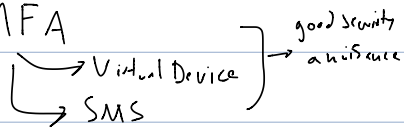


Top-down vs. bottom-up

Web Portal Security

- Username/password

- MFA



AWS Programmatic Access

ACCESSKEY } 2 LARGE
ACCESS KEY VALUE } Random #s

IAM identity & access management Active Directory

- Create user

- fine-grained access control

WHAT vs. HOW

- least privilege

Policy vs. Mechanism

- RBAC (Role-based access control)

- Federation - reuse account info

SHIBBOLETH - federation of campuses

PRO

CON

1. least privilege

1. Diff to use by nonexpert

2. least privilege

false positive

false negative

PA3 - IAM + ELS

- SERVICE IAM ROLE

AWS COMPUTE

- (1) IaaS - OS security
- (2) PaaS - less attack surface
- (3) Containers -
- (4) Functions - IAM

DATA

IAM

Other Security Services

- (1) CONFIG
- (2) CloudWatch - event-based system
- (3) CloudTrail - APIs

AWS + Data Encryption

- limited utility

BOX

- enforced encryption
- FERPA

1) ROPBOX?

OS Security

- (1) logging on to terminal
- (2) logging across network

Cloud Security

Better

(largest + small)

1. economies of scale

Worse

1. physically sharing w/ other enterprises

2. physical security

2. network isolation

3. not multiplexing humans

3. where is my data exactly?