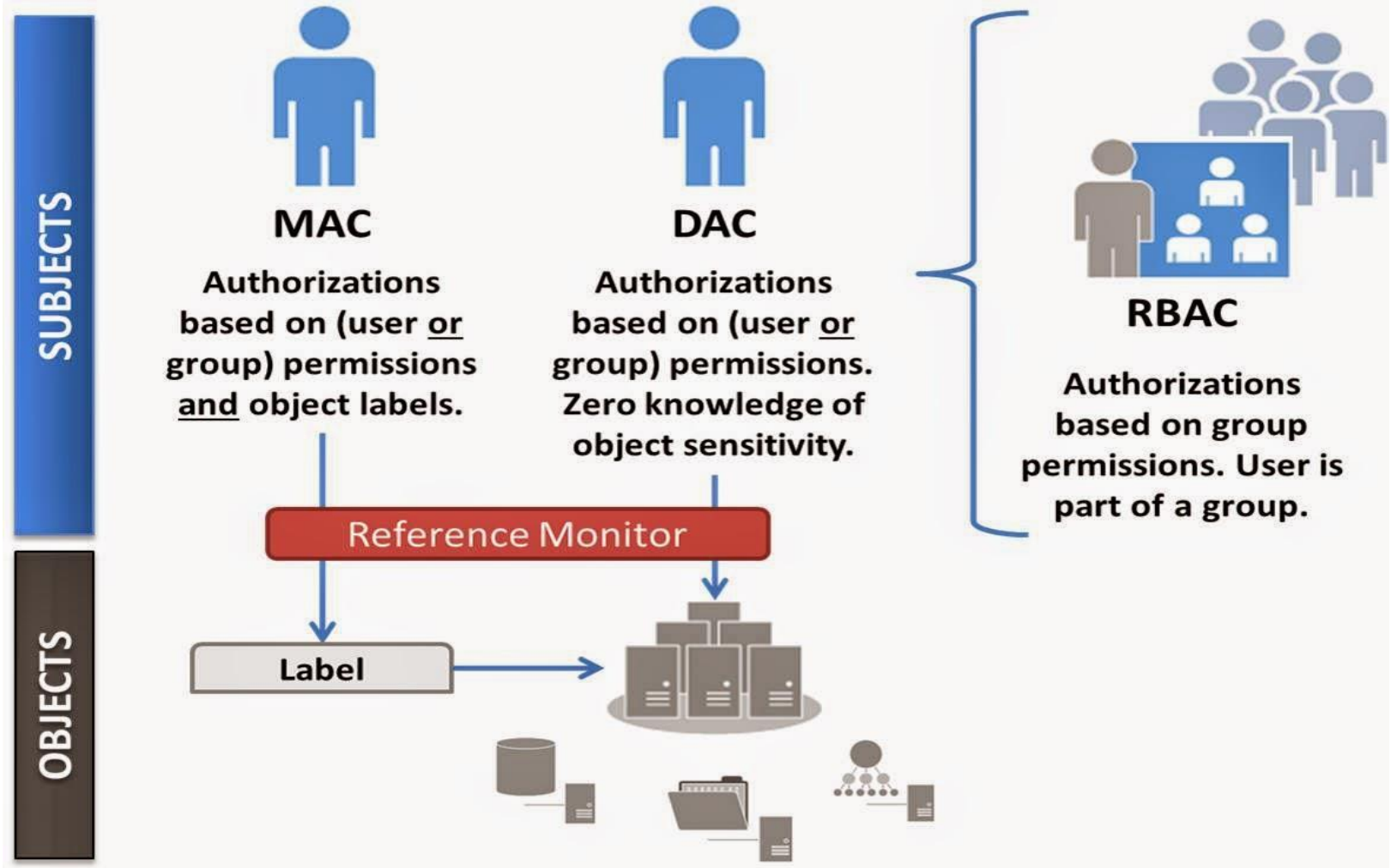


Role Based Access Control (RBAC).

In computer systems security, **role-based access control** (**RBAC**)or **role-based security** is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees

A study by NIST has demonstrated that RBAC addresses many needs of commercial and government organizations


RBAC: Role Based Access Control
Asset
Rule
Role
Role
Role
Attributes
Rules
Explicit
Role
Attributes
Rules
Explicit
User
Attribs
User
Attribs
User
Attribs


SUBJECTS
OBJECTS
MAC
Authorizations based on (user or group) permissions and object labels.
DAC
Authorizations based on (user or group) permissions. Zero knowledge of object sensitivity.
RBAC
Authorizations based on group permissions. User is part of a group.
Reference Monitor
Label

Mandatory Access Control (MAC): • Only system owner manages access control. • End user has no control over any privileges.	**Based Access Control (RBAC):** • Provides access based on the position an individual has in an organization.
Discretionary Access Control (DAC): • Least restrictive model. • Allows an individual complete control over any objects they own.	**Rule Based Access Control (RBAC).** • Dynamically assign roles to users based on criteria defined by owner or system administrator.

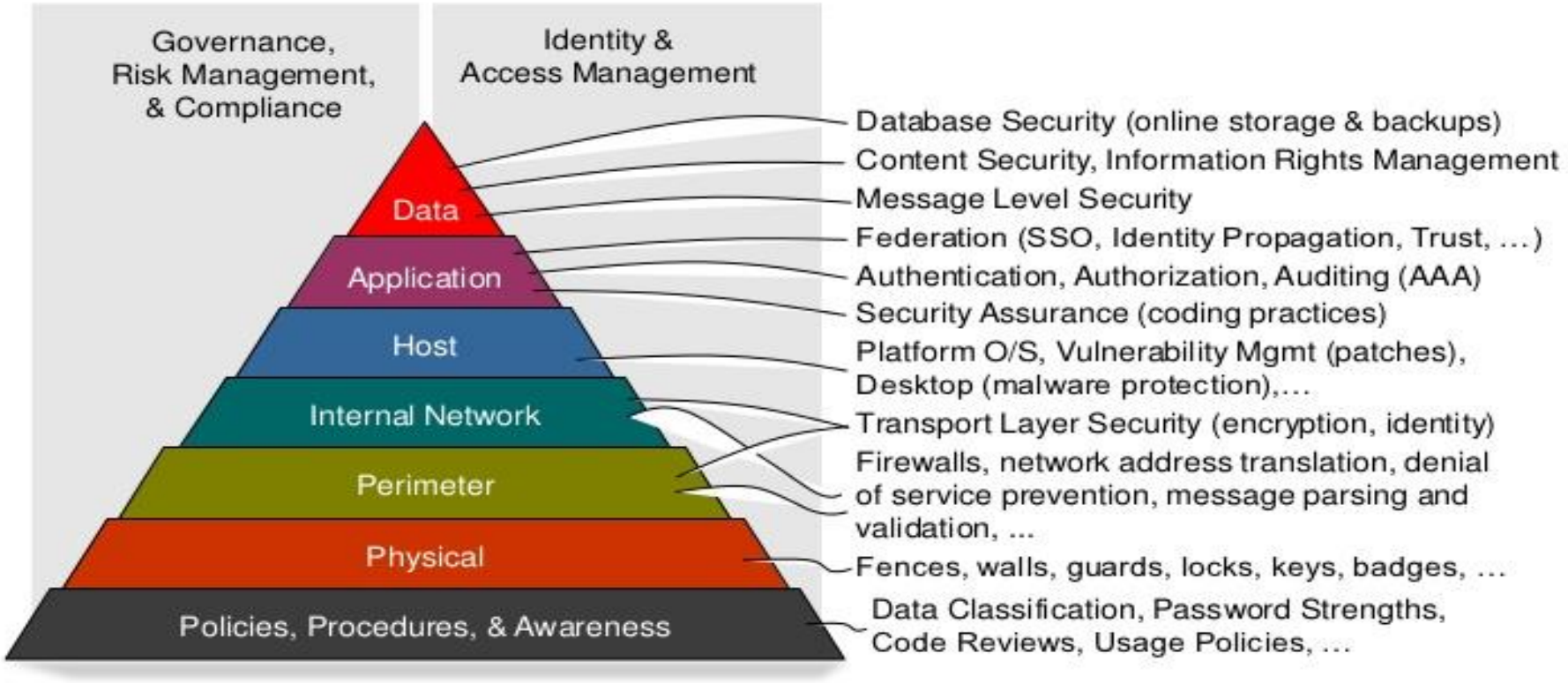
Defence-in-depth

- Defence-in-depth, or “cloud-in-depth” as it could be called, fit into the world of cloud security?
- Defence-in-depth is a security strategy that has been popular for a number of years (it pre-dates cloud computing). It is considered to be a best practice for IT security.
- Defense in depth is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system.

- Defense-in-depth represents the use of multiple security defenses to help mitigate the risk of security threats, if one component of the defense is being compromised.
- An example, could be an antivirus software installed on individual VM when there is already a virus protection on the firewalls within the same environment.
- Different security products from multiple vendors may be deployed to defend different potential vulnerable resources within the network.

- Defense-in-depth is an information assurance strategy in which multiple layers of defense are placed throughout the system.
- For this reason, it is also known as a “layered approach to security”. Because there are multiple measures of security at different levels, defense-in-depth gives additional time to detect and respond to an attack.
- This reduces the scope of a security breach. However, the overall cost of deploying defense-in-depth is often higher, compared to single-layered security mechanisms

Defense in Depth



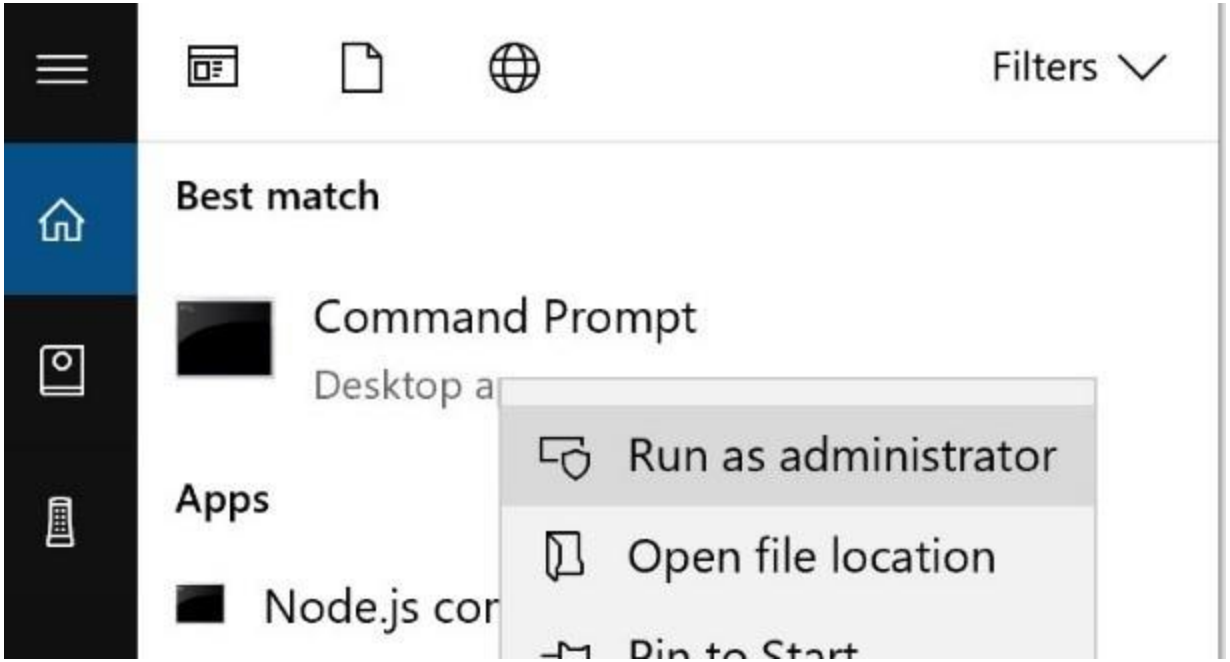
ORACLE

OTN Architect Day 2011

Least privilege

- Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.
- Applied to people, least privilege, sometimes called the principle of least privilege (POLP), means enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role. However, least privilege also applies to processes, applications, systems, and devices (such as IoT), in that each should have only those permissions required to perform an authorized activity.

In the Windows desktop, User Access Control (UAC) performs a POLP function – blocking or requesting access for administrative privileges as needed.




Thank You