Cloud Security & Monitoring

IT4090 – Cloud Computing

Software Defined Security

Software-defined security (SDS) is a type of security model in which the information security in a computing environment is implemented, controlled and managed by security software.

It is a software-managed, policy-driven and governed security where most of the security controls such as intrusion detection, network segmentation and access controls are automated and monitored through software.

The Principal of Least Privilege (PLOP)

PLOP is an information security concept

A user or a process should only be granted privileges that are essential to perform its intended function.

Identity and Access Management (IAM)

IAM solves the Principal of Least Privileges

IAM is a framework of policies and technologies to ensure users/process have the appropriate access to technology resources.

IAM is used to identify, authenticate and authorize users/processes who/which will be utilizing these technology resources.

IAM Components

Logical Organization

- The logical boundaries and operating domains for a given user/process.

Users

- Users/applications/services within the logical organization which needs to access resources.
- Has its own security credentials
- Can be part of one or more groups
- By default no permission to do anything

Groups

- Collection of users
- Does not have security credentials

IAM Components

Policies

- Collection of permissions.
- Permissions determine whether a request is allowed or denied

Roles

- Main component of Role Based Access Control
- Collection of policies
- Roles can be assumed by users/services
- When assumed, it gives you with temporary security credentials for your role session

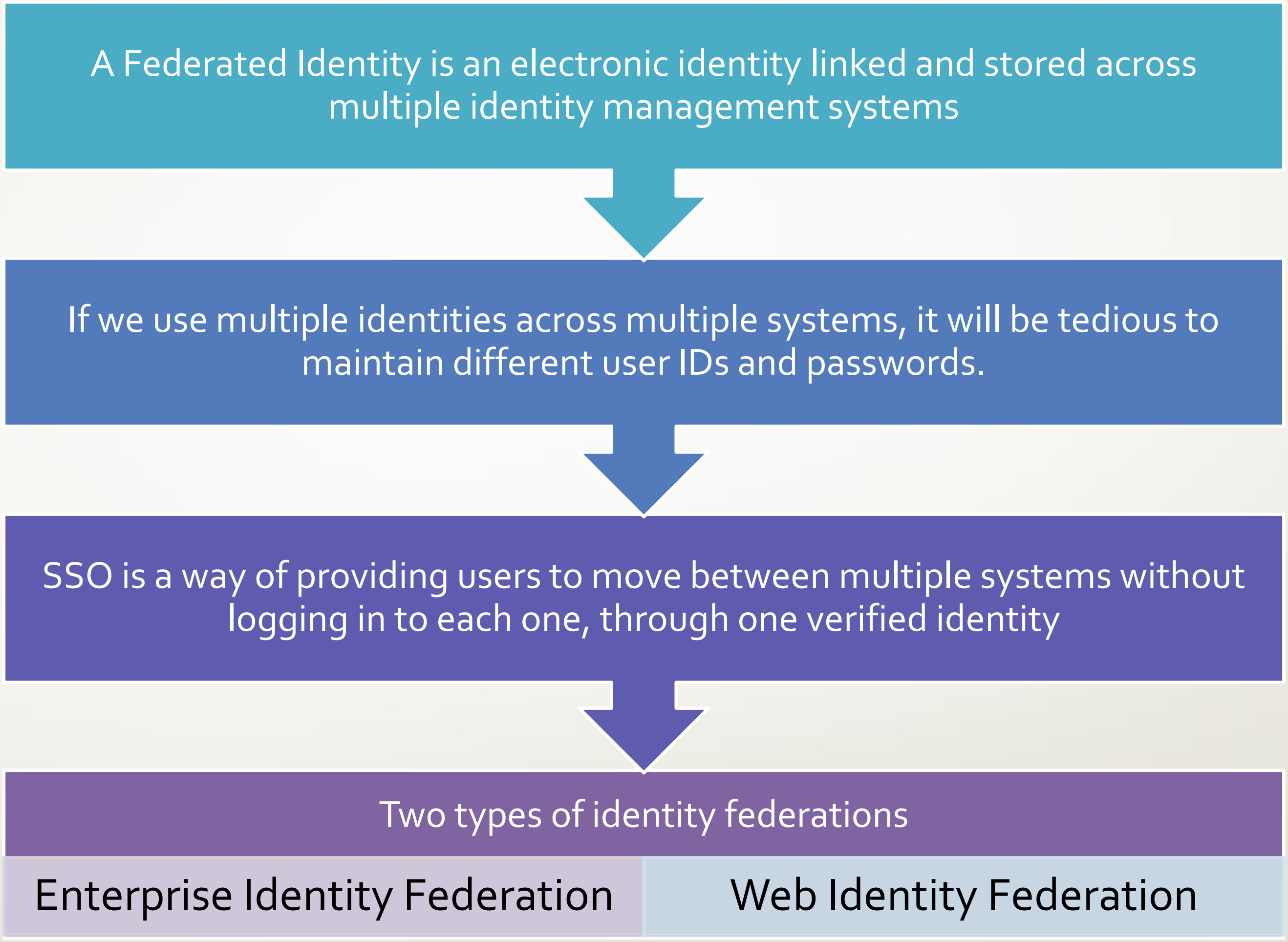
Multi Factor Authentication (MFA)

An electronic authentication method in which a user is granted access to a system only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

Factors

- Something the user has
  - Security token, smart card
- Something the user knows
  - Password, PIN
- Something the user is
  - Biometrics (fingerprint, face, voice, iris)
- Somewhere the user is
  - GPS location

Federated Identity & Single Sign On



A Federated Identity is an electronic identity linked and stored across multiple identity management systems

If we use multiple identities across multiple systems, it will be tedious to maintain different user IDs and passwords.

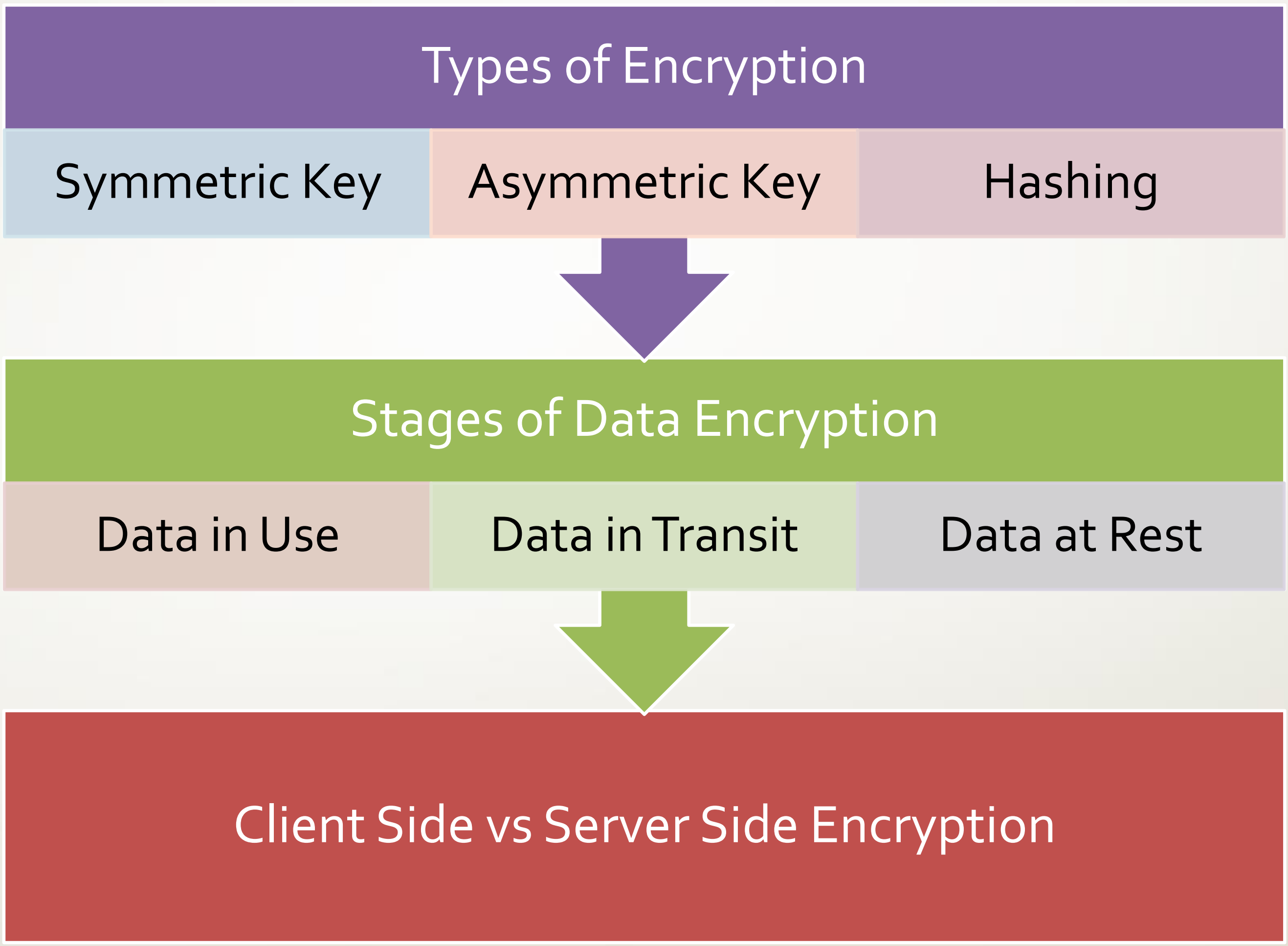
SSO is a way of providing users to move between multiple systems without logging in to each one, through one verified identity

Two types of identity federations

Enterprise Identity Federation

Web Identity Federation

Encryption - Recap



Types of Encryption

Symmetric Key

Asymmetric Key

Hashing

Stages of Data Encryption

Data in Use

Data in Transit

Data at Rest

Client Side vs Server Side Encryption

Cloud Security Risks & Threats

- Poor Access Management
- Data Breach / Leak / Loss
- Misconfiguration
- Insecure APIs
- Account Hijacking
- Lack of Visibility
- DoS / DDoS Attacks

Monitoring in Cloud

Cloud monitoring is a method of reviewing, observing, and managing the operational workflow in a cloud-based IT infrastructure.

Manual or automated management techniques confirm the availability and performance of websites, servers, applications, and other cloud infrastructure.

Example Services

- Datadog
- AppDynamics
- Azure Monitor
- Amazon CloudWatch

Metrics, Events & Logs

Metrics

- Raw data about resource usage or behaviour
- Collected via a monitoring agent
- Ex:- Details on CPU, memory, disk space usage

Events

- Events are generated by systems when something happens
- Captures what happened, where it happened, when it happened etc.
- Ex:- events from automation tools

Logs

- Provide information about what systems have been doing
- Extremely valuable in troubleshooting

Alerts

Reactive element of the monitoring system

Triggers actions based on changes in metrics / events / logs

Types of alerts

- Threshold based alerts
- Anomaly detection based alerts
- Heartbeat alerts

Alert output types

- Notifications
- Automated Actions